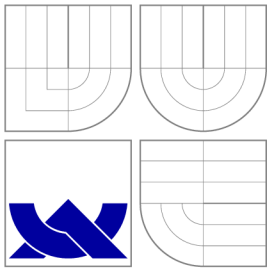
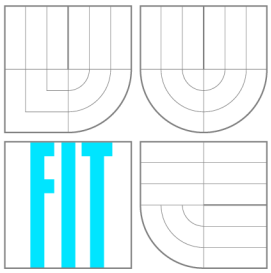


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ZACHOVÁNÍ VALIDITY MS EXCHANGE HLAVIČEK NA FILTRUJÍCÍM SMTP PROXY-SERVERU

PRESERVING VALIDITY OF MS EXCHANGE HEADERS ON FILTERING SMTP PROXY-SERVER

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PETER SZABÓ
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN RICHTER
SUPERVISOR

BRNO 2012

Abstrakt

Cílem této práce je lokalizace a návrh optimálního řešení problému, způsobujícího vzájemnou nekompatibilitu SMTP proxy-serveru AVG Linux Server Edition a poštovního serveru Microsoft Exchange. Práce popisuje různé možnosti řešení tohoto problému a určuje tu nejvhodnější z nich. V teoretické části poskytuje tato práce základní přehled o protokolu SMTP a o protokolech serveru Microsoft Exchange. Dále popisuje nejčastější hrozby týkající se e-mailové komunikace uživatelů a různé způsoby ochrany před nimi.

Abstract

The aim of this thesis is the localization and finding an optimal solution for a compatibility issue between two products, the AVG Linux Server Edition SMTP proxy-server and the Microsoft Exchange e-mail server. There are several possible solutions of this issue described and the most effective one is suggested as the final solution. In the first part, this thesis is providing a basic overview of the SMTP protocol and the protocols used in the Microsoft Exchanage server. The most common threats in the e-mail communication are also discussed here and several available solutions of protection against them are presented.

Klíčová slova

proxy-server, SMTP, server Exchange, e-mail, malware, spam, phishing, antivirus, šifrování e-mailových zpráv, postmarking

Keywords

proxy-server, SMTP, Exchange Server, e-mail, malware, spam, phishing, antivirus, e-mail encryption, postmarking

Citace

Peter Szabó: Zachování validity MS Exchange hlaviček na filtrujícím SMTP proxy-serveru, bakalářská práce, Brno, FIT VUT v Brně, 2012

Zachování validity MS Exchange hlaviček na filtrujícím SMTP proxy-serveru

Prohlášení

Prohlasuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pánů Ing. Lubomíra Kaštovského a Ing. Jana Richtera

.....
Peter Szabó
15. května 2012

Poděkování

Rád bych poděkoval firmě AVG Technologies CZ, s. r. o., která mi umožnila tuto práci vytvořit a poskytla mi technické prostředky k její realizaci. Dále bych rád poděkoval Ing. Lubomíru Kaštovskému z firmy AVG Technologies, který mi po celou dobu poskytoval užitečné odborné rady týkající se produktů firmy AVG Technologies a různých částí této práce. Velké poděkování patří i vedoucímu mé práce, Ing. Janovi Richterovi, za jeho rady především při psaní této práce.

Obsah

1 Úvod **3**

2 Protokoly SMTP/ESMTP a Microsoft Exchange protokol **4**
2.1 Protokol SMTP/ESMTP 4
2.1.1 Dôležité príkazy protokolu SMTP 4
2.1.2 Príklad komunikácie pomocou protokolu SMTP 6
2.1.3 Významné rozšírenia protokolu SMTP 7
2.2 Protokoly servera Microsoft Exchange 7
2.2.1 Protokoly RPC Primer a RPC Storage and Retrieval 7
2.2.2 Protokoly na konverziu dát a súborov 8
2.2.3 Protokoly služby ActiveSync 8
2.2.4 Protokoly Directory services a Profile services 8
2.2.5 Protokoly Name Service Provider Interface 8
2.2.6 Rozšírenia protokolov založených na štandardoch 8
2.2.7 Protokoly na spracovanie správ 9
2.2.8 Rozšírenia protokolu WebDAV 9
2.2.9 Protokoly založené na webových službách a na protokole HTTP . . 9

3 Možnosti ochrany e-mailovej komunikácie a používateľov **10**
3.1 Hrozby pri e-mailovej komunikácii 10
3.1.1 Malware 11
3.1.2 Spam 12
3.1.3 Phishing 13
3.2 Ochrana e-mailovej komunikácie na strane používateľa 14
3.3 Ochrana e-mailovej komunikácie na strane servera 15
3.3.1 Použitie rôznych antivírusových riešení u klientov a na serveroch . . 15
3.3.2 Viacnásobná antivírusová ochrana 15
3.4 Ochrana podpisovaním a šifrovaním správ 16
3.4.1 Protokol S/MIME 17
3.4.2 Protokol OpenPGP 18

4 Ochrana e-mailovej komunikácie pomocou SMTP proxy-servera **19**
4.1 Možnosti nasadenia SMTP proxy-servera 19
4.2 Výhody a nevýhody použitia SMTP proxy-servera 20
4.3 Možnosti filtrovania prechádzajúcich e-mailových správ na proxy-serveri . . 20
4.3.1 Riešenie prítomnosti škodlivého obsahu v e-mailovej správe 20

5 Realizácia proxy-servera pomocou AVG Linux Server Edition **23**
5.1 Popis produktu AVG Linux Server Edition 24
5.2 Testovacie prostredie 24
5.2.1 Zapojenie, nastavenie a činnosť proxy-servera 24
5.2.2 Spôsob testovania 26
5.2.3 Zistené problémy 26
5.3 Zdroj problému nevalidných e-mailových správ 26
5.3.1 Postmarking správ pomocou hlavičiek X-CR-HashedPuzzle a X-CR-PuzzleID 27
5.4 Zachovanie validity správ 27
5.4.1 Prepočítavanie podpisu e-mailových správ 28
5.4.2 Test algoritmu na výpočet podpisu e-mailových správ 29
5.4.3 Odstránenie SMTP hlavičiek e-mailových správ s podpisom 30
5.4.4 Najideálnejšie riešenie v prípade skúmaného produktu 30

6 Záver **32**

A Ukážky e-mailových správ **35**
A.1 Podvodná správa obsahujúca phishing 35
A.2 Hlavičky testovacích e-mailových správ 36
A.2.1 Doručená, neinfikovaná e-mailová správa odoslaná z klienta Thunderbird bez zapojeného SMTP proxy-servera 36
A.2.2 Doručená, infikovaná e-mailová správa odoslaná z klienta Thunderbird so zapojeným SMTP proxy-serverom 36
A.2.3 Doručená, infikovaná e-mailová správa odoslaná z klienta Outlook bez zapojeného SMTP proxy-servera 37
A.2.4 Doručená, neinfikovaná e-mailová správa odoslaná z klienta Outlook so zapojeným SMTP proxy-serverom 37
A.2.5 Nedoručená, infikovaná e-mailová správa odoslaná z klienta Outlook so zapojeným SMTP proxy-serverom 38

B Konfiguračné súbory **39**
B.1 Ukážka časti konfiguračného súboru programu avgtcpd 39

C Obrázky **40**
C.1 Schéma testovacej počítačovej siete 40
C.2 Zapnutie generovania podpisov v odosielaných správach v aplikácii Outlook 2007 41

D Tabuľky **42**
D.1 Zhrnutie testovacích e-mailov s infikovaným obsahom 42
D.2 Výsledky testov generovania podpisu e-mailových správ 43

E Obsah CD **44**

Kapitola 1

Úvod

E-mailová komunikácia hrá v dnešnej dobe dôležitú úlohu predovšetkým pri každodennej firemnej komunikácii, no nemenej dôležitá je aj pri komunikácii osobného charakteru. Je preto nesmierne dôležité, aby bola čo najviac spoľahlivá. Spoľahlivosť e-mailovej komunikácie ale často ohrozujú rôzne faktory, pred ktorými je potrebné sa chrániť. Ide predovšetkým o spam, phishing a malware. Na trhu existuje množstvo rôznych nástrojov a metód, ktoré poskytujú účinnú ochranu pred týmito hrozbami. Táto práca má za cieľ priblížiť čitateľovi tieto hrozby a rôzne možnosti ochrany voči nim. Práca ďalej predvádza príklad konkrétneho komerčného riešenia v ktorom lokalizuje a rieši problémy týkajúce sa spoľahlivosti doručovania e-mailových správ.

Práca v prvej časti kapitoly 2 pojednáva o protokole SMTP, základnom stavebnom prvku celého systému e-mailovej komunikácie, o jeho príkazoch a rozšíreniach. Druhá časť tejto kapitoly stručne popisuje protokoly a ich rozšírenia používané serverom Microsoft Exchange a klientskými aplikáciami, ktorí s ním komunikujú. Ďalej kapitola 3 poskytuje základný prehľad o rôznych hrozbách číhajúcich hlavne na používateľov e-mailovej komunikácie, no často aj na administrátorov, ktorý jej funkčnosť zabezpečujú. Ďalej sa v tejto kapitole popisujú rôzne spôsoby ochrany používateľov a serverov voči spomínaným hrozbám. Kapitola 4 sa zameriava na jeden konkrétny druh ochrany e-mailovej komunikácie, a to pomocou nasadenia proxy-servera, ktorý prechádzajúce e-mailové správy kontroluje a filtruje. Na záver sa práca v kapitole 5 zaoberá produktom *AVG Linux Server Edition*, ktorý poskytuje antivírusovú a antispamovú ochranu pre poštové servery prostredníctvom SMTP proxy-servera.

Hlavným cieľom tejto práce, ktorý je obsiahnutý v kapitole 5, je lokalizácia a návrh efektívneho riešenia problému spôsobujúceho nekompatibilitu produktu *AVG Linux Server Edition* s poštovým serverom *Microsoft Exchange*, kvôli ktorej dochádza k nedoručovaniu niektorých e-mailových správ prechádzajúcich cez proxy server obsiahnutý v tomto produkte. Práca popisuje samotný proces zisťovania a odhaľovania spomínaného problému a popisuje rôzne možnosti jeho riešenia. Jednotlivé možnosti riešenia ďalej porovnáva a snaží sa poukázať na to najefektívnejšie a najpraktickejšie z nich.

Kapitola 2

Protokoly SMTP/ESMTP a Microsoft Exchange protokol

Protokol **SMTP/ESMTP** slúži k odosielaniu elektronickej pošty (e-mailov). Klient, ktorý odosiela e-mail komunikuje s poštovým serverom pomocou tohoto protokolu. Rovnaký protokol používajú aj samotné poštové servery predávajúce si e-maily medzi sebou. [13] Momentálne je prevažne používaná verzia **ESMTP**, ktorá je vylepšeným a rozšíreným nasledovníkom staršieho protokolu **SMTP**.

Poštový server počúva štandardne na **TCP** porte *25*. Po inicializácii pripojenia klientom server odošle uvítaciu správu obsahujúcu informácie o sebe, a klientovi tým oznamuje, že je pripravený na komunikáciu. Klient následne začne so serverom komunikovať a pomocou štandardných príkazov predá odosielanú správu serveru. Server ju po prijatí buď rovno uloží do e-mailovej schránky príjemcu (ak je schránka príjemcu umiestnená na danom serveri), alebo prepošle na príslušný server, na ktorom sa e-mailová schránka príjemcu nachádza. [27]

2.1 Protokol SMTP/ESMTP

Jeho podrobná pôvodná špecifikácia sa nachádza v dokumente *RFC-821* [21] z roku 1982. Protokol je *case insensitive* t. j. nezáleží na veľkosti znakov a server by ich nemal rozlišovať. Každý príkaz sa ukončuje sekvenciou znakov `<CR><LF>` (***C**arriage **R**eturn* – `ASCII 0x0D`, ***L**ine **F**eed* – `ASCII 0x0A`).

Pôvodná verzia protokolu (viď [21]) obsahovala striktne štrnásť príkazov, každý zložený zo štyroch znakov. Protokol bol časom upravený a rozšírený o nové možnosti tak, aby vyhovoval dnešným požiadavkám týkajúcich sa predovšetkým bezpečnosti e-mailovej komunikácie.

2.1.1 Dôležité príkazy protokolu SMTP

Protokol **SMTP** podporuje nasledovné základné príkazy: **HELO**, **EHLO**, **MAIL**, **RCPT**, **DATA**, **RSET**, **VRFY**, **EXPN**, **NOOP**, **QUIT** a **HELP**. [13]

Príkazy HELO a EHLO

Tiento príkazy slúžia na inicializáciu komunikácie medzi klientom a serverom a súčasne na identifikáciu klientského počítača. Klient posiela príkaz **HELO/EHLO** a za ním med-

zerou (<SP> ***Sp**ace* – ASCII 0x20) oddelenú svoju identifikáciu (*FQDN* adresa klienta[1]). V prípade, že sa komunikácia inicializuje príkazom **EHLO**, server umožní klientovi použiť rozšírenia protokolu **SMTP**, ktoré podporuje a klientovi odpovie zaslaním zoznamu týchto rozšírení. Ak server rozšírenia neakceptuje, klient obdrží oznam, že príkaz **EHLO** nie je podporovaný [14]. Ak ale klient inicializuje komunikáciu príkazom **HELO**, ide o komunikáciu v pôvodnej verzii protokolu **SMTP** a je možné používať iba základné príkazy bez rozšírení.
Príklad zápisu príkazu:

```
HELO client.example.com<CR><LF>
```

Príkaz MAIL

Príkazom **MAIL** sa začína samotný proces prenosu e-mailovej správy. Ako prvý parameter príkazu musí byť povinne kľúčové slovo **FROM:** a následne v druhom parametri sa špecifikuje odosielateľ správy (e-mailová adresa odosielateľa správy obalená špicatými zátvorkami).
Príklad zápisu príkazu:

```
MAIL FROM: <john.doe@example.com><CR><LF>
```

Príkaz RCPT

Tento príkaz slúži na špecifikáciu jedného alebo viacerých príjemcov správy. Prvý parameter príkazu je kľúčové slovo **TO:** a za ním nasleduje e-mailová adresa príjemcu správy obalená špicatými zátvorkami. Ak je príjemcov správy viacero, príkaz **RCPT** sa zadáva viackrát – pre každého príjemcu zvlášť.
Príklad zápisu príkazu:

```
RCPT TO: <jane.doe@mail.com><CR><LF>
```

Príkaz DATA

Samotný text správy sa zadáva príkazom **DATA**. Tento príkaz nemá žiadne parametre a po jeho zadaní SMTP server čaká na zadanie textu správy, ktorý musí končiť špeciálnou sekvenciou znakov <CR><LF>.<CR><LF>.
Príklad zápisu príkazu:

```
DATA<CR><LF>
 Test message from John Doe to Jane Doe.<CR><LF>
.<CR><LF>
```

Príkaz RSET

Príkazom **RSET** sa ruší aktuálna transakcia, teda anulujú sa všetky príkazy zadané od odoslania poslednej správy, prípadne od vytvorenia spojenia so serverom ak sa ešte žiadna správa neodosielala (okrem príkazu **HELO**). Príkaz nemá žiadne parametre a ruší vždy aktuálne prebiehajúcu transakciu.

[1] **FQDN** (**Fully Qualified Domain Name**, plne kvalifikované doménové meno) je jednoznačné doménové meno, ktoré absolútne udáva pozíciu uzla v stromovej hierarchii DNS [20]

Príkaz VRFY

Tento príkaz slúži na overenie, či zadaný reťazec je prihlasovacie meno (login) existujúceho používateľa. Ak áno, server vráti celé meno používateľa aj s jeho e-mailovou adresou. Tento príkaz predstavuje bezpečnostné riziko a môže slúžiť na získanie e-mailových adries používateľov napríklad pre účely rozosielania *spamu*[16]. Na väčšine serverov je preto vypnutý alebo povolený iba pre autentizovaných používateľov.
Príklad zápisu príkazu:

```
VRFY john.doe<CR><LF>
```

Príkaz EXPN

Príkaz **EXPN** overuje existenciu zadaného názvu zoznamu adries (mailing list). Ak zoznam existuje, server vráti zoznam adries v ňom zahrnutých. Tento príkaz podobne ako aj príkaz **VRFY** predstavuje bezpečnostné riziko, pomocou ktorého je možné získať zoznam e-mailových adries[16]. Preto sa táto funkcia na väčšine serveroch taktiež vypína, prípadne povoľuje sa iba pre autentizovaných používateľov.
Príklad zápisu príkazu:

```
EXPN mailing.list.name<CR><LF>
```

Príkaz NOOP

Príkaz **NOOP** nemá žiadny parameter a nijako neovplyvňuje odosielanie správy. Server na tento príkaz iba pošle odpoveď **OK**. Príkaz môže slúžiť napríklad na overenie, či je spojenie so serverom stále aktívne.

Príkaz QUIT

Príkaz **QUIT** slúži na ukončenie spojenia. Server po prijatí tohoto príkazu pošle odpoveď **OK** a následne ukončí spojenie s klientom. Príkaz nemá žiadny parameter.

2.1.2 Príklad komunikácie pomocou protokolu SMTP

```
S: 220 smtp.example.com Simple Mail Transfer Service Ready
C: HELO client.example.com
S: 250 Hello client.example.com
C: MAIL FROM:<john.doe@example.com>
S: 250 OK
C: RCPT TO:<jane.doe@mail.com>
S: 250 OK
C: DATA
S: 354 Send message content; end with <CRLF>.<CRLF>
C: Test message from John Doe to Jane Doe.
C: .
S: 250 OK, message accepted for delivery: queued as 12345
C: QUIT
S: 221 Bye
```

2.1.3 Významné rozšírenia protokolu SMTP

Medzi najvýznamnejšie rozšírenia protokolu **SMTP** patria nasledovné: **8BITMIME**, **AUTH**, **STARTTLS**, **SMTPUTF8**.

Rozšírenie AUTH

Pomocou tohoto rozšírenia môže server vyžadovať od klienta aby sa autentizoval pred tým, ako začne odosielať e-maily. Taktiež použitie príkazov **VRFY** a **EXPN** (viď 2.1.1) môže byť z bezpečnostných dôvodov limitované na použitie až po úspešnej autentizácii. Použitím autentizácie sa zabráni tomu, aby pomocou daného servera odosielali správy cudzí ľudia (typicky spameri) [26]. Možností autentizácie je niekoľko: **PLAIN**, **LOGIN**, **OTP**, **DIGEST-MD5**, **KERBEROS**, **ANONYMOUS**. [5]

Rozšírenie STARTTLS

Toto rozšírenie používa *TLS (Transport Layer Security)*, ktoré rozširuje komunikáciu *TCP* o šifrovanie pre zaistenie súkromia a integrity správ. Hlavným účelom tohoto rozšírenia je zaistenie súkromia komunikácie medzi klientom a serverom a taktiež overuje totožnosť daného servera. Ďalšou užitočnou možnosťou je nasadenie šifrovania v kombinácii s rozšírením **AUTH** v prípade overovania metódou **PLAIN**. Pri tejto metóde sa totiž heslo používateľa posiela v otvorenej textovej podobe, čo je možné bez šifrovania spojenia ľahko zneužiť. [5]

2.2 Protokoly servera Microsoft Exchange

Microsoft Exchange server používa množstvo rôznych protokolov na komunikáciu s ostatnými produktami firmy Microsoft. Patria k nim rôzne štandardné protokoly ako sú napríklad SMTP, POP3, IMAP a pod., ich štandardné aj neštandardné rozšírenia, no aj špeciálne protokoly používané výlučne na komunikáciu medzi produktami firmy Microsoft. [18]

2.2.1 Protokoly RPC Primer a RPC Storage and Retrieval

Do tejto skupiny patrí veľké množstvo protokolov (vyše 30), ktoré zabezpečujú prenos dát medzi klientmi a servermi. Protokoly *RPC Primer* dáta zoskupujú do väčších celkov a následne ich naraz prenášajú, pričom protokoly *Storage and Retreival* umožňujú ukladanie a získavanie správ týkajúcich sa kalendárov, úloh a kontaktov používateľa. [18]

Do skupiny RPC Primer patria nasledovné najdôležitejšie protokoly: **Wire Format Protocol**, **Remote Operations (ROP) List and Encoding Protocol**, **Store Object Protocol**, **Message and Attachment Object Protocol** a **Table Object Protocol**. Ich podrobný popis je k dispozícii v kap. 2.2.2.1 v [18].

Skupinu RPC Storage and Retreival Protocols tvoria protokoly umožňujúce ukladanie a získavanie správ týkajúcich sa kalendárov, úloh a kontaktov používateľa [18]. Ide predovšetkým o tieto protokoly: **Best Body Retrieval Algorithm**, **Configuration Information Protocol**, **E-Mail Object Protocol**, **Reminder Settings Protocol**, **E-Mail Rules Protocol**, **Offline Address Book (OAB) Public Folder Retrieval Protocol** a **Sharing Message Object Protocol**. Kompletný zoznam týchto protokolov aj s ich stručným popisom je taktiež k dispozícii v [18], v kap. 2.2.2.2.

2.2.2 Protokoly na konverziu dát a súborov

Tieto protokoly umožňujú klientom a serverom konvertovať rôzne typy súborov a ďalších dát na formáty podporované serverom Microsoft Exchange [18]. Patria sem predovšetkým protokoly **iCalendar to Appointment Object Conversion Algorithm**, **RFC2822 and MIME to E-Mail Object Conversion Algorithm**, **S/MIME E-Mail Object Algorithm**, **Rich Text Format (RTF) Compression Algorithm** a **vCard to Contact Object Conversion Algorithm**. Popis týchto protokolov sa nachádza v kap. 2.2.3 v [18].

2.2.3 Protokoly služby ActiveSync

Tieto protokoly umožňujú zdieľanie a synchronizáciu dát medzi serverom a mobilnými zariadeniami. Poskytujú taktiež možnosť notifikácie klientov ak nastane nejaká zmena na serveri. Napríklad ak sa do schránky používateľa doručí nová e-mailová správa. [18] Ide napríklad o protokoly **ActiveSync Calendar Class Protocol**, **ActiveSync Command Reference Protocol**, **ActiveSync Contact Class Protocol**, **ActiveSync Data Types**, **ActiveSync E-Mail Class Protocol**, **ActiveSync HTTP Protocol**, **ActiveSync Short Message Service (SMS) Protocol** a **ActiveSync Tasks Class Protocol**. Kompletný zoznam protokolov aj s ich popisom sa nachádza v kap. 2.2.4 v [18].

2.2.4 Protokoly Directory services a Profile services

Ide o protokoly umožňujúce klientom automatické zisťovanie a následné použitie konfigurácie e-mailového servera. Patrí sem konkrétne protokol **Autodiscover HTTP Service Protocol**, ktorý rozširuje službu DNS a adresárové služby tak, aby klientom poskytovali aj nastavenia e-mailového servera. Ďalej ide o protokol **Autodiscover Publishing and Lookup Protocol** umožňujúci klientom zistiť kde služba využívajúce predošlý protokol (Autodiscover HTTP service) beží. [18]

2.2.5 Protokoly Name Service Provider Interface

Tieto protokoly umožňujú klientom prístup k informáciám o adresáre kontaktov, používateľoch a skupinách používateľov prostredníctvom adresárovej služby. Slúžia napríklad na presmerovanie požiadaviek od klientov na príslušný adresárový server, či ako rozhranie pre klientov pristupujúcich k adresárovej službe prostredníctvom protokolu MAPI. [18] Patria sem napríklad protokoly **Address Book Name Service Provider Interface (NSPI) Referral Protocol** a **Exchange Server Name Service Provider Interface (NSPI) Protocol**. Ich popis spolu s popisom ostatných protokolov z tejto kategórie sa nachádza v kap. 2.2.6 v [18].

2.2.6 Rozšírenia protokolov založených na štandardoch

Server Exchange podporuje niekoľko rôznych štandardných protokolov pre e-mailovú komunikáciu ako sú napr. SMTP, POP3, IMAP4 a WebDAV a protokol LDAP pre adresárové služby. Tieto rozšírenia sa týkajú predovšetkým autentizácie a autorizácie používateľov pripájajúcich sa na server prostredníctvom týchto štandardných protokolov. Dokumentácie týchto rozšírení ďalej obsahujú zoznam príkazov spomínaných štandardných služieb, mieru ich podpory a popis ich funkčnosti na serveri Exchange. [18] Ide napríklad o protokoly **Internet Message Access Protocol Version 4 (IMAP4) Extensions**, **Lightweight**

Directory Access Protocol (LDAP) Version 3 Extensions, **Post Office Protocol Version 3 (POP3) Extensions**, **Simple Mail Transfer Protocol (SMTP) Mail Submission Extensions** a **SMTP Protocol: AUTH LOGIN Extension**. Pre podrobnejšie informácie viď kap. 2.2.7 v [18].

2.2.7 Protokoly na spracovanie správ

Patria sem rôzne protokoly a algoritmy využívané na interpretáciu metadát v e-mailových správach. **Journal Record Message File Format** popisuje štruktúru e-mailových správ odosielaných zo servera Exchange. **Spam Confidence Level Protocol** a **Phishing Warning Protocol** slúžia na odhalenie e-mailových správ obsahujúcich spam, resp. phishing. A napokon **E-Mail Postmark Validation Algorithm** popisuje algoritmus slúžiaci na podpisovanie užitočných e-mailových správ a ich následné rozlíšenie od spamu. Tento algoritmus je významnou súčasťou problému riešeného v kapitole 5 tejto práce a je podrobnejšie popísaný v kapitole 5.3.1. [18]

2.2.8 Rozšírenia protokolu WebDAV

Protokol WebDAV (Web Distributed Authoring and Versioning Protocol) rozširuje protokol HTTP/1.1 o ďalšie hlavičky, metódy a pod. Umožňuje čítanie dát zo serverov a taktiež ich zapisovanie na ne (viď RFC 2518). Server Exchange protokol WebDAV ďalej rozširuje, a to napríklad týmito protokolmi: **WebDAV Extensions for Calendar Support**, **WebDAV Extensions for Contacts Support**, **WebDAV Extensions for Documents Support**, **WebDAV Extensions for E-Mail Support** a **WebDAV Extensions for Search**. [18] Kompletný zoznam týchto rozšírení aj s ich popisom je k dispozícii v kap. 2.2.9 v [18].

2.2.9 Protokoly založené na webových službách a na protokole HTTP

Tieto protokoly servera Exchange sú založené na implementácii protokolu HTTP/1.1. Protokoly označované ako webové služby sú zase založené na implementácii protokolu *WS-I Basic Profile 1.0*[2] [18]. Patrí sem veľké množstvo protokolov, medzi inými aj **Web Service Configuration Protocol**, **Attachment Handling Web Service Protocol**, **Folder Sharing Web Service Protocol**, **Notifications Web Service Protocol**, **Push Notifications Web Service Protocol**, **Mailbox Search Web Service Protocol** a **User Configuration Web Service Protocol**. Kompletný zoznam protokolov aj s ich stručným popisom sa nachádza v kap. 2.2.10 v [18].

[2] **WS-I Basic Profile 1.0** – `http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html`

Kapitola 3

Možnosti ochrany e-mailovej komunikácie a používateľov

V dnešnej dobe, keď nevyžiadaná pošta tvorí väčšinu svetovej e-mailovej komunikácie je ochrana proti vírusom, spamu a ďalším hrozbám veľmi dôležitá. Ako uvádza firma *Symantec Corporation* vo svojej mesačnej správe[1], vo februári 2012 tvoril spam až **68%** všetkých odoslaných e-mailových správ. Toto číslo je pri tom relatívne nízke vzhľadom k štatistikám z roku 2010, keď v mesiaci august sa množstvo spamu vyšplhalo až na hodnotu vyše **92%** všetkých odoslaných e-mailových správ[2].

Používateľom je preto potrebné poskytnúť dostatočnú ochranu pred nevyžiadanou poštou. Chrániť ich možno priamo na poštovom serveri, kde sa nevyžiadaná pošta automaticky zmaže, umiestni sa do samostatnej zložky, prípadne sa prítomnosť vírusu, spamu či inej hrozby vyznačí v predmete správy. Taktiež je možné prípadný vírus zo správy odstrániť a na túto akciu upozorniť v predmete alebo tele samotnej správy.

Používateľ sa môže samozrejme chrániť aj sám použitím antivírusového softvéru priamo vo svojom počítači, tablete či smartphone. V tomto prípade antivírusový software kontroluje správy počas ich prijímania z poštového servera a na prítomnosť hrozby používateľa včas upozorní.

3.1 Hrozby pri e-mailovej komunikácii

Pri používaní e-mailovej komunikácie na nás číha mnoho rôznych hrozieb. Z nich je v súčasnosti najväčším a najrozsiahlejším problémom spam. Tieto správy sú pre skúseného používateľa väčšinou neškodné. Skúsený používateľ totiž je schopný odhaliť potenciálne hrozby a nenechá sa teda oklamať a nalákať na rôzne podvody. V prípade menej skúsených používateľov, ľudí bez informatického vzdelania ovládajúcich iba základné činnosti na počítači, je ale situácia úplne iná. Práve oni sú týmto hrozbám najviac vystavovaní.

Väčšina týchto hrozieb sa zameriava práve na neskúsených používateľov, ktorí majú tendenciu im ľahko podľahnúť. Stačí ich totiž nalákať pomocou predmetu e-mailovej správy sľubujúceho alebo ponúkajúceho na prvý pohľad zaujímavú skutočnosť a je relatívne jednoduché ich tým oklamať.

[1] `http://www.symanteccloud.com/download.get?filename=SYMCINT_2012_02_February_FINAL.PDF`
[2] `http://www.symanteccloud.com/download.get?filename=MLI_2010_08_August_Final_EN.pdf`

3.1.1 Malware

Malware je súhrnné označenie pre rôzne druhy škodlivého softvéru ako sú napr. *počítačové vírusy*, *trójske kone*, *spyware* a *adware*.

Malware je program, ktorý sa sám, bez vedomia používateľa, nainštaluje na napadnutý počítač. Jeho cieľom je často získať, upraviť alebo zmazať dáta uložené v ňom. Ďalšie druhy malware-u môžu mať za cieľ zneprístupniť napadnutý počítač pre vonkajší svet (servery) alebo naopak umožniť útočníkovi napadnutý počítač ovládať a použiť ho napríklad na účely počítačovej kriminality [10]. Typickým príkladom sú tzv. *botnety*[3], kde sú tisícky až milióny počítačov napadnutých malwarom použitých napríklad na synchronizované *DDoS*[4] útoky či rozosielanie spamu.

Malware sa môže šíriť rôznymi spôsobmi. Najčastejšie sa tak stáva pomocou infikovaných USB kľúčov, webových stránok využívajúcich zraniteľnosti webových prehliadačov no taktiež pomocou e-mailov obsahujúcich infikované prílohy, prípadne odkazy na napadnuté webové stránky. V poslednom čase sa čoraz častejšie stretávame s útokmi škodlivého softvéru cez chat na rôznych sociálnych sieťach, kedy škodlivý softvér z napadnutého počítača rozosiela pochybné odkazy používateľom zo zoznamu kontaktov napadnutého používateľa.

Počítačové vírusy

Jednoznačne najznámejšou a najobávanejšou počítačovou hrozbou medzi bežnými používateľmi sú *počítačové vírusy*. Pojmom „počítačový vírus“ sa medzi laickými používateľmi často nesprávne označujú všetky typy malwaru. V skutočnosti ale ide iba o jednu z podskupín súhrnne označovaných ako **malware**.

Napadnutie počítačovým vírusom môže mať rôzne následky:

- Môžu byť „nedeštruktívne“ a používateľa iba nejakým spôsobom obťažovať a obmedzovať: zobrazovať obrázky, animácie, správy, prehrávať hudbu alebo zvukové efekty... Takéto útoky sú väčšinou neškodné a ich cieľom je iba vystreliť si z používateľa, prípadne ho upozorniť na nejakú tému alebo udalosť. [10]

- Existujú ale aj tzv. „deštruktívne“ vírusy spôsobujúce používateľovi oveľa väčšie problémy. Tieto vírusy môžu mať za cieľ odcudziť citlivé dáta, prípadne ich nejakým spôsobom poškodiť (vymazať alebo náhodne upraviť obsah súborov, naformátovať celý pevný disk a pod.) alebo ich inak zmanipulovať – napr. zašifrovaním celého obsahu pevného disku. Ich úlohou môže tiež byť zníženie dostupnosti systému (náhodné reštarty operačného systému, simulácia poškodeného hardvéru, ...). Iné vírusy zase môžu na napadnutom počítači hromadiť nelegálny materiál, prípadne ho využiť za účelom získavania nelegálneho materiálu a spôsobiť tak napadnutému používateľovi problémy so zákonom (viď str. 340 v [10]). [10]

Trójske kone

Pojem *trójsky kôň* sa spája s literárnym dielom Odysea gréckeho básnika Homéra. Je to jednoduchý počítačový program skladajúci sa z klientskej a serverovej časti. Serverová časť

[3] **Botnet** – Skupina veľkého množstva malwarom napadnutých počítačov („bot“) pripojených do internetu ovládaných z jedného zdroja [22]

[4] **DDoS** (Distributed Denial of Service) – Rozsiahle synchronizované útoky na jednu počítačovú sieť alebo konkrétny server s cieľom ich preťaženia a tým znemožnenia ich fungovania

po nainštalovaní sa na napadnutý počítač tajne umožní útočníkovi pristupovať pomocou klientskej časti k tomuto počítaču. [10]

Serverová časť je väčšinou program ukrytý v inom, na prvý pohľad neškodnom, programe. Akonáhle sa tento „neškodný“ program spustí, nainštaluje sa serverová časť trójskeho koňa bez vedomia používateľa. Taký trójsky kôň môže mať množstvo rôznych funkcií závisiacich od povahy daného programu. Môže napríklad reštartovať napadnutý počítač, odosielať z neho používateľove súbory, spúšťať iné programy, ničiť dáta, zaznamenávať a odosielať stlačené klávesy, atď. [10]

Trójske kone ale potrebujú počúvať na nejakom porte, aby sa k nim klientská časť mohla pripojiť. Preto pri použití správne nastaveného *firewallu* je možné hrozbu, ktorú predstavujú celkom úspešne eliminovať. Správne napísaný trójsky kôň, ktorý ešte nebol zverejnený môže totiž antivírusový program ľahko prehliadnuť. Firewall je preto účinný prostriedok na zamedzenie škôd spôsobených trójskymi koňmi [10].

Spyware

Pod pojmom *spyware* sa označuje akákoľvek počítačová technológia slúžiaca k získaniu informácií o nejakej osobe alebo organizácii bez ich vedomia a súhlasu. Spyware môže byť nainštalovaný na počítač niekoľkými skrytými spôsobmi. Môže byť napríklad súčasťou počítačového vírusu alebo iného programu nainštalovaného samotným používateľom. Spyware môže taktiež existovať ako samostatný program ktorý je potrebné na cieľovom počítači ručne nainštalovať. [8] Akýkoľvek program odosielajúci dáta z počítača, v ktorom je nainštalovaný, bez súhlasu používateľa je považovaný za spyware [25].

Spyware sa často používa na získavanie rôznych informácií ako sú napríklad zoznam stlačených kláves (získavanie hesiel), zoznam navštívených webových stránok, zoznam nainštalovaných programov, verzia operačného systému a pod. Tieto programy môžu taktiež získavať kontakty, údaje kreditných kariet a iné osobné informácie uložené v napadnutom počítači. [8]

Adware

Za *adware* sa vo všeobecnosti považuje softvér, ktorý do počítača sťahuje reklamy a následne ich zobrazuje. Tieto programy môžu reklamy zobrazovať buď náhodne, alebo tie dokonalejšie môžu sledovať aktivitu používateľa (navštívené webové stránky a pod.) a ponúkať mu predovšetkým cielenú reklamu. [25]

Niektoré z týchto programov sa do počítača dostávajú vo forme vírusov alebo trójskych koní – takéto programy možno definitívne považovať za adware. Iné programy spadajúce do tejto kategórie si ale používateľ často inštaluje sám a úplne dobrovoľne. Sú to väčšinou programy ponúkané zadarmo a reklamy sú ich súčasťou ako cena za ich používanie. Často sa napríklad stáva, že práve adware je maskovaný ako softvér slúžiaci na vyhľadanie a odstránenie škodlivých programov v počítači (viď PurityScan[5]). [25]

3.1.2 Spam

Definitívne najrozšírenejšou hrozbou, ktorá sa rozšírila hlavne v posledných rokoch je nevyžiadaná pošta, t. j. *spam*. Spam totiž momentálne predstavuje drvivú väčšinu e-mailovej komunikácie, čo je naozaj veľmi alarmujúce. Neustále sa nasadzujú nové riešenia v boji

[5] `http://www.symantec.com/security_response/writeup.jsp?docid=2003-090516-2325-99`

proti nevyžiadanej pošte a aj napriek jej značnému poklesu v posledných dvoch rokoch je toto číslo stále príliš vysoké.

Za spam sa považuje predovšetkým nevyžiadaná reklamná pošta rozposielaná hromadne veľkému množstvu príjemcov bez toho, aby o ňu žiadali [1]. Definícií spamu je niekoľko:

- Medzi spam jednoznačne patria automaticky zasielané správy množstvu adresátom, ktorí si ich neobjednali a nemajú možnosť si ich sami zrušiť. Tieto správy spravidla pochádzajú zo zahraničia, sú písané v najrôznejších jazykoch (prevláda angličtina) a ponúkajú najrôznejšie produkty (nelegálny software, lieky, a pod.). Tieto správy chodia často opakovane tým istým príjemcom. [1]

- Inou, menej agresívnou, formou spamu sú väčšinou jednorázovo a ručne zasielané ponuky od rôznych českých či slovenských firiem. Odber týchto správ sa väčšinou dá spoľahlivo zrušiť a každý seriózny obchodník takúto požiadavku používateľa rešpektuje [1]. Takéto ponuky môžu byť pre niektorých používateľov často aj užitočné a preto je ich označovanie za spam celkom individuálne.

- Za tzv. spamovanie možno označiť aj preposielanie rôznych reťazových správ, ktoré nenesú žiadny informatívny, či inak užitočný obsah. Takéto správy sa šírili hlavne v minulých rokoch a momentálne už ich výskyt upadá.

3.1.3 Phishing

Phishing je forma sociálneho inžinierstva, pri ktorej sa útočník snaží podvodom vylákať tajné alebo citlivé údaje od používateľa. Podvod spočíva v napodobnení elektronickej komunikácie (e-mailová správa) od dôveryhodnej alebo verejnej organizácie. Používateľ je následne zo správy odkázaný na podvodnú stránku, ktorá náramne pripomína, prípadne je úplne rovnaká ako originálna stránka. Táto napodobenina originálnej stránky slúži na vylákanie citlivých údajov od používateľa, ako sú napríklad prihlasovacie meno a heslo, údaje platobných kariet, atď. [12] Používateľ, ktorý si nevšimne že sa nenachádza na skutočnej stránke, v snahe prihlásiť sa do svojho konta zadá svoje prihlasovacie údaje, ktoré sa na podvodnej stránke iba uložia. Následne môže byť používateľ presmerovaný na originálnu stránku, a preto vôbec nemusí zaregistrovať, že sa stal obeťou phishingu.

Typy phishingových útokov

Existuje množstvo rôznych spôsobov ako vykonať útok pomocou phishingu. Stále vznikajú novšie a sofistikovanejšie metódy, voči ktorým je potreba účinne sa brániť. Phisheri sú väčšinou skúsení profesionáli, ktorí presne vedia ako na bezbranných a nevedomých používateľov zaútočiť. Majú dostatočné zdroje a môžu si dovoliť investovať čas a peniaze k vytvoreniu premyslených útokov. Málokrát sa stáva, aby takéto útoky vykonávali amatéri. [12]

Útok pomocou jednej konkrétnej metódy je málo pravdepodobný. Častejšie sa používa kombinácia rôznych metód pre dosiahnutie čo najväčšej efektivity útoku. Príkladom použitia kombinovaného útoku môže byť podvodný e-mail, ktorý odkáže používateľa na infikovanú stránku. Táto stránka následne nainštaluje na používateľov počítač jednoduchý malware. Tento malware po tom ako sa spustí, pozmení obsah súboru *hosts*[6] a pridá do neho záznam, ktorý pre nejakú potencionálne kritickú stránku (napr. stránka banky)

[6]**Súbor *hosts*** – súbor operačného systému obsahujúci preklady DNS názvov na IP adresy, ktoré sa použijú prioritne bez kontaktovania DNS servera.

vráti namiesto správnej IP adresy IP adresu iného servera, na ktorom sa nachádza podvodná verzia originálnej stránky. Následne, keď sa nič netušiaci používateľ pokúsi prihlásiť do svojho internetového bankovníctva, zadá do internetového prehliadača adresu banky a miesto originálnej stránky sa mu zobrazí tá podvodná. To všetko napriek tomu, že adresa v prehliadači je správna. [12]

3.2 Ochrana e-mailovej komunikácie na strane používateľa

U používateľa je najúčinnejšou formou ochrany obozretnosť a dodržovanie základných pravidiel bezpečného surfovania na internete:

- Neotvárať prílohy a neklikať na odkazy v e-mailoch od neznámych ľudí či organizácií. Obzvlášť ak ide o správy predovšetkým v anglickom jazyku ponúkajúce rôzne lieky, pornografiu a iné nevyžiadané produkty.
- Na webových stránkach neklikať na rôzne podozrivé reklamy sľubujúce napríklad peniaze alebo produkty zadarmo.
- Pravidelne si aktualizovať operačný systém aj aplikácie nainštalované v počítači.
- Používať zložité heslá a mať rôzne heslá pre rôzne služby. Minimálne je dôležité registrovať sa na stránkach pod iným heslom ako je heslo do e-mailovej schránky ktorej adresu pri danej registrácii taktiež uvádzame. Je dobré mať dôležitejšie heslá (zvlášť heslo pre prihlasovanie na počítač, zvlášť pre e-mailovú schránku a pod.) a menej dôležité heslá (pre rôzne jednorázové registrácie na menej dôležitých webových stránkach) a aspoň tie dôležité pravidelne obmieňať za nové.
- Mať nainštalovaný *firewall* a povoľovať v ňom iba aplikácie, ktoré poznáme a o ktorých vieme, že k svojej činnosti potrebujú prístup do internetu.

Nemenej dôležité je aj použitie kvalitného antivírusového softvéru. Väčšina moderných antivírusových programov disponuje rôznymi rozšíreniami, ktoré spolupracujú priamo s poštovými klientmi a umožňujú tak účinnú ochranu proti malwaru, spamu a ďalším hrozbám. Je nepísaným pravidlom, že za dobré a kvalitné veci sa platí, preto je dobré antivírusovú ochranu nepodceniť a za kvalitný softvér si radšej zaplatiť.

Samozrejme nestačí mať antivírusový softvér zakúpený a nainštalovaný, je veľmi dôležité zabezpečiť, aby mal vždy aktuálnu databázu definícií. Bez najnovších aktualizácií totiž aj ten najkvalitnejší antivírusový program môže byť ľahko prekonateľný najnovším škodlivým softvérom. Antivírusové programy chránia používateľov v prípade že si e-maily čítajú pomocou poštových klientov nainštalovaných lokálne v počítači, no aj v prípade, že si poštu prezerajú online, pomocou webového prehliadača.

V prípade lokálnych poštových klientov pracujú antivírusové programy väčšinou vo forme rozširujúceho modulu, ktorý automaticky kontroluje všetky prijaté aj odoslané správy. Z infikovaných správ následne odstraňujú nebezpečné prílohy, filtrujú spam a správy podozrivé z phishingu.

V prípade klientov pracujúcich online priamo vo webovom prehliadači sú možnosti ochrany na strane používateľa čiastočne obmedzené. V tomto prípade je možné kontrolovať iba prílohy správ, a aj tie iba vtedy, ak sa ich používateľ rozhodne stiahnuť do svojho počítača. V takom prípade antivírusové programy väčšinou sťahovanie infikovanej prílohy

zablokujú. Ochrana proti spamu a phishingu je v tomto prípade prakticky nemožná, no dá sa veľmi efektívne realizovať na strane servera (viď 3.3).

Firewall nainštalovaný v počítači klienta má kľúčovú funkciu hlavne vtedy, ak je už počítač nakazený malwarom. Správne nakonfigurovaný firewall totiž nedovolí hociktorej aplikácii aby komunikovala s okolím a tým efektívne zabraňuje šíreniu malwaru na ďalšie počítače [23]. Veľký význam má hlavne vo firemných sietiach, kde sa malware môže z jedného nakazeného počítača veľmi rýchlo rozšíriť na ostatné počítače nachádzajúce sa v rovnakej sieti a spôsobiť tým firme nemalé škody.

3.3 Ochrana e-mailovej komunikácie na strane servera

Množstvo antivírusových programov sa vyvíja aj vo verziách pre servery. Tieto programy následne umožňujú kontrolovať a filtrovať e-maily už na serveri ešte pred tým, než sa dostanú k používateľovi. Kontrola e-mailových správ priamo na serveri je dôležitá hlavne vtedy, ak si používatelia prezerajú e-maily cez webové rozhranie. Vtedy totiž nie je možné filtrovať spam a iný nevhodný obsah pomocou antivírusového programu nainštalovaného v počítači klienta a je potrebné takúto kontrolu vykonávať už na serveri. Antivírusová ochrana sa môže do poštového servera integrovať buď ako rozširujúci modul (plugin) alebo formou proxy-servera (viď kapitola 4).

Kontrola e-mailov na strane servera má samozrejme význam aj v prípade, že používateľ sťahuje e-maily do svojho počítača pomocou poštového klienta. V tom prípade sa pošta kontroluje dvakrát, väčšinou rôznymi antivírusovými programami, čo znižuje šancu na preniknutie e-mailu obsahujúceho nevhodný obsah.

Medzi serverovými riešeniami má najväčší význam antispamová ochrana, ktorá pri správnej konfigurácii dokáže používateľa úplne odbremeniť od spamu a ďalších nežiaducich správ. Spam sa väčšinou premiestňuje do špeciálneho adresára, z ktorého sa správy po určitom čase automaticky odstraňujú. To, či sa tento adresár má na počítač používateľa sťahovať spolu s ostatnou prijatou poštou, si už každý používateľ môže nastaviť sám.

3.3.1 Použitie rôznych antivírusových riešení u klientov a na serveroch

Aj keď je na klientských počítačoch nasadené kvalitné antivírusové riešenie, je dôležité, aby bolo na serveroch nasadené riešenie od iného výrobcu. Nikdy sa totiž nestáva, aby práve jedno konkrétne antivírusové riešenie malo aktualizácie k novému vírusu ako prvé (viď kap. 3.3.2). [28]

Takéto riešenie teda jednoznačne zvyšuje šancu na zachytenie nového vírusu. Ak príde aktualizácia k novému vírusu do antivírusového programu bežiaceho na serveri, vírus v infikovanej e-mailovej správe sa zachytí už tu. Ak sa ale aktualizácia objaví skôr v antivírusovom programe bežiacom na klientských počítačoch, vírus sa zachytí až po stiahnutí prijatej e-mailovej správy do e-mailového klienta, no ešte stále včas. [28]

Tento spôsob ochrany samozrejme tiež, tak ako žiadna iná, nechráni na sto percent, no je určite účinnejšia ako používanie rovnakého antivírusového riešenia na klientských počítačoch aj na serveroch.

3.3.2 Viacnásobná antivírusová ochrana

Táto forma antivírusovej ochrany spočíva v nasadení viacerých antivírusových riešení od rôznych výrobcov na ochranu jedného servera. Možno tak dosiahnuť ešte vyšší stupeň

ochrany ako pri riešení spomínanom v kapitole 3.3.1. Hlavne vo veľkých firmách je dôležité nespoliehať sa na včasné aktualizácie jedného konkrétneho antivírusového programu, ale zvýšiť ochranu nasadením viacerých riešení [23].

Za normálnych okolností nie je možné mať na jednom počítači nainštalovaných viacero antivírusových programov, keďže by jednotlivé programy mohli považovať databázy definícií ostatných za vírusy a odstrániť ich. Existujú však riešenia, ktoré kombináciu viacerých antivírusových programov umožňujú (napr. GFI MailSecurity[7] v sebe zapuzdruje až 5 rôznych antivírusových programov).

Viacnásobná antivírusová ochrana pomáha výrazne znížiť čas medzi vypustením vírusu a stiahnutím potrebnej aktualizácie na daný server. Žiadny z dostupných antivírusových riešení totiž nie je vždy jednoznačne najrýchlejší a najefektívnejší [11]. Rýchlosť vydania aktualizácie k novo objavenému vírusu a efektivita jeho nájdenia sa totiž u každého jedného vírusu značne líši. Firme, ktorá k jednému vírusu vydá aktualizáciu ako prvá už behom pár hodín, to pri inom víruse môže trvať aj niekoľko dní (viď tab. 1 a tab. 2 na str. 4 v [11]).

Napriek tomu, že viacnásobná antivírusová ochrana je lepšia ako nasadenie jedného konkrétneho antivírusového riešenia, je treba mať na pamäti, že nejde o doslova „viacnásobnú ochranu“. Päť antivírusových programov totiž neochráni server päť krát viac, iba poskytne päť šancí na zachytenie škodlivého softvéru, ktorý sa snaží do chránenej počítačovej siete preniknúť. Možno to prirovnať k prechodu cez päť bezpečnostných kontrol na letisku. Každá kontrola je viac-menej rovnaká, no každá prebieha trocha inak a tým sa zvyšuje šanca na zachytenie nechcenej hrozby. [11]

3.4 Ochrana podpisovaním a šifrovaním správ

Ochrana podpisovaním a šifrovaním správ, alebo tzv. end-to-end zabezpečenie umožňuje zabezpečiť integritu e-mailových správ, prípadne znemožňuje zobrazenie obsahu správ tretím osobám. Používateľa môže čiastočne ochrániť pred phishingom a spamom, no nie pred prenosom malwaru. End-to-end zabezpečenie správy vykonáva odosielateľ a správa ostáva zabezpečená počas celej cesty až k adresátovi bez toho, aby jej zabezpečenie mohol niekto počas cesty porušiť [7]. Správy môžu byť zašifrované celé, takže ich obsah nie je možné prečítať v prípade odchytenia správy treťou osobou. Táto možnosť je síce bezpečnejšia, no napriek tomu menej využívaná. Druhá možnosť je posielať správy v otvorenej podobe, no s priloženým podpisom, ktorý zabezpečuje integritu správy a chráni pred jej modifikáciou treťou osobou.

Podpisovanie e-mailových správ spočíva v použití súkromných a verejných kľúčov. Odosielateľ podpisuje správu pomocou svojho súkromného kľúča a to tak, že sa vytvorí hash správy a ten sa pomocou súkromného kľúča zašifruje a priloží do tejto e-mailovej správy. Adresát po prijatí e-mailovej správy nezávisle vypočíta jej hash a porovná s hashom získaného dešifrovaním podpisu priloženého v prijatej správe pomocou verejného kľúča odosielateľa. [7]

Pri šifrovaní e-mailových správ sa často používa tzv. elektronická obálka. Svoje opodstatnenie má pri použití *asymetrickej kryptografie* (šifrovanie pomocou súkromného a verejného kľúča), ktorá je pri šifrovaní dlhých správ príliš pomalá. Preto sa správa najprv zašifruje pomocou *symetrickej kryptografie* (šifrovanie aj dešifrovanie jedným spoločným kľúčom) použitím náhodne vygenerovaného tajného kľúča. Tento kľúč sa následne asymetricky zašifruje pomocou verejného kľúča adresáta správy a vloží sa do elektronickej obálky.

[7] `http://www.gfi.com/exchange-antivirus-software#features`

Adresát potom dešifruje šifrovací kľúč pomocou svojho súkromného kľúča a pomocou získaného kľúča dešifruje aj samotnú e-mailovú správu. Takýto postup je výhodný aj v prípade, že má správa viac adresátov. V tom prípade sa náhodný kľúč použitý k symetrickému šifrovaniu správy zašifruje asymetricky toľko krát, koľko má správa adresátov. Pre každého adresáta sa na šifrovanie náhodného kľúča použije jeho verejný kľúč. Všetky kľúče sa potom vložia do elektronickej obálky. [7]

Šifrované (podpísané) správy si teda medzi sebou môžu posielať iba osoby, ktoré sa na tom dopredu dohodnú a vymenia si svoje verejné kľúče. V praxi je napríklad možné používať podpisovanie správ pri komunikácii v rámci firmy, či s bankou alebo iným subjektom s ktorým sa vymieňajú citlivé údaje. No nič nebráni v používaní šifrovanej komunikácie aj v e-mailoch osobného charakteru.

Proti phishingu je možné sa chrániť napríklad tak, že sa dva subjekty (napr. zamestnanci firmy) medzi sebou dohodnú, že budú všetky správy povinne podpisovať a nepodpísané správy nebudú považovať za vierohodné. Ak teda jednému zamestnancovi dorazí nepodpísaná správa, v ktorej ho druhý zamestnanec žiada o zaslanie citlivých údajov, môže ju považovať za podozrivú a jej pravosť si u druhého zamestnanca overiť. Potenciálny útočník totiž privátny kľúč druhého zamestnanca k dispozícii nemá a nemôže preto správu, v ktorej sa tvári ako on, právoplatne podpísať. V praxi sa takáto situácia často rieši firemnými politikami, ktoré vyslovene zakazujú výmenu citlivých informácií (napr. prístupové mená a heslá na servery) prostredníctvom e-mailu a zamestnanci k nim majú prístup napríklad cez patrične zabezpečené firemné úložisko. No aj napriek tomu podpisovanie či šifrovanie e-mailových správ svoje praktické uplatnenie nájde. Každé bezpečnostné opatrenie, ktoré používateľov príliš nezaťažuje je totiž užitočné a znižuje riziko potenciálneho útoku na počítač používateľa či celú firemnú sieť.

Možností šifrovania a podpisovania e-mailových správ je niekoľko. V minulosti existovali protokoly **PEM** a **MOSS**, no v poslednej dobe sa rozšírili predovšetkým protokoly **S/MIME** a **OpenPGP**, pričom jasným favoritom sa ukazuje práve protokol S/MIME [7, 15]. Žiaľ, ani jeden z nich nie je príliš rozšírený medzi ľudmi so základnými počítačovými znalosťami [4]. Najväčším problémom je, že pri šifrovaní e-mailovej komunikácie je potrebné aby k tomu aktívne prispel samotný používateľ, pričom napríklad pri šifrovaní webovej komunikácie pomocou SSL certifikátov zariadi všetko webový server a webový prehliadač používateľa [4]. Väčšia zložitosť má samozrejme svoje opodstatnenie. Pri šifrovaní webovej komunikácie sa používateľ väčšinou nezaujíma o identitu druhej strany (neplatí pri používaní internet bankingu a podobných citlivých stránok), no pri e-mailovej komunikácii je overenie a potvrdenie identity odosielateľa správy kľúčové [4].

3.4.1 Protokol S/MIME

Protokol S/MIME sa najviac rozšíril predovšetkým kvôli jeho natívnej podpore v množstve e-mailových klientov. Je založený na infraštruktúre *PKI*, kde sú verejné kľúče používateľov podpísané certifikačnou autoritou, ktorej odosielateľ aj adresát zabezpečenej e-mailovej správy dôverujú. Aj vďaka natívnej podpore e-mailových klientov je teda jeho použitie pri šifrovaní e-mailových správ oproti konkurenčnému OpenPGP relatívne jednoduché.

Protokol S/MIME disponuje troma ľubovoľne kombinovateľnými funkciami použiteľnými na zabezpečenie e-mailových správ. Správy umožňuje digitálne podpisovať, šifrovať ich celý obsah a taktiež komprimovať. Použiť ich je síce možné v ľubovoľnom poradí, no je dobré nasadzovať ich v správnom poradí tak, aby bol výsledok čo najefektívnejší. Ideálne je preto správu najprv komprimovať, následne zašifrovať a nakoniec ešte elektronicky

podpísať. Efektívna je samozrejme aj kombinácia, kde sa po komprimácii najprv podpisuje až potom šifruje obsah správy. V druhom prípade ale nie je možné podpis správy automaticky verifikovať bez jej predošlého dešifrovania a sprístupnenia jej obsahu, čo nie je príliš praktické v prípade hromadného automatického overovania podpisov prijatých e-mailových správ. [7]

3.4.2 Protokol OpenPGP

Narozdiel od protokolu S/MIME, OpenPGP používa decentralizovanú správu dôveryhodnosti verejných kľúčov a nepotrebuje preto certifikačné autority. Používatelia si svoje verejné kľúče podpisujú vzájomne a vytvára sa tým veľká sieť ľudí, ktorí si navzájom dôverujú (tzv. „Web of Trust“). [15]

Podobne ako S/MIME aj OpenPGP umožňuje e-mailové správy nielen digitálne podpisovať ale aj šifrovať. OpenPGP sa okrem zabezpečenia obsahu e-mailových správ často používa aj na šifrovanie súborov na disku, prípadne existujú nástroje[8], ktoré pomocou tohoto protokolu dokážu zašifrovať aj celý obsah pevného disku.

Web of Trust

Web of Trust je sieť ľudí, ktorí používajú protokol OpenPGP na šifrovanie a podpisovanie svojich správ a súborov. Títo používatelia si navzájom zabezpečujú dôveryhodnosť svojich verejných kľúčov. Každý používateľ podpíše kľúč tým používateľom, ktorých pozná, dôveruje im a vie dosvedčiť, že ide naozaj o toho používateľa, za ktorého sa daný používateľ vydáva a že údaje uvedené v jeho kľúči sú pravdivé. Každý používateľ má teda aj svoj kľúč podpísaný od ľudí, ktorí ho poznajú a dôverujú mu.

V prípade, že používateľovi A dorazí digitálne podpísaná e-mailová správa od iného používateľa B, ktorého on síce nepozná, ale jeho kľúč je podpísaný používateľom C ktorého používateľ A (príjemca správy) pozná a dôveruje mu, tak používateľ A vie, že používateľ B je ten za koho sa vydáva a môže mu dôverovať, lebo mu dôveruje aj používateľ C. Takto to funguje aj v prípade vzdialenejších vzťahov, kedy jeden používateľ môže dôverovať druhému, ktorého nepozná priamo on, ani žiadny z jeho známych, no pozná ho a dôveruje mu napr. známy jeho známeho. [15]

[8] PGP Whole Disk Encryption – `http://www.symantec.com/whole-disk-encryption`

Kapitola 4

Ochrana e-mailovej komunikácie pomocou SMTP proxy-servera

Ochrana e-mailovej komunikácie pomocou SMTP proxy-servera predstavuje veľmi efektívne a hlavne univerzálne riešenie použiteľné v kombinácii s hociktorým poštovým serverom. Proxy-server sa totiž neintegruje priamo do poštového servera, ale predstavuje medzičlánok, ktorý komunikuje s externými klientmi a následne prijaté správy preposiela na ďalšie spracovanie do poštového servera. Proxy-server teda maskuje skutočný poštový server [2] a tým výrazne znižuje šancu jeho napadnutia hackermi alebo škodlivým softvérom.

Okrem odbremenenia poštového servera od priamej komunikácie s externými klientmi SMTP proxy-server slúži často aj na filtrovanie spamu, malwaru a ďalších hrozieb [2]. Túto úlohu môže vykonávať buď sám pomocou zabudovaného antivírusového riešenia, alebo pomocou externej služby, ktorej sa jednotlivé správy predajú na kontrolu. Činnosti vykonávané proxy-serverom pri filtrovaní e-mailov sú podrobnejšie popísané v kapitole 4.3.

4.1 Možnosti nasadenia SMTP proxy-servera

SMTP proxy-server môže byť nasadený na ochranu poštového servera dvomi spôsobmi.

Ten prvý, jednoduchší, no súčasne menej bezpečný spôsob je, že proxy-server beží na jednom fyzickom serveri spolu s poštovým serverom. Takéto riešenie je vhodné hlavne v malých počítačových sietiach s minimálnym bezpečnostným ohrozením. V tomto prípade slúži proxy-server iba na zamedzenie priameho prístupu na poštový server z vonkajšej siete.

Druhý spôsob si vyžaduje nasadenie dvoch fyzických serverov. Jeden je vyhradený pre proxy-server a na druhom beží samotný poštový server. Toto riešenie je síce nákladnejšie, no oveľa bezpečnejšie. Okrem výhod ktoré ponúka prvé riešenie, navyše chráni poštový server pred napadnutím napríklad DoS/DDoS útokom, prípadne inými hrozbami, ktoré by mali za následok pád poštového servera. Týmto hrozbám totiž čelí iba proxy-server, no ten neobsahuje žiadne e-mailové správy ani iné dáta, ktoré by sa mohli stratiť alebo poškodiť.

Reálne sa nasadenie SMTP proxy-serverov kombinuje s tzv. demilitarizovanou zónou (DMZ). Ide o sieť, ktorá sa nenachádza ani v internej, ani v externej sieti, ale na ich rozhraní. Vytvorenie takejto siete musí byť podporované na firewalle, ktorý je na ochranu internej siete použitý. Pravidlá firewallu sú nastavené tak, aby sa do DMZ dalo dostať z externej aj internej siete, no z DMZ sa do internej už dostať nedalo a komunikácia z DMZ do internej siete musela prechádzať výhradne cez firewall [6]. SMTP proxy-servery sa často umiestňujú práve do DMZ kde sa na nich pripájajú klienti z externej siete a skontrolované

správy sa následne cez firewall preposielajú na poštový server umiestnený v internej sieti.

4.2 Výhody a nevýhody použitia SMTP proxy-servera

Jednoznačnou a jednou z najväčších výhod nasadenia SMTP proxy-servera je zvýšenie bezpečnosti e-mailovej komunikácie v počítačovej sieti. Proxy-server totiž slúži ako „vstupná brána“ k poštovému serveru a navonok nevidno, čo sa za ňou nachádza. Potenciálny útočník preto nemá možnosť dostať sa priamo k poštovému serveru a kompromitovať ho. Za proxy-serverom môže byť umiestnených aj viacero serverov, ktoré si medzi sebou rozdeľujú záťaž. Navonok sa ale všetky javia ako jeden (vidno iba proxy-server). V prípade útoku je teda ohrozený iba proxy-server, no ten zvyčajne pri aplikácii správnych bezpečnostných opatrení žiadne dôležité dáta neobsahuje. Preto prípadné odstavenie proxy-servera spôsobí iba minimálne škody formou nedostupnosti služieb, no nestratia sa, ani neuniknú žiadne dôležité dáta.

Ďalšou výhodou je univerzálnosť a nezávislosť ochrany. SMTP proxy-server predstavuje samostatnú jednotku, ktorá je schopná spolupracovať s každým poštovým serverom. Dokáže relatívne jednoducho filtrovať e-mailové správy, ktoré ním prechádzajú, odstraňovať z nich vírusy, prípadne na ne v predmete alebo v tele správy upozorňovať. Možno ho taktiež použiť na filtrovanie akéhokoľvek nevhodného obsahu e-mailových správ, na filtrovanie adries odosielateľa či príjemcov. V prípade poruchy je možné proxy-server jednoducho vymeniť bez potreby akýchkoľvek zásahov do samotného poštového servera.

Nevýhodou je potreba vyhradiť pre STMP proxy-server samostatný fyzický server. Táto investícia je ale vzhľadom k miere prínosu k zvýšeniu bezpečnosti siete maximálne výhodná. SMTP proxy-server môže samozrejme bežať aj na rovnakom fyzickom serveri ako samotný poštový server ktorý chráni. Cena takejto realizácie je oveľa nižšia ako realizácia pomocou samostatného fyzického servera, no z hľadiska bezpečnosti chráni takáto realizácia poštový server iba symbolicky. V tomto prípade je použiteľný iba na ochranu e-mailových správ pred vírusmi a spamom, čím ale zostáva nevyužitý jeho značný potenciál.

4.3 Možnosti filtrovania prechádzajúcich e-mailových správ na proxy-serveri

Ako už bolo v kapitole 4.2 spomínané, SMTP proxy-server predstavuje univerzálne riešenie schopné spolupracovať s akýmkoľvek poštovým serverom. E-mailové správy prechádzajúce cez neho môže ľubovoľne modifikovať – pozmeniť napríklad ich predmet, text, prílohy či príjemcov správy. To z neho robí mohutný nástroj s na prvý pohľad nebezpečnými funkciami, ktoré ale pri správnom nasadení a správnej konfigurácii SMTP proxy-servera žiadne nebezpečenstvo nepredstavujú. Naopak, tieto funkcie sú nesmierne užitočné a nevyhnutné pre plnohodnotnú ochranu používateľov a samotného poštového servera pred e-mailovými správami so škodlivým obsahom (pre podrobnejšie informácie o škodlivom obsahu vyskytujúcom sa v e-mailových správach viď kap. 3.1).

4.3.1 Riešenie prítomnosti škodlivého obsahu v e-mailovej správe

Po identifikácii škodlivého obsahu v kontrolovanej e-mailovej správe má SMTP proxy-server niekoľko možností ako sa zachovať. Ak je nájdená hrozba identifikovaná ako malware, je najbezpečnejšie ju zo správy odstrániť. Môže sa jednať o prílohu kontrolovanej e-mailovej

správy alebo odkaz na webovú stránku obsahujúcu danú hrozbu. Odstránenie hrozby je teda veľmi jednoducho realizovateľné, no takéto riešenie môže mať aj svoje nevýhody. Príloha správy, či odkaz v nej môže totiž byť označený za potenciálnu hrozbu aj omylom. Žiadny antivírusový softvér totiž nie je dokonalý, a môže hrozbu identifikovať nesprávne. V tom prípade by teda došlo k odstráneniu neškodného obsahu správy, ktorý mohol byť pre príjemcu dôležitý. Je preto dôležité aby sa odstránenie prílohy alebo iného obsahu e-mailovej správy patrične indikovalo v tele alebo v predmete správy. Taktiež je veľmi užitočné, ak má príjemca správy možnosť sa k odstránenému obsahu dostať ak je presvedčený o tom, že tento obsah je bezpečný. To je možné riešiť napríklad dočasným umiestnením odstráneného obsahu na zabezpečený webový server a poskytnutím unikátneho odkazu na jeho stiahnutie v tele modifikovanej e-mailovej správy. Aj kvôli týmto dôvodom sa škodlivý obsah z e-mailových správ často neodstraňuje, iba sa upozorní na jeho prítomnosť v tele správy alebo v jej predmete a záleží len na používateľovi, ako s daným obsahom naloží.

V prípade nasadenia sofistikovanejšieho SMTP proxy-servera disponujúcim dokonalejším antivírusovým riešením či rozšírením, je možné prílohy infikované malwarom aj automaticky liečiť. V takomto prípade proxy server odovzdá infikovaný súbor z prílohy antivírusu, ten, ak je to možné, z neho odstráni malware a vyliečený súbor vráti proxy serveru, ktorý ním pôvodnú prílohu e-mailovej správy nahradí. Na takýto krok je ale vhodné tiež adresáta upozorniť a to buď v texte alebo v predmete kontrolovanej e-mailovej správy.

V prípade iných hrozieb ako sú napríklad spam či phishing má SMTP proxy server dve možnosti. Takúto správu môže jednoducho zahodiť a ďalej ju už neprepposielať alebo na prítomnosť hrozby v správe iba upozorniť. Upozorniť na hrozbu môže podobne ako v prípade malwaru buď indikáciou v predmete správy alebo v jej tele. Ideálne je upozornenie umiestniť do predmetu e-mailovej správy, keďže ju potom používateľ nemusí vôbec otvárať a pri väčšom množstve takýchto správ mu to ušetrí množstvo času.

Jedna z univerzálnych funkcií aplikovateľných na všetky e-mailové správy prechádzajúce SMTP proxy-serverom je ich preposielanie. Proxy-server má v tomto prípade niekoľko možností. Z e-mailovej správy môže odstrániť všetkých adresátov a preposlať ju iba na jednu preddefinovanú adresu alebo môže pôvodných príjemcov v e-mailovej správe ponechať a na preddefinovanú adresu doručiť iba kópiu tejto správy. Preposielanie je možné zase dvomi spôsobmi: server danú správu buď odošle sám pripojením sa na príslušný SMTP server spravujúci e-mailovú adresu, na ktorú sa správa preposiela, alebo túto adresu iba pridá do zoznamu adresátov a o doručenie sa postará poštový server, ktorého správy daný SMTP proxy-server filtruje.

Funkcia preposielania správ SMTP proxy-serverom na inú, preddefinovanú, adresu, je z hľadiska bezpečnosti a súkromia danej e-mailovej komunikácie celkom otázna. Porušuje sa tým súkromie príjemcu tejto e-mailovej správy, keďže sa jej obsah dostáva do rúk tretej osoby. Napriek tomu môže mať takáto funkcia svoje opodstatnenie a pri správnom nastavení SMTP proxy-servera môže byť často veľmi užitočná. SMTP proxy-server môže byť napríklad vo firme nastavený tak, aby všetky e-mailové správy obsahujúce nebezpečný obsah (spam, phishing, malware) preposielal okrem pôvodným adresátom aj administrátorovi firemnej počítačovej siete. Ten môže následne obsah týchto správ analyzovať a včas odhaliť prípadné pokusy o útok na počítačovú sieť či už pomocou malwaru, alebo podvodnej správy (phishig). Takéto e-mailové správy môžu mať za cieľ získanie prístupu k citlivým firemným údajom cez menej skúsených zamestnancov, ktorým sú tieto e-mailové správy odoslané. Administrátor môže pri zistení takejto skutočnosti vykonať potrebné bezpečnostné opatrenia a prípadnému útoku tak efektívne zabrániť.

SMTP proxy-server môže taktiež slúžiť na filtrovanie e-mailových správ na základe ad-

ries odosielateľa a adresátov správy. Môže obsahovať tzv. čiernu (blacklist) a bielu (whitelist) listinu zakázaných a povolených e-mailových adries. V tom prípade môže napríklad brániť doručovaniu e-mailových správ od odosielateľov, ktorých adresy sa nachádzajú na čiernej listine, či povoliť doručovanie iba od tých, ktorých adresy sú na bielej listine. Podobné zoznamy môžu existovať aj pre e-mailové adresy príjemcov. Zamietnuté e-mailové správy sa následne môžu buď zahadzovať, alebo zase preposielať administrátorovi počítačovej siete, či inej zodpovednej osobe.

Kapitola 5

Realizácia proxy-servera pomocou AVG Linux Server Edition

Praktickou časťou tejto práce bola realizácia menšej testovacej siete, v ktorej bol nasadený proxy-server **AVG Linux Server Edition**[1]. Realizácia prebiehala vo virtuálnom prostredí pomocou virtualizačného nástroja **VMware Workstation**[2]. Cieľom praktickej časti bolo predovšetkým overenie funkčnosti proxy-servera v spolupráci s poštovým serverom **Microsoft Exchange Server 2007**. Súčasťou toho bolo tiež nájdenie možných problémov spôsobujúcich nekompatibilitu týchto dvoch produktov, ich presná lokalizácia a analýza potenciálnych riešení nájdených problémov. Nakoniec bolo potrebné navrhnúť a poprípade aj naimplementovať najvhodnejšie riešenie.

Vznik tejto práce podnietil už známy problém existujúci medzi týmito dvomi produktami. Šlo o nedoručovanie niektorých e-mailových správ, resp. ich doručovanie do spamového koša aj v prípade, že žiadny spam neobsahovali. Jednalo sa o správy, v ktorých AVG proxy-server objavil nežiaduci obsah (spam, malware, phishing) a následne pozmenil ich predmet.

Je síce pravda, že správy obsahujúce spam do spamového koša patria, no nie vždy to platí aj u správ, v ktorých bol identifikovaný malware. Tie by mali byť doručené medzi ostanú poštu s jasne vyznačeným upozornením na identifikovaný malware. Používateľ následne môže sám rozhodnúť o tom, akú dôležitosť bude danému upozorneniu prikladať. Obsah e-mailovej správy totiž mohol byť identifikovaný ako škodlivý aj omylom a preto je niekedy (hlavne v prípade skúsených používateľov) lepšie ponechať konečné rozhodnutie o osude správy priamo na používateľa.

Spomínaný problém môže obmedzovať prácu proxy-servera aj v prípade iných potenciálnych funkcií nesúvisiacich s vyhľadávaním spamu, malwaru či phishingu. Napríklad, ak by proxy-server obsahoval funkciu na filtrovanie e-mailov na základe odosielateľov, či iných kritérií. E-maily by podľa týchto kritérií mohol zaraďovať do skupín a podľa toho do ktorej skupiny správa patrí, by bola „označkovaná“ pridaním značky (názvu skupiny, skratky skupiny, atď.) do predmetu správy.

V prípade „značkovania“ e-mailových správ, či iných praktických funkcií je teda zaradenie správy do spamového koša príjemcu maximálne neprijateľné. Presná lokalizácia a následné riešenie tohoto problému je teda veľmi dôležité a boli preto primárnym cieľom praktickej časti tejto práce.

[1] `http://www.avg.com/cz-cs/avg-linux-email-server-edition`
[2] `http://www.vmware.com/products/workstation/overview.html`

5.1 Popis produktu AVG Linux Server Edition

AVG Linux Server Edition je balík programov určený pre nasadenie na serveroch s nainštalovaným operačným systémom Linux alebo FreeBSD. Jeho účelom je predovšetkým antivírusová ochrana e-mailových správ prechádzajúcich serverom, no taktiež ochrana súborového systému servera a jeho ďalších súčastí. Jeho najdôležitejšie komponenty sú nasledovné [3]:

- **avgupd** – aplikácia slúžiaca na sťahovanie a inštaláciu aktualizácií definícií pre antivírusový skener.
- **avgcfgctl** – aplikácia pre správu konfiguračného súboru. Umožňuje zobraziť a upravovať hodnoty jednotlivých nastavení. Taktiež umožňuje export a import všetkých nastavení do/zo súboru.
- **avgtcpd** – je samotný SMTP proxy-server a skener e-mailových správ ktorým sa aj táto práca zaoberá. Aplikácia počúva na určitom preddefinovanom porte a prijíma e-mailové správy prostredníctvom protokolu SMTP. Správy následne preposiela na kontrolu antivírusovému programu a skontrolované správy preposiela ďalej na preddefinovaný poštový server.
- **avgctl** – aplikácia spravuje jednotlivé služby obsiahnuté v balíčku. Má na starosti predovšetkým spúšťanie a zastavovanie týchto služieb (napr. **avgtcpd**).

5.2 Testovacie prostredie

Pre účely testovania bolo použitých niekoľko virtuálnych operačných systémov zapojených do jednej počítačovej siete (viď schéma testovacej počítačovej siete – obr. C.1). Testovacia počítačová sieť bola rozdelená do troch podsietí. Každá podsieť predstavovala jednu doménu (test1.local, test2.local a test3.local) a v nej bol umiestnený jeden poštový server, ktorý v nej spravoval e-mailovú komunikáciu. Aj vďaka virtualizácii bolo možné testovanie relatívne zjednodušiť a výrazne urýchliť. Použité boli nasledovné operačné systémy:

- 2 x **Windows Server 2008** – poštový server (**Microsoft Exchange Server 2007**)
- **Ubuntu Server 10.04 LTS** – poštový server (**Postfix 2.8**), proxy-server (**AVG Linux Server Edition**)
- **Windows 7** – klientský počítač (**Outlook 2007**, **Mozilla Thunderbird 10**)

5.2.1 Zapojenie, nastavenie a činnosť proxy-servera

Proxy-server bol umiestnený do testovacej siete `test1.local` (viď obr. C.1). `MX` záznamy na serveri DNS boli nastavené tak, aby sa všetka e-mailová komunikácia posielala na proxy-server, kde aplikácia **avgtcpd** počúvala na porte `25`. Proxy-server sa teda pre servery v ostatných podsietiach tváril ako poštový server siete `test1.local` a spracovával všetky prichádzajúce e-mailové správy. Skutočný poštový server bol pre ostatné servery skrytý a slúžil iba na prijímanie a následné doručovanie e-mailových správ odoslaných lokálnymi klientmi.

Proxy-server **avgtcpd** prijaté e-mailové správy posielala automaticky na kontrolu antivírusovému programu. Ten v nich vyhľadáva malware a na základe analýzy obsahu správy zisťuje, či správa neobsahuje spam alebo phishing. Výsledky analýzy sa predajú naspäť

proxy-serveru, ktorý na ich základe vykoná potrebné opatrenia na kontrolovanej e-mailovej správe (pridanie upozornenia do predmetu správy, úprava zoznamu adresátov) podľa aktuálnych nastavení programu. Tieto dve aplikácie medzi sebou komunikujú podobne ako aj s poštovým serverom, teda cez protokol `TCP`. Proxy-server má pre tento účel vyhradený ďalší port, na ktorom počúva (viď konfiguračný súbor v prílohe B.1) a na ktorý mu antivírusový program posiela výsledky analýzy prijatých e-mailových správ.

Proxy-server **avgtcpd** robí v e-mailových správach, ktoré nim prechádzajú niekoľko úprav. V každej správe, nezávisle od toho, či obsahuje alebo neobsahuje nebezpečný obsah, pribudnú dve nové SMTP hlavičky (viď hlavičky testovacích e-mailových správ v prílohách A.2.2, A.2.4 a A.2.5). Pridávanie týchto hlavičiek je samozrejme možné v nastaveniach aplikácie vypnúť, no prednastavená hodnota týchto nastavení je, že sa hlavičky do správ pridávajú (viď riadky 10 a 21 v ukážke konfiguračného súboru v prílohe B.1).

Jednou z týchto hlavičiek je `X-Antispam-Avg` a poskytuje informácie o spamovej kontrole. Hlavička obsahuje tri údaje. Prvý údaj má tvar reťazca s hodnotou `YES` alebo `NO` a uvádza, či bola daná správa označená ako spam. Druhý údaj označuje verziu aplikácie vyhľadávajúcu v správe spam, napr. `6.2.1`. Napokon tretí údaj obsahuje číselné skóre, ktoré bolo správe priradené antispamovou kontrolou v tvare `Score: 90`. Môže mať ľubovoľnú celočíselnú hodnotu, ktorej rozmedzie je nastaviteľné v konfiguračnom súbore. Prednastavené rozmedzie je od `1` do `99`. Hodnotu pri ktorej sa správa považuje za spam je možné taktiež meniť v nastaveniach aplikácie. Preddefinovaná hodnota je v tomto prípade `90`.

Druhá hlavička je `X-Antivirus-Avg`. Táto hlavička, ako aj jej názov napovedá, obsahuje informácie o antivírusovej kontrole, ktorá nad danou e-mailovou správou prebehla. Obsahuje tiež tri hodnoty. Prvou z nich je verzia použitého antivírusového programu (napr. `AVG 10.0.1 for Linux/FreeBSD mailserver`). Druhou informáciou je verzia vírusovej databázy a dátum jej vydania (`Virus DB 1517/3812 2011-08-05`). A posledným údajom je informácia o tom, či v správe bola alebo nebola nájdená hrozba. Hlavička obsahuje reťazec `mail clean` v prípade správy bez malwaru a reťazec `mail infected` v prípade infikovanej správy. V druhom prípade táto hlavička obsahuje aj podrobnejšiu informáciu o identifikovanej hrozbe (napr. `Virus identified EICAR_Test`).

Po obdržaní výsledkov antivírusovej a antispamovej kontroly môže server okrem pridania nových hlavičiek do e-mailovej správy, vykonať ešte niekoľko zmien v správe v závislosti od aktuálne platných nastavení proxy servera. Je možné vybrať si z troch akcií, ktoré budú vykonané so správou po identifikovaní hrozby v nej. Server môže túto správu jednoducho zahodiť a oznámiť odosielateľovi jej neúspešné doručenie, môže správu preposlať na inú adresu, alebo nemusí vykonať nič, a správu pustí ďalej. V prípade, že sa správa nezahadzuje, je ešte možné do tejto správy pridať upozornenie na prítomnosť hrozby do jej predmetu. Štandardne sa pridáva pred pôvodný predmet správy reťazec `[VIRUS]` resp. `[SPAM]` alebo `[PHISHING]`. Hodnotu týchto reťazcov je možné si ľubovoľne prispôsobiť v konfiguračnom súbore aplikácie. V prípade preposielania sa ignoruje obsah hlavičky `TO:` a ako adresát sa pri preposielaní správy poštovému serveru prostredníctvom protokolu SMTP použije adresa z konfiguračného súboru. E-mailová správa sa nakoniec prostredníctvom protokolu SMTP prepošle na samotný poštový server (v tomto prípade MS Exchange – port `10 025`). Všetky porty je možné nastaviť v konfiguračnom súbore (viď príloha B.1) pomocou nástroja **avgcfgctl**.

5.2.2 Spôsob testovania

Testovanie prebiehalo posielaním e-mailových správ s rôznym obsahom (škodlivým aj neškodlivým). Správy sa posielali rôzne medzi jednotlivými servermi prostredníctvom protokolov SMTP (Outlook aj Thunderbird) aj MAPI (Outlook), so zapojeným aj odpojeným proxy-serverom a skúmalo sa, či všetky správy dorazia do e-mailových klientov používateľov neporušené. Ako e-mailový klient boli použité programy **Microsoft Outlook 2007** a **Mozilla Thunderbird 10**. E-mailové správy s neškodlivým obsahom boli doručené vždy, nezávisle od použitého klienta, alebo či bol proxy-server zapojený alebo odpojený. Údaje o jednotlivých testovacích správach, ktoré obsahovali škodlivý obsah, sú zhrnuté v tab. D.1.

Neškodlivé správy obsahovali iba neutrálny text, tie škodlivé mali v sebe texty so spamom a iné obsahovali testovací vírus **EICAR**. Ide o malý súbor spustiteľný v prostredí DOS s presne definovaným obsahom. Pre počítač, na ktorom sa spúšťa, nie je ničím škodlivý, no antivírusové programy ho vždy identifikujú ako vírus. Slúži na neškodné testovanie a demonštráciu funkčnosti antivírusovej ochrany. [9]

5.2.3 Zistené problémy

Ako aj z tabuľky D.1 vidno, nie všetky odoslané správy boli do cieľového e-mailového klienta doručené v poriadku. Niektoré končili v spamovom koši aj napriek tomu, že tam nepatrili. Vzhľadom k tomu, že sa to stávalo iba pri zapojenom proxy-serveri a súčasnom použití e-mailového klienta Outlook 2007 na odosielanie aj prijímanie týchto e-mailových správ, je možné vyvodiť, že problém súvisí s určitou vzájomnou nekompatibilitou týchto aplikácií. Tento zistený problém bol následne podkladom ďalšieho skúmania podrobne popísaného v kapitole 5.3.

5.3 Zdroj problému nevalidných e-mailových správ

Z výsledkov testovacích správ zhrnutých v tab. D.1 vidieť, že sa e-mailové správy nedoručujú iba v prípade, že ako zdrojový aj cieľový klient je použitý program **Microsoft Outlook 2007** a testovacie e-maily so škodlivým obsahom prechádzajú cez zapojený proxy-server.

Z hlavičiek týchto e-mailov (viď príloha A.2) odoslaných z klientov Thunderbird a Outlook 2007 vidno, že klient Outlook pridáva do správy svoje vlastné, neštandardné, hlavičky, ktoré medzi hlavičkami správ odoslaných z klienta Thunderbird nie sú. Ide konkrétne o hlavičky `X-Mailer`, `X-CR-HashedPuzzle` a `X-CR-PuzzleID`. Je teda veľmi pravdepodobné, že nedoručovanie infikovaných správ spôsobuje práve niektorá z týchto hlavičiek, keďže sa skúmané správy v žiadnych iných relevantných častiach nelíšia.

Ďalším možným zdrojom problému môžu byť hlavičky pridávané do správy proxy-serverom **avgtcpd** (viď kap. 5.2.1). No pri podrobnejšej analýze vidno, že tieto hlavičky sú obsiahnuté aj v správe z prílohy A.2.2, ktorá bola odoslaná z klienta Thunderbird, a bola úspešne doručená. Z toho teda jasne vyplýva, že tieto hlavičky daný problém nespôsobujú.

Ostávajú teda tri hlavičky pridávané do správy klientom Outlook. Keďže hlavička `X-Mailer` označuje softvér použitý na odosielanie e-mailu, jej hodnota nemá ako ovplyvniť validitu správy a spôsobiť tým jej nedoručenie. Preto ako posledným zdrojom daného problému môžu byť už len hlavičky `X-CR-HashedPuzzle` a `X-CR-PuzzleID`. Po preskúmaní ich účelu bolo zistené, že obsahujú hash rôznych údajov obsiahnutých v správe a slúžia z časti na jej zabezpečenie voči modifikácii počas doručovania, no hlavne majú za úlohu zaručiť, že daná správa obsahujúca tieto hlavičky nie je spam [24]. Ide o tzv. „postmarking“ a je to

dielo firmy Microsoft používané v aplikácii Outlook 2007 [17]. Podrobná špecifikácia týchto hlavičiek je k dispozícii v [17].

5.3.1 Postmarking správ pomocou hlavičiek X-CR-HashedPuzzle a X-CR-PuzzleID

Poštový klient Outlook 2007 obsahuje možnosť pridávať do odosielaných e-mailových správ podpis (hash). Túto funkciu je možné v prípade potreby jednoducho vypnúť (viď príloha C.2). Podpis sa generuje z rôznych údajov obsiahnutých v správe tak, aby bol jedinečný pre každú správu. Pri generovaní podpisu sa preto používa predmet správy, odosielateľ, počet adresátov, zoznam adresátov, dátum a čas odoslania a ID správy generované tiež poštovým klientom [17]. Vygenerovaný podpis Outlook pridáva do e-mailovej správy pomocou hlavičiek `X-CR-HashedPuzzle` a `X-CR-PuzzleID` [24].

Hlavným cieľom tohoto podpisovania je lepšia identifikácia užitočných e-mailových správ medzi spamom a zabránenie náhodnému zaradeniu užitočnej správy medzi spam. Poštový server aj klient adresáta by totiž mal kontrolovať, či je podpis správny a správy so správnym podpisom nepovažovať za spam, prípadne im aspoň výrazne znížiť hodnotenie určujúce či je daná správa spam alebo nie. [24]

Celý tento systém je založený na fakte, že podpis sa generuje pomocou výpočetne náročného algoritmu. Prejavuje sa to miernym oneskorením pri odosielaní e-mailovej správy (rádovo sekundy – viď tab. D.3), ktoré si ale bežný používateľ, ktorý odosiela denne maximálne stovky správ, vôbec nevšimne a žiadnym spôsobom ho to v jeho činnosti neobmedzuje. Naopak spamera, ktorý potrebuje odoslať čo najviac správ v čo najkratšom čase (niekedy aj milióny správ denne), by toto, hoci aj minimálne, oneskorenie pri takomto veľkom počte odosielaných správ výrazne obmedzilo. Spamer si preto nemôže dovoliť generovať týmto algoritmom podpis pre každú jednu odoslanú správu. Preto teda poštový server aj poštový klient adresáta správy môžu predpokladať, že správa s platným podpisom nie je spam. [24]

Je otázne, nakoľko bude toto riešenie efektívne a použiteľné aj v budúcnosti. Pri súčasných trendoch rýchleho zvyšovania výkonu počítačového hardvéru je totiž veľmi pravdepodobné, že spameri budú mať v budúcnosti k dispozícii dostatočne výkonný hardvér na prekonanie tohoto problému. Túto teóriu potvrdzuje aj postup firmy Microsoft, ktorá z poslednej verzie programu Outlook (Outlook 2010) už túto funkciu úplne vypustila (viď sekciu „Mail“ v [19]).

Ďalšou značnou nevýhodou tohoto riešenia je, že je podporované iba produktami firmy Microsoft (Exchange Server, Outlook 2007 [17]). Žiadny ďalší zo všeobecne rozšírených a používaných e-mailových klientov (overené na Mozilla Thunderbird, Claws Mail, Evolution a Opera) nevkladá do odosielaných e-mailových správ tieto hlavičky s podpisom, takže pri filtrovaní spamu nie je možné sa na ne úplne spoliehať, ale je potrebné stále filtrovať spam aj na základe rôznych iných bežne používaných kritérií (vyhľadávanie podozrivých kľúčových slov v texte správy, čierna listina odosielateľov, čierna listina IP adries odosielajúcich SMTP serverov, atď.).

5.4 Zachovanie validity správ

Analyzovaný proxy-server od firmy AVG odhalené infikované e-mailové správy často modifikuje, v závislosti od použitých nastavení. Proxy-server môže infikované správy ignorovať a prepustiť bezo zmeny, môže ich úplne zahodiť, taktiež ich môže automaticky preposielať na inú e-mailovú adresu uvedenú v nastaveniach, alebo môže indikovať prítomnosť hrozby

v správe pridaním varovania do predmetu správy (viď konfiguračný súbor aplikácie **avgtcpd** v prílohe B.1). V posledných dvoch prípadoch ide o zásahy, ktoré spôsobujú, že e-mailové správy odoslané z programu Outlook 2007 opatrené hlavičkami s podpisom popísanými v kap. 5.3.1 sa stávajú nevalidnými. To spôsobuje značné problémy predovšetkým v prípade, keď príjemca správy používa taktiež ako e-mailového klienta program Outlook 2007. Ten totiž validitu týchto správ overuje a nevalidné správy automaticky zaraďuje do spamového koša.

Validitu týchto správ možno zachovať dvomi spôsobmi. Prvý spôsob je implementácia algoritmu na výpočet podpisu priamo v proxy-serveri a následné prepočítavanie podpisov všetkých modifikovaných správ opatrených týmito hlavičkami. Druhá možnosť je hlavičky obsahujúce podpis zo správy jednoducho odstrániť. Obe možné riešenia majú svoje výhody aj nevýhody, preto to najlepšie riešenie môže byť iné pre každý jeden špecifický prípad.

5.4.1 Prepočítavanie podpisu e-mailových správ

Algoritmus výpočtu podpisu je relatívne jednoduchý na implementáciu, no celkom náročný na výpočetný výkon. Vyžaduje totiž značné množstvo procesorového času, čo môže spôsobovať problémy predovšetkým pri použití tohoto algoritmu na serveroch za účelom hromadného výpočtu podpisov pre veľké množstvo e-mailových správ.

Ako vstup algoritmu sú použité rôzne unikátne údaje z podpisovanej e-mailovej správy (viď kap. 2.2.3.1 v [17]). V prvom kroku sú tieto údaje spojené do jedného reťazca z ktorého sú odstránené biele znaky a následne pomocou špeciálne modifikovanej verzie hashovacieho algoritmu *SHA-1* (*Son-Of-SHA-1*) sa získa jeho hash H. Modifikovaná verzia pôvodného algoritmu je použitá predovšetkým kvôli zamedzeniu jednoduchej akcelerácie výpočtu využitím hardvérovej implementácie pôvodného algoritmu SHA-1 [17]. Táto modifikovaná verzia algoritmu SHA-1 je totiž unikátna a neexistuje žiadna jeho bežne dostupná hardvérová implementácia. Navyše využíva operácie so 64-bitovými celočíselnými hodnotami, čím sa komplikuje jeho implementácia na 32-bitovej architektúre. Preto jediným riešením je využitie jeho softvérovej implementácie vyžadujúcej určitý výpočetný výkon procesora, čo je práve hlavným cieľom celého systému podpisovania správ, t. j. „postmarkingu“. Podrobný popis algoritmu Son-Of-SHA-1 je k dispozícii v kap. 2.3 v [17].

Po získaní prvého hashu (H) je v ďalšom kroku potrebné nájsť metódou *brute-force* 16 ($0 < n < 16$) náhodných reťazcov. Každý z týchto reťazcov sa pripojí pred hash H, čím vznikne 16 nových reťazcov z ktorých sa vypočítajú ďalšie hashe G_n ($G_0 - G_{16}$). Pre všetky hashe G_n potom musia platiť nasledovné podmienky:

- Minimálne prvých x bitov každého hashu G_n musí byť 0. x je celé číslo označujúce náročnosť výpočtu. Program Outlook 2007 používa hodnotu 7, no možno použiť ľubovoľné celé kladné číslo. Platí však pravidlo: Čím vyššie číslo, tým väčšia náročnosť výpočtu. Poštové servery a klienti triediace spam by preto mali vyššie čísla, teda náročnejší výpočet podpisu, zohľadňovať pozitívne pri hodnotení týchto správ. [17]

- Posledných 12 bitov každého hashu G_n musí byť rovnakých. Nemusí to byť žiadny konkrétny reťazec, no musí byť totožný vo všetkých vypočítaných hashoch G_n. [17]

Metóda brute-force používaná pri nájdení 16 náhodných reťazcov spĺňajúcich stanovené podmienky spočíva v postupnom skúšaní všetkých možných kombinácií znakov vyhovujúcich týmto podmienkam. Začína sa typicky od najkratších reťazcov (1 – 2 znaky) a postupne sa skúšajú dlhšie, až kým sa nenájde 16 takých, ktoré daným podmienkam vyhovujú. Táto metóda je málo efektívna, keďže skúša všetky možné riešenia problému a proces

vyhľadávania nijak neoptimalizuje. Na riešenie tohoto konkrétneho problému ale žiadne iné možné riešenie nie je známe, čo je maximálne vyhovujúce, keďže možnosť urýchlenia výpočtu podpisu by bola v tomto prípade veľmi nežiadúca [17].

V poslednom kroku algoritmu po nájdení šestnástich reťazcov spĺňajúcich obe spomínané podmienky sa týchto 16 reťazcov spojí do jedného reťazca, pričom sú od seba oddelené medzerou. Výsledný reťazec sa pripojí na začiatok úplne pôvodného reťazca poskladaného z údajov získaných z podpisovanej e-mailovej správy a až tento vzniknutý reťazec sa použije ako hodnota hlavičky `X-CR-HashedPuzzle`. [17]

5.4.2 Test algoritmu na výpočet podpisu e-mailových správ

Algoritmus bol naimplementovaný na základe popisu, ktorý je k dispozícii v [17]. Testovacia aplikácia pozostáva z dvoch hlavných častí. Prvá časť je hashovacia funkcia Son-Of-SHA-1, ktorá je modifikáciou funkcie SHA-1. Keďže algoritmus Son-Of-SHA-1 narozdiel od pôvodného SHA-1 obsahuje aj operácie so 64-bitovými celočíselnými hodnotami, aplikácia bola kvôli zjednodušeniu implementácie vytvorená pre 64-bit OS Windows. Druhá časť aplikácie je samotný algoritmus výpočtu podpisu, t. j. generovania 16 náhodných reťazcov vyhovujúcich stanoveným podmienkam. Algoritmus metódou brute-force postupne skúša všetky možné kombinácie bajtov, až kým nenájde 16 vhodných riešení. Začína sa 1-bajtovými riešeniami a postupne sa počet bajtov zvyšuje. Každý vygenerovaný podpis spolu s dobou trvania jeho výpočtu sa priebežne zapisuje do súboru až sa nakoniec vypočíta priemerná doba výpočtu podpisu a tá sa taktiež pridá do výstupného súboru.

Cieľom testovania bolo vypočítať priemernú dobu výpočtu podpisu pre jednu e-mailovú správu na rôznych počítačových zostavách a potvrdiť tým, že tento algoritmus je naozaj náročný na výpočet a vyžaduje určitý nezanedbateľný výkon a procesorový čas počítača. Test sa vykonával na niekoľkých počítačoch s rôznymi konfiguráciami. Boli medzi nimi výkonnejšie počítače porovnateľné so servermi aj menej výkonné používané typicky bežnými používateľmi. Na každom testovanom počítači bola spustená sada 100 testov. Každý test vypočítal podpis pre jednu náhodne vygenerovanú e-mailovú správu. Zaznamenával sa pri tom čas trvania každého testu a na konci sa vyhodnotil priemerný čas trvania všetkých testov. Zhrnuté výsledky testov sú k dispozícii v tab. D.3 a kompletné výstupy testovacieho programu vrátane vygenerovaných podpisov a doby trvania každého jedného testu možno nájsť na CD nosiči priloženom k práci v adresári `tests_results`.

Vzhľadom k tomu, že sa pri každom testovaní vygenerovala unikátna sada e-mailových správ, nie je možné tieto výsledky medzi jednotlivými počítačmi plnohodnotne porovnávať. To ale vôbec neznamená, že by boli výsledky nepoužiteľné. Vzorka 100 testov je totiž dostačujúca, keďže aj po niekoľkonásobnom spustení sady rôznych 100 testov na tom istom počítači, sa priemerné doby výpočtu jedného podpisu líšili iba v desatinách sekúnd (viď tab. D.2). Ďalej je dôležité, že cieľom testovania bolo iba potvrdiť, že výpočet trvá určitú nezanedbateľnú dobu a reálne overiť jeho približné hodnoty na rôzne výkonných počítačov.

Z výsledkov testov na jednotlivých počítačoch zhrnutých v tab. D.3 vidno, že výpočet podpisu trvá v najhoršom prípade v priemere až necelých 13 sekúnd (test č. 7). V reálnom prípade to teda spôsobí 13-sekundové oneskorenie pri odosielaní e-mailovej správy. To je pre bežného používateľa určite akceptovateľná doba, ktorá ho v jeho práci vo väčšine prípadov skoro vôbec neobmedzí. V prípade, že uvažujeme spamera, ktorý má k dispozícii hoci aj hardvér z testu č. 9 (najlepší spomedzi testovaných), generovanie podpisu ho aj tak výrazne obmedzí. Uvažujme, že je za normálnych podmienok schopný odoslať napríklad 5 e-mailových správ za sekundu, t. j. **432 000** e-mailových správ behom 24 hodín. Ak by

chcel tento spamer odoslané správy podpisovať, musel by na každú v priemere obetovať 4,96 s, čo by znamenalo **17 419** odoslaných správ behom 24 hodín, čo je iba **4%** toho, čo by bol schopný odoslať bez podpisovania.

5.4.3 Odstránenie SMTP hlavičiek e-mailových správ s podpisom

Najjednoduchším a najrýchlejším riešením tohoto problému je odstránenie hlavičiek s podpisom z modifikovaných správ. Na prvý pohľad ide o zúfalý amatérsky zásah, ktorý porušuje pôvodnú štruktúru správy, no v skutočnosti to tak nie je. Podpisovanie e-mailových správ je totiž príliš špecifické a málo rozšírené riešenie. Väčšina poštových serverov totiž tieto podpisy ignoruje a s podpísanými správami zaobchádza úplne rovnako ako s klasickými nepodpísanými. Poštový server Exchange od verzie 2007 podpisy v týchto hlavičkách síce kontroluje, no správy bez podpisu voči tým podpísaným nijako neznevýhodňuje.

U poštových klientov je situácia veľmi podobná. Jediným poštovým klientom podporujúcim takéto podpisovanie správ je Outlook 2007. Ostatní klienti zaobchádzajú s podpísanými správami rovnako ako s nepodpísanými. Jedine Outlook 2007 pri zisťovaní či je správa spam alebo nie prihliada na podpis umiestnený v hlavičke `X-CR-HashedPuzzle` a takýmto správam výrazne znižuje šancu zaradenia medzi spam. To ale neznamená, že správy bez podpisu by boli nejakým spôsobom znevýhodňované. Takéto správy sa proti spamu kontrolujú štandardnými metódami.

Preto vzhľadom k minimálnemu využitiu tohoto podpisu, je teda zachovanie validity e-mailových správ jeho odstránením úplne legitímne riešenie, ktoré nijako neovplyvní ich doručovanie.

5.4.4 Najideálnejšie riešenie v prípade skúmaného produktu

Zo záverov vyplývajúcich z kapitol 5.4.2 a 5.4.3 možno skonštatovať, že v prípade produktu AVG Linux Server Edition v aplikácii **avgtcpd** pracujúcej ako SMTP proxy-server nemá význam podpisy e-mailových správ ošetrených hlavičkami `X-CR-HashedPuzzle` a `X-CR-PuzzleID` prepočítavať. Prepočítavanie podpisu by totiž pri väčšom množstve prechádzajúcich e-mailových správ iba zbytočne zaťažilo server a prinieslo minimálny úžitok.

Rozmýšľať o riešení problému nevalidných správ prepočítavaním podpisu by malo význam iba v prípade, že by sa táto forma ochrany pred spamom viac rozšírila. No vzhľadom k tomu, že sa tak nedeje a už ani samotná firma Microsoft s nasadením tejto metódy v novších verziách svojich produktov nepočíta, je zbytočné uberať výkon proxy-servera a miesto toho je efektívnejšie použiť metódu odstraňovania príslušných hlavičiek popísanú v kap. 5.4.3.

Predovšetkým v prípade viac vyťažených proxy-serverov, ktorými naraz prechádzajú aj stovky e-mailov sa môže nasadenie tohoto algoritmu spôsobovať problémy. Odstraňovaním hlavičiek sa teda šetrí výkon, ktorý by sa musel použiť na prepočítavanie podpisov. Výpočetne náročné prepočítavanie podpisov by totiž mohlo server príliš spomaliť (viď testy v kap. 5.4.2) a obmedziť tak jeho primárnu funkciu, ktorou je antivírusová/antispamová kontrola a preposielanie prijatých e-mailových správ. Taktiež by sa mohlo stať, že by server nestíhal vybavovať všetky požiadavky, čo je maximálne nežiadúce. Odstránenie príslušných hlavičiek pritom zaberie iba minimálny čas aj výkon, takže nie je problém to realizovať aj na viac vyťažených serveroch.

Najideálnejším riešením je ale napriek tomu do aplikácie **avgtcpd** naimplementovať obe navrhované metódy a o nasadení algoritmu na prepočítavanie podpisov nechať rozhodnúť

administrátora servera nastavením príslušnej hodnoty v konfiguračnom súbore. Ďalšia možnosť je, že by o nasadení jednej alebo druhej metódy rozhodovala priamo samotná aplikácia v závislosti od aktuálneho vyťaženia servera na ktorom beží.

Každopádne nasadenie či už jednej, druhej alebo oboch navrhovaných metód umožní produktu AVG Linux Server Edition rozšíriť svoju kompatibilitu medzi produkty spoločnosti Microsoft (Outlook 2007 a Exchange Server). Celkovo sa tým skvalitnia funkcie tohoto produktu a upevní jeho postavenie na trhu medzi ostatnými konkurenčnými produktami.

Kapitola 6

Záver

Hlavným cieľom práce bolo lokalizovať problém s kompatibilitou medzi produktami AVG Linux Server Edition a Microsoft Exchange Server. Túto úlohu sa podarilo v plnej miere splniť. Boli preskúmané všetky možné riešenia nekompatibility, zvážili sa ich výhody aj nevýhody a nakoniec sa navrhlo to najvýhodnejšie. Počas ďalšieho skúmania a testovania týchto dvoch produktov sa dospelo k záveru, že šlo o jediný problém a jeho vyriešením sa odstránia všetky prekážky v kompatibilite týchto dvoch produktov.

Taktiež sa zistilo, že pôvodné zadanie uvažujúce o zneplatňovaní hlavičiek servera Exchange proxy-serverom AVG nebolo úplne správne. Vyšlo totiž najavo, že problém je spôsobovaný výlučne e-mailovým klientom Outlook 2007. K tomuto záveru viedli predovšetkým informácie vyvodené z množstva testovacích e-mailových správ odoslaných z rôznych e-mailových klientov a taktiež informácie získané z rôznych dokumentácií produktov firmy Microsoft.

Ďalším krokom v pokračovaní tejto práce by mala byť implementácia navrhnutého riešenia priamo do proxy-servera produktu AVG Linux Server Edition. Je potrebné naimplementovať samotný algoritmus na výpočet podpisu a skombinovať ho s možnosťou jednoduchého odstraňovania zmieňovaných SMTP hlavičiek. Implementáciou odporúčaného riešenia sa zabezpečí predovšetkým kompatibilita tohoto produktu s produktami firmy Microsoft. Ďalej sa posilní jeho konkurencieschopnosť medzi podobnými produktami iných firiem a výrazne sa rozšíria možnosti nasadenia tohoto produktu v praxi, keďže produkty určené pre e-mailovú komunikáciu od firmy Microsoft používa značné množstvo používateľov. Táto práca teda v konečnom dôsledku prispeje k rozšíreniu a skvalitneniu tohoto produktu od firmy AVG.

Projekt by v ďalšej fáze mohol pokračovať rozšírenejším testovaním zameraným na ďalšie často používané poštové servery. Taktiež by sa mali kompletne otestovať klientské aplikácie slúžiace na prijímanie a odosielanie elektronickej pošty. Minimálne tie, ktoré sú medzi používateľmi najviac rozšírené.

Literatura

[1] Adámek, M.: *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu.* Grada Publishing a.s., 2009, ISBN 978-80-247-2638-0.

[2] Andrés, S.; Kenyon, B.: *Security Sage's Guide to Hardening the Network Infrastructure.* Syngress, 2004, ISBN 978-1-931-83601-2.

[3] AVG Technologies: Anti-Virus for Linux/FreeBSD [online]. `http://aa-download.avg.com/filedir/doc/AVG_Anti-Virus_for_Linux/avg_alb_uma_en_2011_1.pdf`, 2011 [cit. 2012-04-25].

[4] Bauer, M. D.: *Linux Server Security.* O'Reilly Media, Inc., 2005, ISBN 978-0-596-00670-9.

[5] Dent, K. D.: *Postfix: kompletní průvodce.* Grada Publishing a.s., 2005, ISBN 978-80-247-1029-7.

[6] Donahue, G.: *Network Warrior.* O'Reilly Media, Inc., 2011, ISBN 978-1-449-30935-0.

[7] Dostálek, L.; Vohnoutová, M.: *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Computer Press, 2006, ISBN 978-8-025-10828-4.

[8] Erbschloe, M.: *Trojans, worms, and spyware: a computer security professional's guide to malicious code.* Butterworth-Heinemann, 2005, ISBN 978-0-750-67848-3.

[9] European Expert Group for IT-Security: Anti-Malware Testfile [online]. `http://www.eicar.org/anti_virus_test_file.htm`, 2006 [cit. 2012-05-08].

[10] Éric Filiol: *Computer viruses: from theory to applications.* Birkhäuser, 2005, ISBN 978-2-287-23939-7.

[11] GFI Software: Why one virus engine is not enough [online]. `http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf`, 2011 [cit. 2012-04-03].

[12] Jakobsson, M.; Myers, S.: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* John Wiley & Sons, 2006, ISBN 978-0-470-08609-4.

[13] Klensin, J.: Simple Mail Transfer Protocol, Internet RFC-5321 [online]. `http://www.ietf.org/rfc/rfc5321.txt`, Říjen 2008 [cit. 2012-03-22].

[14] Klensin, J.; Freed, N.; Rose, M.; aj.: SMTP Service Extensions, Internet RFC-1869 [online]. `http://www.ietf.org/rfc/rfc1869.txt`, Listopad 1995 [cit. 2012-03-20].

[15] Lucas, M.: *PGP and GPG: Email for the Practical Paranoid*. No Starch Press, 2006, ISBN 978-1-593-27071-1.

[16] McKeag, L.: Securing SMTP mail servers [online]. `http://howto.techworld.com/security/408/securing-smtp-mail-servers/`, Březen 2004 [cit. 2012-03-19].

[17] Microsoft Corporation: E-Mail Postmark Validation Algorithm [online]. `http://download.microsoft.com/download/5/D/D/5DD33FDF-91F5-496D-9884-0A0B0EE698BB/[MS-OXPSVAL].pdf`, 2012 [cit. 2012-04-15].

[18] Microsoft Corporation: Exchange Server Protocols System Overview [online]. `http://download.microsoft.com/download/5/D/D/5DD33FDF-91F5-496D-9884-0A0B0EE698BB/[MS-OXPROTO].pdf`, 2012 [cit. 2012-05-03].

[19] Microsoft Corporation: Discontinued features and modified functionality in Outlook 2010 [online]. `http://office.microsoft.com/en-us/outlook-help/discontinued-features-and-modified-functionality-in-outlook-2010-HA010354944.aspx`, 2012 [cit. 2012-05-08].

[20] Mockapetris, P.: Domain Names – Concepts and facilities, Internet RFC-1034 [online]. `http://www.ietf.org/rfc/rfc1034.txt`, Listopad 1987 [cit. 2012-03-13].

[21] Postel, J. B.: Simple Mail Transfer Protocol, Internet RFC-821 [online]. `http://www.ietf.org/rfc/rfc821.txt`, Srpen 1982 [cit. 2011-11-25].

[22] Puri, R.: Bots &; Botnet: An Overview [online]. `http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299`, Srpen 2003 [cit. 2012-03-29].

[23] Rash, W.: Going the anti-virus distance. *InfoWorld*, ročník 25, č. 24, 2003: s. 32–33, ISSN 0199-6649.

[24] Redmond, T.: *Microsoft Exchange Server 2007 with SP1: Tony Redmond's Guide to Successful Implementation*. Digital Press, 2008, ISBN 978-1-555-58355-2.

[25] Salomon, D.: *Elements of Computer Security*. Springer, 2010, ISBN 978-0-857-29005-2.

[26] Schryen, G.: *Anti-spam measures: analysis and design*. Springer, 2007, ISBN 978-3-540-71748-5.

[27] Tanenbaum, A. S.: *Computer Networks*. Prentice Hall, 2002, ISBN 0-13-066102-3.

[28] TechRepublic: *IT Security Survival Guide*. CNET Networks, Inc., 2004, ISBN 978-1-932-50937-3.

Příloha A

Ukážky e-mailových správ

A.1 Podvodná správa obsahujúca phishing

From: <jm.pointet@esiee.fr>
Date: Fri, Mar 23, 2012 at 20:07
Subject: United Parcel Service (UPS)

Good Day

After much attempts to reach you on phone, I˜deemed it necessary and urgent to contact you via your e-mail and to notify you finally about your outstanding compensation payment.

During our last annual calculation of your banking activities we have realized that you are eligible to receive a compensation payment of $2,811,041.00 USD.

This compensation is being made to all of you who have suffered loss as a result of fraud, accident or illness. For more info, contact the assigned UPS agent for the delivery of your cashier check.

United Parcel Service (UPS)
Contact Name: Mr. paul walter
Tel: +2348053433220
E-mail: upsshippment.ng11@hotmail.co.uk

Please take note that you will pay a shipping/handling fee of $95.00 USD to UPS.

Thanks for your patience.

Paul Walter
Programme Manager
United Nations Human Settlements Programme.
E-mail:upsshippment.ng11@hotmail.co.uk

A.2 Hlavičky testovacích e-mailových správ

A.2.1 Doručená, neinfikovaná e-mailová správa odoslaná z klienta Thunderbird bez zapojeného SMTP proxy-servera

```
Received: from [192.168.1.254] (192.168.1.254) by TEST1.test1.local
 (192.168.1.254) with Microsoft SMTP Server (TLS) id 14.0.639.21; Wed, 15 Feb
 2012 11:04:44 +0100
Message-ID: <4F3B833A.5070508@test1.local>
Date: Wed, 15 Feb 2012 11:04:42 +0100
From: Peter Szabo #1 <test@test1.local>
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:10.0.1) Gecko/20120208
 Thunderbird/10.0.1
MIME-Version: 1.0
To: <test@test2.local>
Subject: MSG #1 --> #2
References: <4F3B811A.1040108@test1.local>
In-Reply-To: <4F3B811A.1040108@test1.local>
Content-Type: multipart/alternative;
 boundary="------------000008080408010601010507"
Return-Path: test@test1.local
```

A.2.2 Doručená, infikovaná e-mailová správa odoslaná z klienta Thunderbird so zapojeným SMTP proxy-serverom

```
Received: from avg (192.168.1.110) by TEST1.test1.local (192.168.1.254) with
 Microsoft SMTP Server id 14.0.639.21; Fri, 4 May 2012 10:43:22 +0200
Received: from [192.168.1.254] (192.168.1.254) by TEST2.test2.local
 (192.168.2.254) with Microsoft SMTP Server (TLS) id 14.0.639.21; Fri, 4 May
 2012 10:43:21 +0200
Message-ID: <4FA396A9.3060905@test2.local>
Date: Fri, 4 May 2012 10:43:21 +0200
From: Peter Szabo #2 <test@test2.local>
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:10.0.1) Gecko/20120208
 Thunderbird/10.0.1
To: <test@test1.local>
Subject: [VIRUS] EICAR test from Thunderbird
Content-Type: multipart/mixed;
boundary="------------020305010802010400030806"
Return-Path: test@test2.local
X-Antispam-Avg: : NO; 6.2.1 Score: 90
X-Antivirus-Avg: : AVG 10.0.1 for Linux/FreeBSD mailserver; Virus DB 1517/3812
 2011-08-05; mail infected Virus identified EICAR_Test
X-MS-Exchange-Organization-AuthSource: TEST1.test1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
```

A.2.3 Doručená, infikovaná e-mailová správa odoslaná z klienta Outlook bez zapojeného SMTP proxy-servera

```
Received: from TEST1.test1.local (192.168.1.254) by TEST2.test2.local
 (192.168.2.254) with Microsoft SMTP Server id 14.0.639.21; Fri, 4 May 2012
 11:25:35 +0200
Received: from TEST1 (192.168.1.254) by TEST1.test1.local (192.168.1.254) with
 Microsoft SMTP Server (TLS) id 14.0.639.21; Fri, 4 May 2012 11:25:34 +0200
From: Peter Szabo #1 - Outlook <test@test1.local>
To: <test@test2.local>
Subject: Outlook EICAR no-proxy test
Date: Fri, 4 May 2012 11:25:34 +0200
Message-ID: <001d01cd29d7$db9a1c70$92ce5550$@local>
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_001E_01CD29E8.9F22EC70"
X-Mailer: Microsoft Office Outlook 12.0
Content-Language: en-us
Thread-Index: Ac0p19kN6jm1f/9aRISvLKGDEk++CA==
x-cr-hashedpuzzle: AaWz AawW A31N CaL7 DBs4 DvMY EkJd HICr HWwC Ho5T Hyks ILV6
 IP6k JijY J+mX K6+4;1;dABlAHMAdABAAHQAZQBzAHQAMgAuAGwAbwBjAGEAbAA=;Sosha1_v1;7;
 {DB46C5C2-46DA-436B-9EA2-C93E72CC51F3};
 dABlAHMAdABAAHQAZQBzAHQAMQAuAGwAbwBjAGEAbAA=;Fri, 04 May 2012 09:25:30 GMT;
 TwB1AHQAbABvAG8AawAgAEUASQBDAEEAUgAgAG4AbwAtAHAAcgBvAHgAeQAgAHQAZQBzAHQA
x-cr-puzzleid: {DB46C5C2-46DA-436B-9EA2-C93E72CC51F3}
Return-Path: test@test1.local
X-MS-Exchange-Organization-AuthSource: TEST2.test2.local
X-MS-Exchange-Organization-AuthAs: Anonymous
```

A.2.4 Doručená, neinfikovaná e-mailová správa odoslaná z klienta Outlook so zapojeným SMTP proxy-serverom

```
Received: from avg (192.168.1.110) by TEST1.test1.local (192.168.1.254) with
 Microsoft SMTP Server id 14.0.639.21; Tue, 28 Feb 2012 12:47:01 +0100
Received: from TEST1 (192.168.1.254) by TEST2.test2.local (192.168.2.254) with
 Microsoft SMTP Server (TLS) id 14.0.639.21; Tue, 28 Feb 2012 12:40:54 +0100
From: Peter Szabo #2 - Outlook <test@test2.local>
To: <test@test1.local>
Subject: test
Date: Tue, 28 Feb 2012 12:40:53 +0100
Message-ID: <006101ccf60d$d45108f0$7cf31ad0$@local>
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0062_01CCF616.361570F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: Acz2Dc41KJV00kVVRhmZ+dYJpOa8WQ==
Content-Language: en-us
x-cr-hashedpuzzle: ANNh A6GE BItF Ci1c C1GW DOiY DYSP D6qI FDRe IFep JHDz JMIk
 KBHY KHaj Knj7 K8bJ;1;dABlAHMAdABAAHQAZQBzAHQAMQAuAGwAbwBjAGEAbAA=;Sosha1_v1;7;
 {0104650D-AA76-403C-9C64-5AA48331D155};
 dABlAHMAdABAAHQAZQBzAHQAMgAuAGwAbwBjAGEAbAA=;Tue, 28 Feb 2012 11:40:44 GMT;
```

```
 dABlAHMAdAA=
x-cr-puzzleid: {0104650D-AA76-403C-9C64-5AA48331D155}
Return-Path: test@test2.local
X-Antispam-Avg: : NO; 6.2.1 Score: 2
X-Antivirus-Avg: : AVG 10.0.1 for Linux/FreeBSD mailserver; Virus DB 1517/3812
 2011-08-05; mail clean;
X-MS-Exchange-Organization-AuthSource: TEST1.test1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
MIME-Version: 1.0
```

A.2.5 Nedoručená, infikovaná e-mailová správa odoslaná z klienta Outlook so zapojeným SMTP proxy-serverom

```
Received: from avg (192.168.1.110) by TEST1.test1.local (192.168.1.254) with
 Microsoft SMTP Server id 14.0.639.21; Tue, 28 Feb 2012 11:06:27 +0100
Received: from TEST1 (192.168.1.254) by TEST2.test2.local (192.168.2.254) with
 Microsoft SMTP Server (TLS) id 14.0.639.21; Tue, 28 Feb 2012 11:06:25 +0100
From: Peter Szabo #2 - Outlook <test@test2.local>
To: <test@test1.local>
Subject: [VIRUS] puzzle test with eicar
Date: Tue, 28 Feb 2012 11:06:25 +0100
Message-ID: <001801ccf600$a1359ce0$e3a0d6a0$@local>
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0019_01CCF609.02FA04E0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: Acz2AJ1ls2a/V3QqQOi6Kk658rCS2w==
Content-Language: en-us
x-cr-hashedpuzzle: Aexe Axmh BwXf ChiV DAB6 Dh/S FJF6 GVTo HELT Jb/b J1Tj J+lS
 KmEz LZDP LuBB LzpX;1;dABlAHMAdABAAHQAZQBzAHQAMQAuAGwAbwBjAGEAbAA=;Sosha1_v1;7;
 {89DE25B1-AB44-4CD8-967E-494C3C1CA833};
 dABlAHMAdABAAHQAZQBzAHQAMgAuAGwAbwBjAGEAbAA=;Tue, 28 Feb 2012 10:06:18 GMT;
 cAB1AHoAegBsAGUAIAB0AGUAcwB0ACAAdwBpAHQAaAAgAGUAaQBjAGEAcgA=
x-cr-puzzleid: {89DE25B1-AB44-4CD8-967E-494C3C1CA833}
Return-Path: test@test2.local
X-Antispam-Avg: : NO; 6.2.1 Score: 2
X-Antivirus-Avg: : AVG 10.0.1 for Linux/FreeBSD mailserver; Virus DB1517/3812
 2011-08-05; mail infected Virus identified EICAR_Test
X-MS-Exchange-Organization-AuthSource: TEST1.test1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
```

Příloha B

Konfiguračné súbory

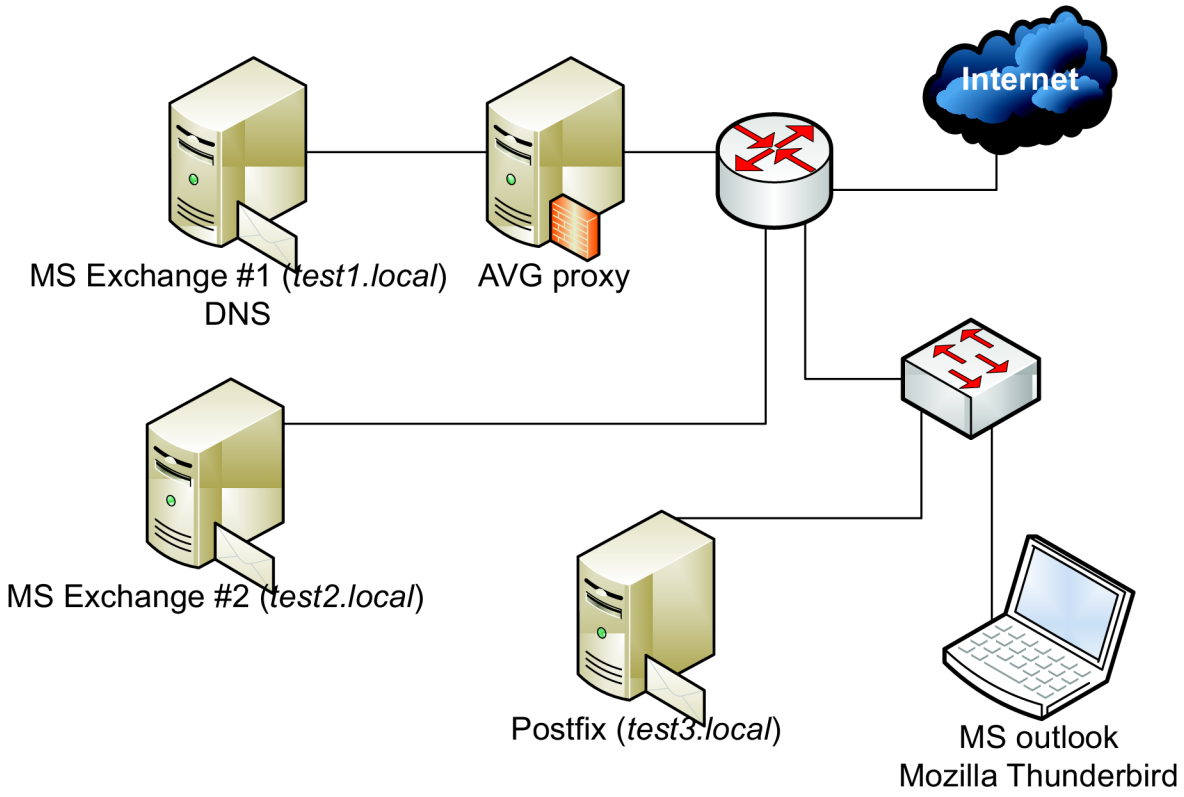
B.1 Ukážka časti konfiguračného súboru programu avgtcpd

```
1.  Default.tcpd.avg.address=127.0.0.1 //adresa na ktorej aplikácia počúva pre
                                       komunikáciu s˜antivírusom prostredníctvom
                                       AVG protokolu
2.  Default.tcpd.avg.enabled=true
3.  Default.tcpd.avg.ports=|54322| //port na ktorom aplikácia počúva pre
                                   komunikáciu prostredníctvom AVG protokolu
4.  Default.tcpd.rules.spam.action=0 //0 - žiadna akcia, 1 - e-mail sa zahodí,
                                       2 - e-mail sa prepošle na adresu
                                       nastavenú v˜"bounce_addr"
5.  Default.tcpd.rules.spam.bounce_addr= //e-mailová adresa
6.  Default.tcpd.rules.phishing.action=0 //rovnako ako v˜prípade "spam.action"
7.  Default.tcpd.rules.phishing.bounce_addr= //e-mailová adresa
8.  Default.tcpd.rules.virus.action=0 //rovnako ako v˜prípade "spam.action"
9.  Default.tcpd.rules.virus.bounce_addr= //e-mailová adresa
10. Default.tcpd.scan.header.enabled=true //povoľuje pridávanie hlavičky
                                          X-Antivirus-Avg do správy
11. Default.tcpd.scan.subj_prefix=[VIRUS] //upozornenie v˜predmete správy
12. Default.tcpd.smtp.address=192.168.1.100//adresa na ktorej aplikácia počúva
                                            pre komunikáciu prostredníctvom
                                            protokolu SMTP
13. Default.tcpd.smtp.client_address=192.168.1.254 //adresa poštového servera
14. Default.tcpd.smtp.client_port=10025 //port na ktorom poštový server počúva
15. Default.tcpd.smtp.enabled=true
17. Default.tcpd.smtp.ports=|54321|25| //porty na ktorých počúva proxy server
18. Default.tcpd.smtp.queue_max=20
20. Default.tcpd.spam.enabled=true
21. Default.tcpd.spam.header.enabled=true //povoľuje pridávanie hlavičky
                                          X-Antispam-Avg do správy
22. Default.tcpd.spam.phish_subj_prefix=[PHISHING] //upozornenie v˜predmete
                                                   správy
23. Default.tcpd.spam.spamscore_level=90 //hranica skóre pri ktorej sa správa
                                         považuje za spam
24. Default.tcpd.spam.subj_prefix=[SPAM] //upozornenie v˜predmete správy
```

Příloha C

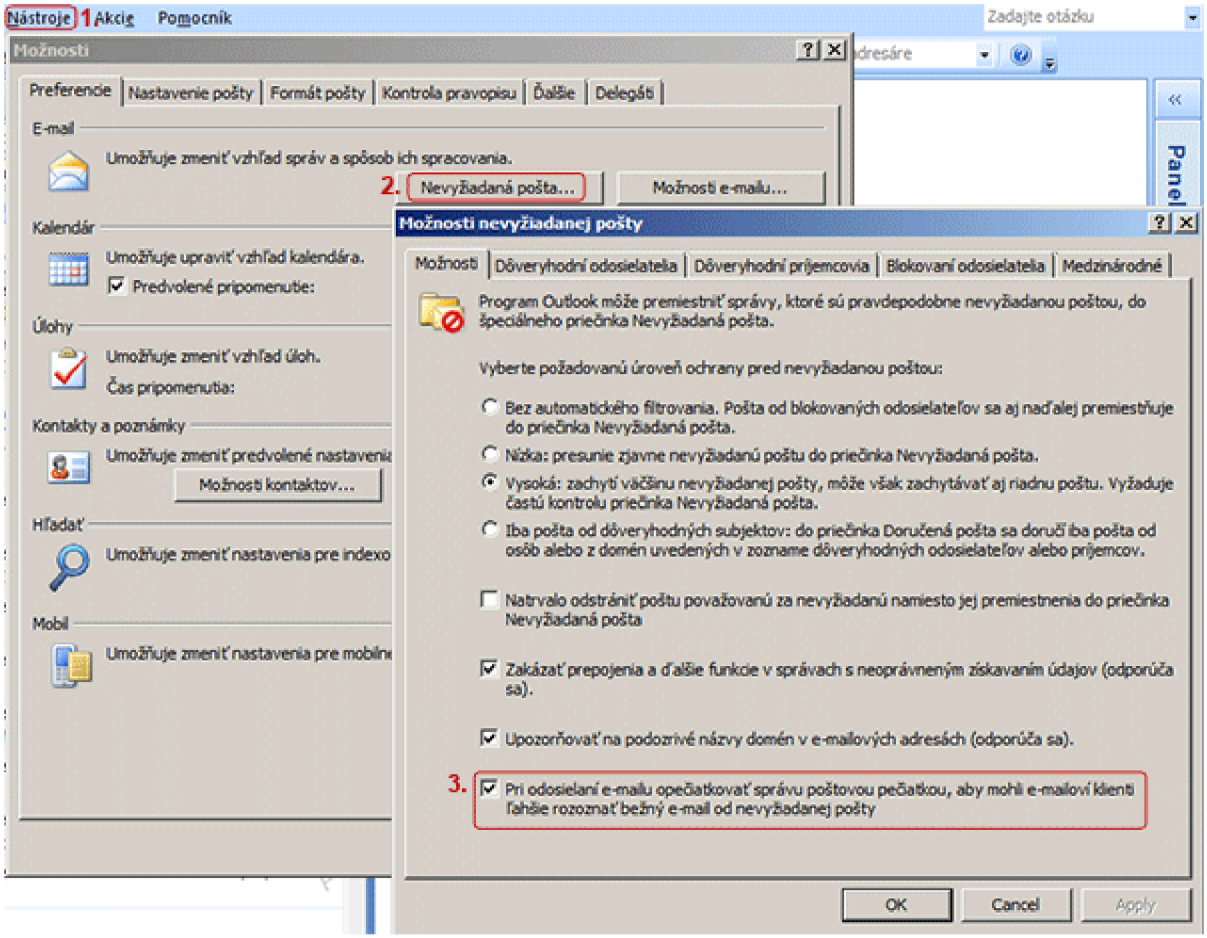
Obrázky

C.1 Schéma testovacej počítačovej siete



Obrázek C.1: Schéma testovacej počítačovej siete

C.2 Zapnutie generovania podpisov v odosielaných správach v aplikácii Outlook 2007



Obrázek C.2: Snímka dialógového okna umožňujúce zapnutie generovania podpisov v odosielaných správach v aplikácii Outlook 2007

Příloha D

Tabuľky

D.1 Zhrnutie testovacích e-mailov s infikovaným obsahom

Zdrojový server	**Cieľový server**	**Zdrojový klient**	**Cieľový klient**	**Použitý protokol**	**Zapojený proxy-server**	**Správne doručenie správy**
Exchange	Exchange	Outlook	Outlook	SMTP	✓	✗
Exchange	Exchange	Outlook	Outlook	MAPI	✓	✗
Exchange	Exchange	Outlook	Thunderbird	SMTP	✓	✓
Exchange	Exchange	Outlook	Thunderbird	MAPI	✓	✓
Exchange	Exchange	Thunderbird	Outlook	SMTP	✓	✓
Exchange	Exchange	Thunderbird	Thunderbird	SMTP	✓	✓
Exchange	Postfix	Outlook	Outlook	SMTP	✓	✗
Exchange	Postfix	Outlook	Outlook	MAPI	✓	✗
Exchange	Postfix	Outlook	Thunderbird	SMTP	✓	✓
Exchange	Postfix	Outlook	Thunderbird	MAPI	✓	✓
Exchange	Postfix	Thunderbird	Outlook	SMTP	✓	✓
Exchange	Postfix	Thunderbird	Thunderbird	SMTP	✓	✓
Postfix	Exchange	Outlook	Outlook	SMTP	✓	✗
Postfix	Exchange	Outlook	Thunderbird	SMTP	✓	✓
Postfix	Exchange	Thunderbird	Outlook	SMTP	✓	✓
Postfix	Exchange	Thunderbird	Thunderbird	SMTP	✓	✓
Exchange	Exchange	Outlook	Outlook	SMTP	✗	✓
Exchange	Exchange	Outlook	Outlook	MAPI	✗	✓
Exchange	Postfix	Outlook	Outlook	SMTP	✗	✓
Exchange	Postfix	Outlook	Outlook	MAPI	✗	✓
Postfix	Exchange	Outlook	Outlook	SMTP	✗	✓

Tabulka D.1: Zhrnutie testovacích e-mailov s infikovaným obsahom

D.2 Výsledky testov generovania podpisu e-mailových správ

Č. testu	Priemerná doba výpočtu
1	**8,25** sekúnd
2	**8,02** sekúnd
3	**8,67** sekúnd
4	**8,35** sekúnd
5	**8,39** sekúnd

Tabulka D.2: Priemerná doba generovania jedného podpisu pri prevedení niekoľkých sád testov na rovnakom počítači (Intel Core 2 Duo T5870 – 2,00 GHz, 4 GB RAM)

Č. testu	Konfigurácia počítača	Priemerná doba výpočtu
5	Intel Core 2 Duo T5870 – 2,00 GHz, 4 GB RAM	**8,39** sekúnd
6	Intel Core 2 Duo P7370 – 2,00 GHz, 4 GB RAM	**7,70** sekúnd
7	AMD Turion X2 Dual-Core RM-74 – 2,20 GHz, 4 GB RAM	**12,88** sekúnd
8	AMD Athlon X2 QL-65 – 2,10 GHz, 4 GB RAM	**12,09** sekúnd
9	Intel Core i5-560M – 2,67 GHz, 8 GB RAM	**4,96** sekúnd
10	Intel Core i7-2720QM – 2,20 GHz, 6 GB RAM	**5,57** sekúnd
11	Intel Core i7-2630QM – 2,00 GHz, 6 GB RAM	**6,11** sekúnd
12	Intel Core 2 Quad Q6600 – 2,40GHz, 8 GB RAM	**9,63** sekúnd

Tabulka D.3: Priemerná doba generovania jedného podpisu pri prevedení 100 testov na rôznych počítačoch

Příloha E

Obsah CD

CD nosič priložený k práci obsahuje nasledovné adresáre:

- `test_results` – Súbory s výsledkami testov algoritmu počítajúceho podpis e-mailových správ
- `test_app` – Zdrojové súbory testovacej aplikácie
- `thesis` – Technická správa vo formáte PDF
- `thesis_src` – Zdrojové súbory technickej správy