

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství



Bakalářská práce

**Konfigurace linuxového poštovního serveru
s implementací proti SPAMu**

David Rigl

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

David Rígl

Informatika

Název práce

Konfigurace linuxového poštovního serveru s implementací ochrany proti SPAMu

Název anglicky

Linux mail server configuration with SPAM protection implementation

Cíle práce

Cílem této práce je návrh a konfigurace poštovního serveru s pokročilou ochranou proti SPAMu. Server bude následně nakonfigurován a otestován v lokálním provozu u AČR.

Metodika

V teoretické části budou vysvětleny technologie, na kterých emailový server funguje a jsou s ním spojené, základní informace o OS, základy emailu, antiSPAM ochrana a metody, které budou v projektu použity.

V praktické části bude provedena implementace postfixu, dovecotu, spamassassina a bezpečnostních metod, které na základě doporučení, zkušeností s provozem a administrací emailového serveru u AČR bude potřeba implementovat pro bezpečnější server a jeho komunikaci. V bakalářské práci nebude chybět případné řešení chybových stavů, kompletní postup práce včetně příkazů a ukázek o funkčnosti konfigurací a výsledky ze závěrečného otestování serveru.

Doporučený rozsah práce

30-40 stran

Klíčová slova

email, server, SPAM, Linux, konfigurace, CentOS, Postfix, Dovecot, SpamAssassin

Doporučené zdroje informací

KOETTER, Patrick. Postfix – Provozujeme poštovní server v Linuxu. Vyd.1. Brno: COMPUTER PRESS, 2006. ISBN 80-251-1020-6.

RENATO CARLOS DE OLIVEIRA a ADRIANA DE OLIVEIRA. Chroot your Red Hat/Centos 8 – Extreme Hardening., 2020. ISBN 979-8556889002.

RUSENKO, David, Carl TAYLOR, Alistair MCDONALD, Patrick BEN KOETTER a Magnus BACK. Linux Email: Set Up and Run a Small Office Email Server. 2005. ISBN 978-1904811374.

SMYTH, Neil. CentOS 8 Essentials: Learn to install, administer and deploy CentOS 8 systems. 2019. ISBN 978-1951442095.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 1. 3. 2022

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 7. 3. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 07. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Konfigurace linuxového poštovního serveru s implementací ochrany proti SPAMu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.03.2022

Poděkování

Rád bych touto cestou poděkoval panu Ing. Marku Píckovi, Ph.D. za velmi vstřícný přístup, konzultace a odborné rady při tvorbě této bakalářské práce.

Konfigurace linuxového poštovního serveru s implementací ochrany proti SPAMu.

Abstrakt

Cílem této práce bylo vytvořit emailový server zaměřený na ochranu proti spamu. Dále se pomocí tohoto projektu lze přesvědčit, že zvolené služby a metody jsou vhodné pro konfiguraci a následné použití v armádním prostředí, pro které je tento projekt podstatným testem. Na serveru jsou použity metody a funkce, které jsou již nyní u AČR používány, avšak aplikovány na novější systém, a navíc přidány i další potřebné funkce pro ochranu. Server slouží pro jednu doménu, která může komunikovat s vnějším světem.

Práce je rozdělena na část teoretickou, kde jsou popsány a vysvětleny technologie, bezpečnostní metody a služby, na kterých a se kterými emailový server pracuje. Dále jsou zde rozebrány jednotlivé typy útoků a mailových podvodů.

V praktické části je provedeno základní nastavení virtuálního serveru, implementace Postfixu, Dovecotu a SpamAssassina. Dále proběhla konfigurace zvolených bezpečnostních metod a dalších potřebných částí. Nechybí ani podrobný postup práce s příkazy. Vše bylo následně otestováno a do projektu přidány obrázky potvrzující funkčnost služeb a metod.

Klíčová slova: Linux, server, CentOS, Postfix, Dovecot, SpamAssassin, OpenDKIM, DMARC, SPF, IMAP, SMTP

Linux mail server configuration with SPAM protection implementation.

Abstract

The aim of this work was to create an email server focused on spam protection. Furthermore, through this project it can be verified that the choice of the services and methods chosen are suitable for configuration and subsequent use in a military environment, for which this project is an essential test. The server uses methods and features that are already in use in the Army of the Czech Republic, but applied to a newer system, plus additional needed features for protection. The server serves a single domain that can communicate with the outside world.

The thesis is divided into a theoretical part where the technologies, security methods and services on which and with which the email server works are described and explained. It also discusses the different types of attacks and mail fraud.

In the practical part, the basic setup of the virtual server, the implementation of Postfix, Dovecot and SpamAssassin are covered. Furthermore, the configuration of the chosen security methods was performed and other necessary parts. There is a detailed procedure for working with commands. Everything has been tested and images have been added to the project to confirm the functionality of the services and methods.

Keywords: Linux, server, CentOS, Postfix, Dovecot, SpamAssassin, OpenDKIM, DMARC, SPF, IMAP, SMTP

Obsah

1 Úvod	10
2 Cíl práce	11
3 Metodika	11
4 Teoretická východiska	12
4.1 Základní informace	12
4.2 Bezpečnost	13
4.2.1 Bezpečnostní metody	13
4.2.2 Spam filtr	15
4.2.3 Bezpečnostní rizika emailu	16
4.2.4 Necurs botnet – bezpečnostní incident	20
4.3 Emailové protokoly	20
4.4 Poštovní služby	21
4.4.1 Agent pro příjem pošty	21
4.4.2 Agent pro přenos pošty	21
5 Vlastní práce	23
5.1 Úvod	23
5.2 Požadavky	23
5.3 Postup konfigurace	24
5.3.1 Nastavení prostředí před konfigurací systému	24
5.3.2 Postfix	25
5.3.3 Firewall	26
5.3.4 Instalace TLS certifikátu a Apache serveru	27
5.3.5 Dovecot	29
5.3.6 Konfigurace šifrování SSL/TLS	30
5.3.7 Vytvoření testovacích uživatelů	31
5.3.8 SPF	32
5.3.9 DKIM	33
5.3.10 Privátní a veřejný klíč	34
5.3.11 Propojení Postfix a OpenDKIM	35
5.3.12 DMARC	36
5.3.13 SpamAssassin	36
5.3.14 Nastavení a použití blacklist a whitelist	37
5.4 Otestování služeb a serveru	38
6 Výsledky a diskuse	40
6.1 Výsledek práce	40
6.2 Diskuse	40

7 Závěr.....	41
8 Seznam použitých zdrojů	42

Seznam obrázků

Obrázek 1 – Komunikace emailových agentů	12
Obrázek 2 – Nastavení MX a A záznamu.....	25
Obrázek 3 – Nastavení reverzního záznamu.....	25
Obrázek 4 – Zobrazení povolených portů po nastavení	26
Obrázek 5 – Výpis konfigurace souboru master.cf.....	28
Obrázek 6 – Vygenerovaný platný certifikát pro naši doménu	29
Obrázek 7 – Úprava konfiguračního souboru SSL/TLS.....	31
Obrázek 8 – SPF záznam v DNS	32
Obrázek 9 – Test odeslaného emailu včetně potvrzení o funkčnosti SPF (z emailového klienta)	32
Obrázek 10 – Kontrola funkčnosti SPF z webové stránky	33
Obrázek 11 – Upravený konfigurační Open DKIM soubor	33
Obrázek 12 – Veřejný klíč zobrazený v záznamu DNS	35
Obrázek 13 – Nastavení DMARC záznamu	36
Obrázek 14 – Ověření funkčního DMARC	36
Obrázek 15 – Nastavení skóre pro blokaci	37
Obrázek 16 – Doručení email od Mailer Deamon o blokaci zprávy z domény @seznam.cz ..38	
Obrázek 17 – Log ze serveru o blokaci emailu z domény @seznam.cz.....	38
Obrázek 18 – Kontrola SpamAssassina, SPF a DKIM.....	38
Obrázek 19 – Potvrzení funkčnosti SPF, DKIM a DMARC z emailového klienta.....	39
Obrázek 20 – Potvrzení funkčnosti odesílání a přijímání pošty	39

1 Úvod

Emailovou komunikaci dnes využívá snad každá společnost či firma. Z toho vyplývá, že v moderním elektronickém světě se bez této služby těžko obejdete. Emailový server jako takový lze provozovat na svém hardware, nebo využít externí firmy, které nabízí virtuální prostředí, na kterém lze emailový server také provozovat. Obě strany mají své pozitivní i negativní stránky a nejvíce záleží, jaký účel má emailový server plnit a jak schopní lidé server budou administrovat.

Díky rozšíření emailové komunikace po celém světě a využívání této služby je potřeba dbát na bezpečnost, jelikož enormně rostou nejen spamové útoky a jejich propracovanost, ale i mnoho dalších hrozeb, které s sebou nesou velké nepříjemnosti v podobě napadení serveru, poškození techniky, zneužití uživatelských dat, vydírání a plno dalších. Pro zamezení a co možná největší ochranu celé emailové sféry se postupně rozšiřují různé druhy a metody ochrany v podobě antivirů, bezpečnostních konfigurací emailového serveru, spam filtrů, veřejných blacklistů apod., které je možné za určitých podmínek a zkušeností implementovat a tím předejít nebezpečí. Nesmíme ale zapomenout na standardně nejslabší článek této struktury a tím je nezkušený uživatel. I ta nejlepší ochrana před hrozbami emailů nezabrání chybným krokům a rozhodnutím nezkušeného uživatele. Jedinou vhodnou metodou, jak zabránit tomuto problému je opakované a kvalitní proškolení uživatelů.

Existuje mnoho způsobů, jak si zajistit funkční emailový server, některé jsou jednoduché, ale velmi drahé, některé složité, finančně však téměř nenákladné. Tento projekt jsem se rozhodl udělat díky mému zaměstnání, kde po mně bylo vyžadováno splnit zadaný úkol v podobě nového emailového serveru, respektive vytvoření testovacího emailového serveru, který při splnění všech podmínek a bezpečnosti bude nasazen jako dočasný primární server.

2 Cíl práce

Cílem práce je navrhnout a nakonfigurovat emailový server s maximální možnou ochranou proti nežádoucím emailům a hrozbám. Tento cíl se neobejde bez volby vhodných konfigurovatelných a výkonných emailových funkcí, a především účinných bezpečnostních metod. Po dokončení bude server, jeho služby a tato práce využity ke konfiguraci nového emailového serveru u AČR jako testovací prostředí pro nový emailový server.

3 Metodika

Na splnění teoretické části bakalářské práce bude potřeba mnoho internetových a knižních zdrojů pro jasné vysvětlení jednotlivých bodů a částí práce. Ze začátku budou popsány základy a princip fungování emailové komunikace. Dále bude podrobně rozebráno podstatné téma bezpečnost, přesněji bezpečnostní metody, spamové filtry, možné hrozby emailové komunikace, a nakonec vysvětlení emailových protokolů a služeb.

V praktické části práce prvně bude nutné si stanovit veškeré požadované náležitosti, které má emailový server obsahovat a vybrat vhodné bezpečnostní metody. Následně dojde na základní konfiguraci prostředí, dále bude implementován postfix, správce brány firewall Firewalld a dojde na povolení všech potřebných portů nutných pro emailovou komunikaci. Po této části konfiguraci bude na řadě implementace dalších poštovních služeb, bezpečnostních metod a software, které budou vybrány a stanoveny jako nutné či vhodné pro použití na server. Nebudou chybět vytvořené testovací účty pro ověření komunikace a funkčních bezpečnostních metod. Nakonec bude nakonfigurovaný emailový server otestován.

4 Teoretická východiska

4.1 Základní informace

Jak už zde bylo řečeno, email využívá dnes téměř každý. Každý emailový účet musí mít vlastní unikátní adresu, z toho vyplývá, že každá emailová adresa je unikátní a nelze mít pojmenované 2 adresy stejně. Emailová adresa se skládá z uživatelského jména, “@“, neboli “zavináče“ a domény. Tyto adresy se používají pro komunikaci s ostatními uživateli emailu. [1]

Každému uživateli po registraci na danou doménu je přiřazen “mailbox“, neboli schránka, ve které může spravovat veškerou poštu. Při odesílání a přijímání emailu se do procesu zapojí hned několik agentů, kteří musí celou akci zpracovat a provést mnoho kroků ke splnění zadaného úkonu od klienta [2]:

- Mail User Agent (MUA)

Je poštovní klient, jehož úkolem je správa schránky, odesílání a přijímání pošty. Velmi často používaným poštovním klientem je Mozilla Thunderbird a Microsoft outlook, případně se využívají služební webmaily.

- Mail Submission Agent (MSA)

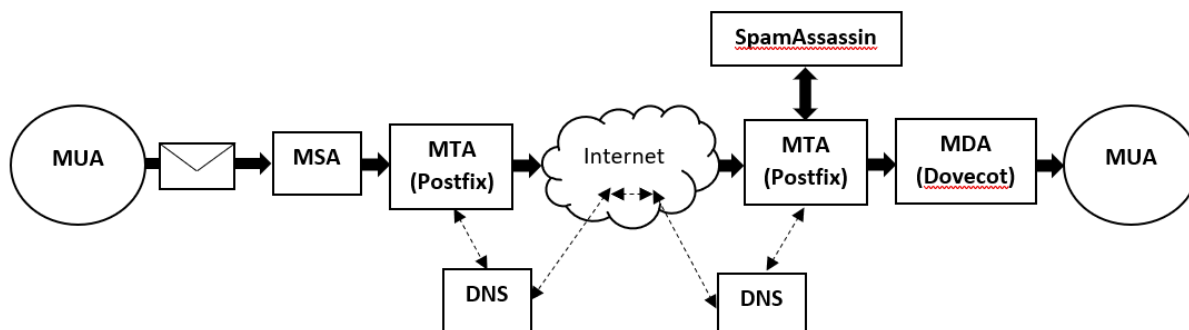
Tento agent slouží pro přebírání a odesílání pošty, přebírá zprávu od MUA a předává ji na MTA.

- Mail Transport Agent (MTA)

Agent přepravující poštu z jednoho serveru na druhý pomocí MX záznamů z DNS.

- Mail Delivery Agent (MDA)

Agent pro doručení pošty, který má za úkol email doručit do schránky příjemce.



Obrázek 1 – Komunikace emailových agentů

4.2 Bezpečnost

4.2.1 Bezpečnostní metody

Vzhledem k velkému množství emailových serverů a využívání jejich komunikace jsou bezpečnostní metody nikoliv možnou, ale nezbytnou součástí při konfiguraci nového emailového serveru. Bez těchto metod je server brán jako nezabezpečený a při komunikaci není důvěrný pro ostatní servery, většinou ani nemožní se s takto nezabezpečeným serverem spojit. Bez implementace metod může vnější svět způsobit ohrožení nejen serveru, ale i dat uživatelů a celé firmy nebo společnosti. [5]

- **Šifrování komunikace SSL/TLS**

SSL (Secure Socket Layer) a TLS (Transport Layer Security) protokoly mají za úkol zabezpečit a šifrovat komunikaci v internetu. Zabezpečují funkcionalitu, která neumožňuje přecházet komunikaci a uživatelskou autorizaci mezi poštovním klientem a serverem. V současnosti se používá SSL verze 3.3 a TLS 1.2, které nejsou téměř odlišné. Fungují na principu ověření certifikátu druhé strany. Každá strana má dva šifrovací klíče, a to veřejný a soukromý. Při zašifrování veřejným klíčem může data rozšifrovat pouze příjemce s identickým veřejným klíčem a k rozšifrování dat použije svůj soukromý klíč. V opačném případě je postup identický, ale veřejný klíč musí nést jednoznačnou identifikaci daného subjektu, kterou musí potvrdit důvěryhodná autorita (protože veřejný klíč má každý). [3][4]

- **SPF**

Neboli Sender Policy Framework je jeden ze základních ochranných prostředků emailového serveru, který zamezuje v šíření phishingu a padělání emailových domén, neboli "spoofingu". Jeho princip spočívá v kontrole IP adresy odesílatele, kdy při zjištění IP adresy, která není v seznamu povolených adres pro rozesílání emailů pod danou doménou, zakáže dané IP adrese předání emailu druhé osobě. S touto metodou roste důvěryhodnost pro emailové servery příjemce a je pravděpodobnější, že Váš email nebude emailovým serverem druhé strany zablokován, nebo označen jako spam. IP adresy, které smí jménem domény rozesílat emaily, určuje administrátor serveru nastavením nového DNS záznamu formou TXT. Tento záznam je složen ze tří částí – z identifikace, že jde o SPF, z povolených zdrojů pro rozesílání emailů a z nastavení, které určí, jak se server zachová v případě, že odesílatel není v povolených zdrojích. [6][7]

Pro povolené zdroje existuje více definic [8]:

- IPv4 adresy, nebo celý rozsah,
- IPV6 adresy, nebo celý rozsah,
- MX záznam,
- Reverzní záznam,
- A nebo AAAA záznam doména (A – Ipv4 / AAAA – Ipv6),
- SPF záznam z jiného serveru (Include).

Dále je potřeba nastavit tzv. kvalifikaci pro rozhodnutí, co má SPF udělat s nevyhovujícími zdroji. Tato kvalifikace se rozděluje na čtyři základní složky značené znaménky [8]:

- “-“, neboli “FAIL“ Tuto zprávu by měl příjemce odmítnout.
- “~“, neboli „NEUTRAL/FAIL“ Tuto zprávu příjemce může označit jako spam, nebo odmítnout.
- “?“ , neboli “NEUTRAL“ Akce s touto zprávou je na rozhodnutí příjemce.
- “+“, neboli “PASS“ Tato zpráva bude bez jakýchkoliv opatření přijata.

• **DKIM**

Neboli DomainKeys Identified Mail společně s SPF zvyšují důvěryhodnost emailů a emailové komunikace. Na rozdíl od SPF, který spojuje konkrétní IP adresy, rozsahy apod., ze kterých může pošta odcházet z dané domény, DKIM pracuje na metodě elektronického podpisu, který je generován Mail Transfer Agentem. DKIM provádí dva základní kroky. První je na serveru odesílatele, kdy vytvoří jedinečný řetězec znaků a elektronicky podepíše hlavičku odchozího emailu a druhý je na serveru příjemce, kdy pomocí veřejného klíče v internetové doméně odesílatele dešifruje tento řetězec znaků ze záhlaví emailu a pokud jsou DKIM podpisy shodné, server příjemce ví, že byl email odeslán z dané domény a není podvodný. [1][9][10]

• **DMARC**

Neboli Domain-based Message Authentication, Reporting & Conformance je protokol, který určuje, jak má server naložit se zprávami, které neodpovídají zásadám domény. Chrání proti neoprávněnému odesílání zpráv ze serveru, před emailovými útoky a pomáhá ke správné konfiguraci emailové struktury. Ke své činnosti potřebuje metodu SPF a DKIM. Tyto metody spojuje dohromady a umožňuje je využít zároveň. Vlastní navíc kompletní přehled odeslaných emailů pod danou doménou a umožňuje tím jejich analýzu. [1][11]

- **PTR a Reverzní DNS záznam**

Pointer records, nebo reverzní záznam slouží pro DNS, jako typ záznamu pro položení reverzního dotazu. Vytváří vzájemnou důvěru serverů, že odeslaný email je opravdu odeslaný z dané domény, či IP adresy, za kterou se vydává. Servery kontrolují dva záznamy a to “dopředný“ a reverzní. Dopředný záznam umožňuje překlad doménového jména na IP adresu a reverzní záznam opačně. Vzhledem k rozšíření PTR po celém světě je vhodné jej implementovat na každý emailový server, který bude komunikovat se servery vnějšího světa. [12][13]

4.2.2 Spam filtr

Dalším důležitým nástrojem pro ochranu emailového serveru a uživatelů emailových schránek je spam filtr. Používají se pro detekci jakkoliv infikovaných emailů a mají za úkol zabránit doručení takového emailu do uživatelské pošty, případně na něj minimálně upozornit. Každý spam filtr k detekci nežádoucí části emailů používá více druhů testů a filtrů jako např. Bayesovský filtr, filtr hlavičky, filtr obsahu zprávy a mnoho dalších. Existuje mnoho druhů spam filtrů, každý má své kladné i záporné stránky. Některé jsou však více propracované a přesné, např. SpamAssassin, Rspamd, Proxmox Mail a mnoho dalších. [14]

- **SpamAssassin**

Jak už název napovídá, jedná se o program, který chrání před hrozbami emailů. Má za úkol filtrovat obsah zprávy a tím detekovat případnou hrozbu. Byl napsán v programovacím jazyce Perl a je pod licencí Apache License 2.0. Je velmi oblíbený vzhledem k jeho přesnosti, rozšíření a možnosti nastavení a konfigurace. Používá metodu “skóre“, která znamená, že označuje při jednotlivých testech (porovnání těla zprávy, pole hlavičky, online databázi, blacklistů, DNS, Bayesovského filtru apod.) dané zprávy výsledkem buď kladně, nebo záporně a po dokončení testů výsledky dá do globálního skóre, podle kterého vyhodnotí, zda je email spam, či nikoliv. Nejpodstatnější je administrátorské nastavení, kdy si administrátor může nastavit limity, při jakém skóre má SpamAssassin email vyhodnotit jako bezpečný, nebo nebezpečný. Zpravidla kladné skóre znamená, že se jedná o spam, záporné poukazuje na neinfikovanou zprávu. [15][16]

- **Rspamd**

Tento spam filtr je napsán v programovacím jazyce “C“. V současné době je velmi rozšířený a je zejména využíván na extrémně vytížených emailových serverech. Jeho základ vychází ze SpamAssassina a nese plno jeho ochranných prvků. Používá taktéž metodu skóre, kterou si může administrátor sám v budoucnu přenastavit. Je distribuován pro hlavní distribuce Linuxu a je dostupný přes porty FreeBSD, NetBSD pkgscr a OpenBSD. [17]

4.2.3 Bezpečnostní rizika emailu

Bezpečnostní rizika v emailu se dělí na mnoho různých kategorií a skupin, zde budou rozděleny na 3 základní skupiny v podobě Spamu a Phishingu, Malware a Spoofingu. Tyto skupiny jsou silně provázané a vzájemně kombinované. Níže budou jednotlivé skupiny rozebrány, popsány, jaké nebezpečí s sebou přináší a co případná infekce zařízení dokáže způsobit.

- **Spam**

Jde nejčastěji o globální rozesílání nevhodného či nežádoucího emailu milionům uživatelů denně a v miliardovém množství. Příjemce se může setkat s nemalým množstvím různých nabídek na určitý druh zboží s velkou slevou nebo na vnučování ke stažení nějakého software zdarma a mnoho dalších. Samotný email v závislosti na typu spamu není pro uživatele nebezpečný, pokud daný email nijak nezpracuje. Dále spam zatěžuje poštovní servery, plní schránky uživatelů, zpomaluje využívanou síť a jiné. [18][19]

- **Phishing**

Velmi rozšířený typ útoku na uživatele emailových schránek, kdy se útočník snaží získat jejich citlivé údaje v podobě přístupových jmen a hesel, čísel kreditních karet, bydliště, osobní údaje apod. Útočník se zpravidla vydává za důvěryhodný subjekt, který je nějakým způsobem známý veřejnosti, ať už jako firma, nebo osoba. Zpravidla bývá zaměřený na velký počet uživatelů, ale může být i cílený na konkrétní osobu. V takovém případě útočník přímo specifikuje podvodný email tak, aby byl dané osobě důvěrnější. V případě, že je útočník zkušený a jeho útok například napodobuje nějakou důvěryhodnou stránku, je pro nezkušeného uživatele tento útok velmi složité rozeznat a často dochází k úniku dat. [19][25]

- **Reklamy**

Tento typ spamu je jednoznačně nejčastější a nejméně nebezpečný. Snad každý ve své emailové schránce najde email s nabídkou na nějaké zboží či služby. Standardně se jedná o podvod, ale najdou se i reálné nabídky, což nic nemění na skutečnosti, že se jedná

o email, který uživatel nechtěl dostat do své schránky. Uživatelské schránky se těmito typy emailů plní a zabírají místo. Pokud je však emailový server správně nakonfigurován a dokáže tyto zprávy rozeznat od “potřebných“, zprávu vůbec nedoručí, nebo přesune do složky “SPAM“, ze které se pošta standardně automaticky maže po 30 ti dnech od doručení. [18]

- Hoax

Tento typ spamu nebyl po dlouhou dobu tak běžný, nebyly na něj brány ohledy a dařilo se jej odhalovat a blokovat. V současné době je však ve velkém množství rozšířený. Má za úkol vyvolat paniku, předávat poplašné zprávy ale i sdílet uživatelské údaje. Hoax často nabízí zázračné zboží, přesvědčuje uživatele o napadení uživatelského zařízení virem, předává nepravdivé informace, uživatele odkazuje na podvodné webové stránky, nutí přeposlat email dalším uživatelům a mnoho dalších. Nejčastějším typem Hoaxu je, že se útočník snaží přesvědčit uživatele, že bylo jeho zařízení napadeno Malware či virem. Z emailu vyplývá, že má odesílatel emailu vhodné a bezpečné řešení, jak se nebezpečí zbavit. Nejčastěji požadují předání určitých uživatelských informací, zaplacení poplatku pro odstranění hrozby, nebo stažení přílohy, která standardně obsahuje nějaký vir, Malware apod. [18][30]

- Finanční podvod

Útočník se snaží od uživatele získat nějakou finanční částku, ať už jako podporu hladových dětí z chudých zemí, pro lidi zasažené přírodní katastrofou, ale i jako investici do budoucna, která se uživateli mnohonásobně vrátí. Tento druh spamu je nebezpečný hlavně pro možnost odevzdání uživatelských platebních údajů do bankovníctví. Nejčastěji však dojde v případě nepozornosti uživatele pouze na finanční podporu útočníka. [18][28][29]

- Bankovní podvody

Poměrně nebezpečný typ Phishingu, kdy se útočník velmi důvěryhodně vydává za pracovníka banky s cílem získat uživatelské bankovní údaje, a to vyplněním online dotazníku, či přihlášením na padělané internetové stránky banky. Tento typ podvodu je složité rozeznat a často dochází k úniku uživatelských informací, i když téměř každá bankovní společnost neustále varuje vlastní zákazníky před těmito hrozbami. [28][29]

- **Malware**

Jeden z dalších druhů nevyžádané pošty, který je však mnohem nebezpečnější a v současné době velmi používaný. Nejčastěji obsahuje odkazy na internetové stránky, nebo přílohy s příponami .exe, .jar, .bat a jiné. Tento druh útoku může poškodit zařízení, smazat uživatelská data, ukrást přihlašovací údaje, zahltit a poškodit celou lokální síť, ale i sledovat uživatelskou činnost. [19][22]

- Ransomware

Je velmi nebezpečný typ Malware, který nejčastěji šifruje uživatelská data, nebo úplně znemožní použití napadeného zařízení, dokud například nezaplatíte požadovanou částku pro odblokování zařízení. Tento program se dokáže rozšířit i do dalších zařízení v síti a sdílených úložišť. V případě infekce není postup “očistění“ jednoduchý. Zpravidla je potřeba spustit antivirovou ochranu a přes zabezpečení systému zařízení úplně vyčistit. Ne vždy je to ale možné, pak dochází na zálohování uživatelských dat a obnova systému, nebo úplná reinstalace. Někdy však nepomáhá ani jedna z uvedených možností, nebo je nelze aplikovat a je nutné vyhledat specialistu, který dokáže zařízení od napadení očistit. Tento postup je však velice nákladný. [20][22]

- Červi

Také známí jako “Worms“ jsou nebezpečný kód, který se sám množí a šíří do dalších zařízení prostřednictvím sítě, nebo přes přenosná média. Jak už z jejich principu fungování vyplývá, množením velmi zatěžují a zpomalují síť, zaplňují úložiště zařízení, zpomalují operační systém, a to až do jeho úplného zastavení/zaseknutí. Ke své činnosti většinou využívá programy přistupující k systému a systémové chyby. Díky červům může útočník využít uživatelský emailový účet k dalšímu rozeslání spamu a jiných bezpečnostních hrozeb. [22][27]

- Trojský kůň

Svým způsobem odpovídá historickému příběhu o dobytí Tróje. Pro uživatele je velmi složitě odhalitelný. Nejčastěji se ukrývá pod odkazem na stažení hry zdarma, nabízeného užitečného programu, doplňkem pro systém apod. Po spuštění v zařízení dokáže zařízení poškodit, mazat data, umožnit pro útočníka ovládat zařízení vzdáleně, sledovat uživatelskou aktivitu, předat osobní údaje nebo spustit další útok. [22][26]

- Scareware

Jak už z názvu vyplývá, u Scareware se útočník snaží uživateli vnutit, že bylo jeho zařízení napadeno a je nutné stáhnout (zakoupit) určitou aplikaci, aby zamezil poškození zařízení. Od uživatele tím získá přístup do bankovníctví, uživatelský emailový účet a dále podle typu software i následné možnosti se zařízením. Tato metoda je poměrně častá i mimo svět emailu, nejčastěji velmi věrohodně vypadající vyskakující okno při prohlížení internetových stránek, nebo spouštění filmů na stránkách zdarma. [22]

- Spyware

Je typ malware, který je velmi těžko odhalitelný. Bývá do zařízení nainstalován při otevření infikovaného emailu, společně s jiným programem zdarma dostupným na internetu, nebo i nevinným stahováním filmů a hudby z různých serverů. Tento program sleduje veškerou uživatelskou aktivitu v podobě aktivity na internetu, plateb, hesel a mnoho dalších. Velmi často předává bez vědomí uživatele všechny tyto informace třetím stranám k dalšímu zneužití. [22][23]

- Adware

Adware se zaměřuje na nevhodné a nechtěné reklamy, které se zobrazují v zařízení v podobě vyskakovacích oken a webových stránek. Samotný Adware není nijak škodlivý, ale je schopný odkazovat na nebezpečné stránky, které již nesou jistá bezpečnostní rizika. Především znepříjemňuje využívání zařízení v podobě vyskakovacích reklam, zakrývání větší části plochy či obrazovky a dokáže měnit i nastavení prohlížeče. V horších případech dokáže shromažďovat osobní informace uživatele, historii prohlížeče a ve výjimečných případech i monitorovat používání klávesnice. [22][24]

• **Spoofing**

Je typ útoku v podobě falešného odesílatele emailové zprávy jednoduchým paděláním hlavičky emailu, což je nedostatek SMTP protokolu. Útočník se zde tváří jako důvěryhodný subjekt, který má přesvědčit příjemce zprávy o důvěryhodnosti doručeného emailu. Velmi často je spoofing součástí phishingového útoku. Jde o poměrně závažnou trhlinu v bezpečnosti, jelikož se může útočník vydávat za téměř kohokoliv a do emailu vložit cokoli, čímž může poškodit jak příjemce pošty, tak i reálného majitele zneužitě adresy. Proti spoofingu adres či domény se používají bezpečnostní metody SPF a DKIM implementované na emailovém serveru. [31][32]

4.2.4 Necurs botnet – bezpečnostní incident

Jednou z velkých emailových afér v podobě rozesílání malware, phishingu, spamu, virů a dalších výše uvedených bezpečnostních rizik má na starosti tzv. Necurs botnet. Byla to obrovská síť centrálně řízených počítačů po celém světě, kterou útočníci získali napadením a infikací počítačů speciálním softwarem, díky kterému mohli zařízení použít k dalším nelegálním činnostem. Za své neaktivnější působnosti dokázali útočníci napadnout 9 milionů počítačů. Tomuto počítačovému “masakru“ zabránila společnost Microsoft a partneři z 35 zemí světa díky přebrání kontroly nad americkou infrastrukturou, kterou Necurs používal pro sdílení škodlivého software. [21]

4.3 Emailové protokoly

- **IMAP**

Protokol sloužící pro příjem pošty. IMAP v současné době lze nastavit na použití 2 různých portů, a to na portu 143, u kterého není komunikace zašifrována a zašifrovaného portu, kde je implementováno šifrování SSL/TLS a pracuje na portu 993. Oproti POP3 protokolu IMAP nechává poštu na serveru a pouze ji zrcadlí do emailového klienta. Uživatel tím manipuluje s poštou přímo na serveru a může se přihlásit do svého emailového účtu z jakéhokoliv klienta i zařízení a poštu bude mít vždy kompletní. [33][34]

- **SMTP**

Jeho úkolem je odesílání pošty z jednoho serveru na druhý pomocí přímého spojení. SMTP funguje nad protokolem TCP a lze ho také nastavit na 2 různých portech, nezabezpečený port 25 a zabezpečený pomocí SSL/TLS na portu 465. Formát odeslané zprávy přes SMTP obsahuje hlavičku a tělo zprávy. Poštu může uživatel odesílat pomocí nakonfigurovaného emailového klienta, případně pomocí webového klienta. [33][35]

- **POP3**

Jeho vlastností oproti IMAP, který zastává stejnou funkci v podobě přijímání pošty je, že si protokol POP3 stahuje poštu do lokálního klienta a nenechává ji na serveru, z toho vyplývá, že po přihlášení na jiné zařízení nebo klienta uživatel předešlou poštu nebude mít dostupnou. POP3 pracuje taktéž na 2 portech, portu 110, který není šifrovaný a na portu 995 šifrovaném pomocí SSL/TLS. [33][36]

4.4 Poštovní služby

Poštovní služby si lze představit jako programy, které dle svých vlastností plní daný úkol v podobě zpracování pošty, ať už její doručení do schránky příjemce, tak zpracování a odeslání pošty od odesílatele. Jejich nedílnou součástí jsou emailoví agenti MDA a MTA. V obou kategoriích existuje mnoho typů s určitým zaměřením, v následující části budou rozebráni ti nejznámější. [37]

4.4.1 Agenti pro příjem pošty

- **Dovecot**

Je MDA emailový agent s protokolem POP3 a IMAP, které podporuje v plné šíři. Ve světě Linuxu je brán jako jeden z nejrychlejších, nejbezpečnějších a nejvýkonnějších serverů IMAP sloužících pro přístup uživatelů do jejich emailových schránek přes různé poštovní klienty, které jsou volně k dispozici. Je jednoduchý na správu, má nízké systémové nároky a lze jej neustále upravovat a rozšiřovat. Velmi často je používán ve spolupráci s postfixem. Dokáže sám analyzovat problém a snaží se ho řešit, přičemž je veškerá činnost logována i pro pozdější analýzu a případné řešení. [37][38]

- **Courier IMAP**

Tento typ IMAP serveru je velmi oblíbený díky snadné manipulaci se stovkami tisíc emailových schránek. Jeho obrovskou výhodou je možnost stáhnout kompletní emailový server Courier, který umožňuje spolupráci s SMTP, IMAP, POP3, webmail a kompletní nastavení emailové komunikace a dokáže tak zastoupit všechny ostatní služby. V opačném případě je kompatibilní s agenty Postfix, EXIM apod. Jeho konfigurační soubory jsou především ve formátu textového souboru a tím umožňuje velké množství konfigurace. [39]

4.4.2 Agenti pro přenos pošty

- **Postfix**

Je MTA emailový agent přenášející poštu mezi emailovými servery, kdy je jeho protokolem SMTP. Stará se o směrování, doručení do schránek, přebírání a předávání jiným severům. Hlavní výhodou Postfixu je, že je rychlý díky správci front, poměrně snadný na konfiguraci, lze jej rozšiřovat a implementovat na většinu distribucí Linuxu a Unixu. Jeho dominantní výhodou je zaměření na bezpečnost. Struktura jeho systému je rozdělena na

mnoho malých na sobě nezávislých spustitelných souborů, které v případě problémů lze nahradit za jiný. Svým způsobem byl navržen, aby nahradil Sendmail. [40][41]

- **Sendmail**

Zabezpečuje stejnou funkci, jako Postfix. Postupně se jeho využívání ztrácí, a to díky vývoji právě Postfixu. Velkou nevýhodou oproti Postfixu je nižší stupeň bezpečnosti a jeho jednoprosocová struktura, která běžela vždy pod superuživatелеm “root“. I když je předinstalován na mnoha komerčních operačních systémech Unixu a lze jej použít i na systému Windows, není v současné době již doporučován k použití. [42][44]

- **EXIM**

Další z MTA emailových agentů, který je velmi rozšířený. Je vyvinutý pro více operačních systémů jako Unix, Linux, Solaris, Mac OSX apod. Jeho dominantními vlastnostmi jsou schopnost zpracování obrovského množství emailů, nabízí nejvíce konfiguračních možností oproti Postfix i Sendmail a podporuje cPanel (ovládací panel pro správu webových stránek). Z bezpečnostního hlediska mírně ztrácí na Postfix. V současné době je brán jako výchozí MTA pro systém Debian Linux. [43][44]

5 Vlastní práce

5.1 Úvod

Hlavním úkolem této části projektu je nakonfigurovat co nejbezpečnější emailový server, který bude splňovat zadané požadavky, obsahovat zadané služby či funkce, bude jej možné co nejjednodušeji obsluhovat a případně najít a naimplementovat další bezpečnostní prvky.

5.2 Požadavky

Již ze zadání bakalářské práce vyplývá, že jsou některé funkce předem zadány a v projektu požadovány. Tyto požadavky mi byly sděleny ještě před samotným rozhodnutím, že budu tento projekt zpracovávat formou bakalářské práce.

Předem stanovené požadavky:

- Použití operačního systému CentOS 8.
- Implementace MTA Postfixu.
- Implementace MDA Dovecotu.
- Implementace spam filtru SpamAssassina.

Požadavky ke zjištění:

- Najít vhodné bezpečnostní metody.
- Možnost využít blacklist a whitelist.
- Funkční emailové protokoly IMAP, SMTP a případně POP3.

Bezpečnostní metody

Na základě konzultace s vedením a dalšími administrátory, zkušenostmi s provozem a administrací emailového serveru u AČR byly zvoleny následující metody:

- Open DKIM
- SPF
- DMARC
- šifrování SSL/TLS

Tyto metody zajistí vyšší emailovou bezpečnost. Jejich standardizace zaručuje širokou kompatibilitu a ztěžuje zneužití e-mailové komunikace na vlastním serveru a zároveň zvyšuje důvěryhodnost serveru ve veřejném sektoru. Jejich nasazení není však jednoduché, neobejde se bez dalších reakčních skriptů a jejich plná konfigurace bude časově náročná.

Jako emailovou doménu jsem použil již existující doménu mail.ugcz.eu, která sloužila dříve pro mé vlastní testování. Doména není v současné době nijak využívána a není evidována v žádných blacklistech.

Pro konfiguraci emailového severu je v našem případě vhodné použít virtuální privátní prostředí (VPS). Nejpodstatnější požadavek na poskytovatele je, aby neblokoval port 25, jeho adresy nejsou na žádných blacklistech a je možné editovat PTR Record. Z toho důvodu bude využito prostředí od společnosti WEDOS, které zaručuje stabilní, výkonné, finančně levné prostředí a splňuje naše požadavky.

5.3 Postup konfigurace

Začneme základní přípravou prostředí, kde je nainstalován operační systém a základním nastavením samotného systému. Poté bude nainstalován a nakonfigurován postfix s firewallem a otevření všech potřebných portů. Dále bude nainstalován TLS certifikát, což obnáší instalaci certifikačního bota a Apache server. Následně bude nainstalován a nakonfigurován Dovecot, nakonfigurováno šifrování SSL/TLS a vytvoření testovacích uživatelů. Poté dojde na základní nastavení a konfiguraci bezpečnostních metod SPF a Open DKIM. Následovat bude vygenerování veřejného a privátního klíče, propojení Postfixu a Open DKIM a nastavení DMARC. Předposledním krokem bude zprovoznění SpamAssassina a nastavení blacklistu a whitelistu. Na závěr otestování služeb a funkcí.

5.3.1 Nastavení prostředí před konfigurací služeb

Před samotnou instalací Postfixu musíme nastavit na serveru hostname. To provedeme příkazem:

```
sudo hostname set-hostname mail.ugcz.eu
```

Následně musíme mimo systém na virtuálním serveru vytvořit své “MX“ a “A“ záznamy pro DNS a PTR záznam.

název	TTL	typ	data
✖	1800	A	89.221.220.161
✖	1800	MX	0 mail.ugcz.eu

Obrázek 2 – Nastavení MX a A záznamu

Reverzní záznamy - IPv4				
	Adresa ↕	Data	Vytvořeno ↕	Upraveno
✖	89.221.220.161	mail.ugcz.eu	08.10.2021 14:43:50	

Obrázek 3 – Nastavení reverzního záznamu

5.3.2 Postfix

Instalace Postfixu

Prvně musíme zaktualizovat instalační manažer balíčků, dále nainstalovat Postfix, spustit jej, nastavit automatické spuštění Postfixu při spuštění serveru a otestovat jeho funkčnost.

```
sudo dnf update
```

```
sudo dnf install postfix -y
```

```
sudo systemctl start postfix
```

```
sudo systemctl enable postfix
```

```
systemctl status postfix
```

Konfigurace Postfixu

Prvně je potřeba zajistit, aby naslouchal na všech interfezech, nejen na localhost, dále změním postfix hostname, vlastní doménu, my origin a my destination. Nakonec zrestartujeme Postfix.

```
sudo postconf -e "inet_interfaces = all"
```

```
sudo postconf -e "myhostname = mail.ugcz.eu"
```

```
sudo postconf -e "mydomain = ugcz.eu"
```

```
sudo postconf -e "myorigin = mail.ugcz.eu"
```

```
sudo postconf -e "mydestination = ugcz.eu \ $myhostname, localhost.\ $mydomain, localhost"
```

5.3.3 Firewall

Provedeme instalaci, spuštění a povolení automatického spuštění firewallu, následně nastavíme povolení permanentního otevření portu 25.

```
sudo systemctl reload firewalld
sudo dnf install firewalld
sudo systemctl start firewalld
sudo systemctl enable firewalld
sudo firewall-cmd -permanent -add-port=25/tcp
```

Následně musíme provést otevření ostatních portů potřebných pro emailovou komunikaci. Povolené porty budou pro http, https, smtp-submission, smtps, imap a imaps. Následně zrestartujeme firewall pro propsání nastavení portů.

```
sudo firewall-cmd --permanent -add-service={http,https,smtpsubmission,smtps,imap,
impas}
sudo systemctl reload firewalld
```

Následující obrázek zobrazuje povolené porty naší domény po úpravě. Lze zjistit na <https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap>

Hostnames
mail.ugcz.eu

PORT NUMBER	STATE	SERVICE NAME	SERVICE PRODUCT	SERVICE INFO
22	Open	ssh	OpenSSH 8.0	protocol 2.0
25	Open	smtp	Postfix smtpd	
80	Open	http	Apache httpd 2.4.37	(centos) OpenSSL/1.1.1k
110	Closed	pop3		
143	Open	imap	Dovecot imapd	
443	Open	ssl	Apache httpd	SSL-only mode
465	Open	smtp	Postfix smtpd	
587	Open	smtp	Postfix smtpd	
993	Open	imap	Dovecot imapd	
995	Closed	pop3s		

Obrázek 4 – Zobrazení povolených portů po nastavení

5.3.4 Instalace TLS certifikátu a Apache serveru

Základem pro TLS certifikát je získání certifikačního bota, který vytvoří certifikát pro náš server a webový server, v našem případě Apache. Nakonec zrestaurujeme Apache server.

```
sudo dnf install epel-release -y
sudo dnf install certbot
sudo dnf install httpd
sudo systemctl start httpd
sudo systemctl enable httpd
sudo dnf install python3-certbot-apache
```

Následně zeditujeme soubor `/etc/httpd/conf.d/ugcz.eu.conf` a zrestartujeme Apache server.

```
<VirtualHost *:80>
    ServerName ugcz.eu
    DocumentRoot /var/www/html/
</VirtualHost>
```

```
sudo systemctl reload httpd
```

Povolíme využití desktopových poštovních klientů (outlook, Thunderbird apod.) pomocí postfixu. Úpravu provedeme dle obrázku 4. v souboru `/etc/postfix/master.cf`.

```

smtp      inet n    -    n    -    -    smtpd
#smtp    inet n    -    n    -    1    postscreen
#smtpd   pass  -    -    n    -    -    smtpd
#dnsmlog unix -    -    n    -    0    dnsmlog
#tlsproxy unix -    -    n    -    0    tlsproxy
submission inet n    -    y    -    -    smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_tls_wrappermode=no
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
#smtps   inet n    -    n    -    -    smtpd
#  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
smtps     inet n    -    y    -    -    smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
#628     inet n    -    n    -    -    qmqpd
pickup    unix n    -    n    60    1    pickup
cleanup   unix n    -    n    -    0    cleanup
qmgr      unix n    -    n    300    1    qmgr
#qmgr     unix n    -    n    300    1    oqmgr
tlsmgr    unix -    -    n    1000?  1    tlsmgr
rewrite   unix -    -    n    -    -    trivial-rewrite
bounce    unix -    -    n    -    0    bounce
defer     unix -    -    n    -    0    bounce
trace     unix -    -    n    -    0    bounce
verify    unix -    -    n    -    1    verify
flush     unix n    -    n    1000?  0    flush
proxymap  unix -    -    n    -    -    proxymap
proxymap  unix -    -    n    -    1    proxymap
smtp      unix -    -    n    -    -    smtp
relay     unix -    -    n    -    -    smtp
  -o syslog_name=postfix/$service_name
#  -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix n    -    n    -    -    showq
error     unix -    -    n    -    -    error
retry     unix -    -    n    -    -    error
discard   unix -    -    n    -    -    discard
local     unix -    -    n    -    -    local
virtual   unix -    -    n    -    -    virtual
lmtpl     unix -    -    n    -    -    lmtpl
anvil     unix -    -    n    -    1    anvil
scache    unix -    -    n    -    1    scache
postlog   unix-dgram n    -    n    -    1    postlogd

```

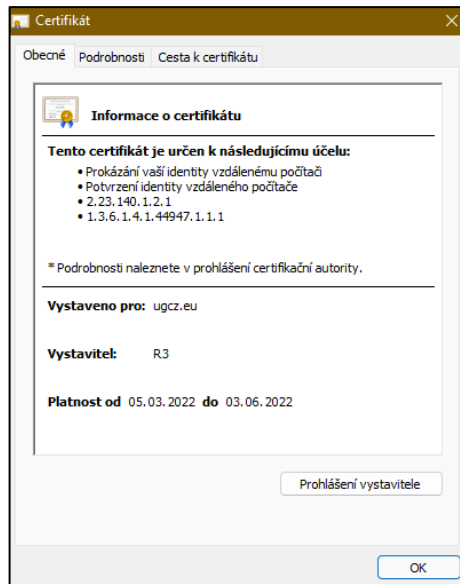
Obrázek 5 – Výpis konfigurace souboru master.cf

Dalším krokem je spuštění certifikačního bota pro vygenerování certifikátu ze stránky <https://letsencrypt.org> na náš server a specifikace složek TLS certifikátů pro náš server.

```
certbot -d ugcz.eu,mail.ugcz.eu,www.ugcz.eu --expand
```

```
sudo postconf "smtpd_tls_cert_file = /etc/letsencrypt/live/ugcz.eu/fullchain.pem"
```

```
sudo postconf "smtpd_tls_key_file = /etc/letsencrypt/live/ugcz.eu/privkey.pem"
```



Obrázek 6 – Vygenerovaný platný certifikát pro naši doménu

Z důvodu bezpečnosti zakážeme starší a nezabezpečené SSL a TLS verze. Úpravu provedeme taktéž v souboru `/etc/postfix/master.cf` dle přiloženého textu níže.

#Vynuceni TLSv1.3 nebo TLSv1.2

smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

mailbox_transport = lmtp:unix:private/dovecot-lmtp

smtputf8_enable = no

policyd-spf_time_limit = 3600

smtpd_recipient_restrictions =

permit_mynetworks,

permit_sasl_authenticated,

reject_unauth_destination,

check_policy_service unix:private/policyd-spf

5.3.5 Dovecot

Instalace Dovecot

Prvně je potřeba stáhnout a nainstalovat Dovecot. Následně jej spustit, nastavit automatické spuštění při spuštění serveru a nakonec si zobrazíme jeho stav.

```
sudo dnf install dovecot -y
sudo systemctl start dovecot
sudo systemctl enable dovecot
systemctl status dovecot
```

Konfigurace Dovecotu

Základní konfiguraci provedeme v souboru */etc/dovecot/dovecot.conf*, kde povolíme IMAP a LMTP protokol.

```
#protocols = imap lmtp submission
protocols = imap lmtp
```

Následně upravíme soubor */etc/dovecot/conf.d/10-master.conf* dle předlohy.

```
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
}
```

Nakonec upravíme konfigurační soubor postfixu */etc/postfix/main.cf*, aby doručoval emaily do úložiště přes Dovecot LMTP a deaktivoval “SMTPUTF8“, protože Dovecot-LMTP toto rozšíření nepodporuje.

```
mailbox_transport = lmtp:unix:private/dovecot-lmtp
smtputf8_enable = no
```

5.3.6 Konfigurace šifrování SSL/TLS

Z hlediska bezpečnosti nastavíme v konfiguračním souboru SSL/TLS */etc/dovecot/conf.d/10-ssl.conf*, aby e-mailoví klienti komunikovali s Dovecotem pomocí šifrování TLS.

```

##
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
# disable plain pop3 and imap, allowed are only pop3+TLS, pop3s, imap+TLS and imaps
# plain imap and pop3 are still allowed for local connections
ssl = required

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/letsencrypt/live/ugcz.eu/fullchain.pem
ssl_key = </etc/letsencrypt/live/ugcz.eu/privkey.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>.
#ssl_key_password =

```

Obrázek 7 – Úprava konfiguračního souboru SSL/TLS

Dále nastavíme autentizaci pomocí SASL mezi Postfixem a Dovecotem, aby mezi sebou komunikovali též šifrovaně. Zeditujeme soubor `/etc/dovecot/conf.d/10-master.conf` následovně.

```

service auth {
    unix_listener /var/spool/postfix/private/auth {
        mode = 0600
        user = postfix
        group = postfix
    }
}

```

5.3.7 Vytvoření testovacích uživatelů

Pro otestování komunikace a správného nastavení serveru je nutné vytvořit testovací emailové adresy. Vytvoříme testovací účty `User1` a `User2`. Vytvoření a nastavení hesla provedeme následovně dle předlohy pro tvorbu účtu `User1`:

```

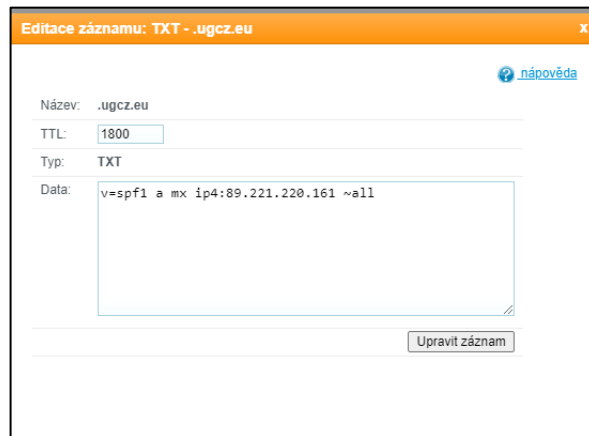
sudo adduser User1
sudo passwd User1

```

Následně zadáme heslo, které napíšeme znovu pro ověření a testovací uživatel je vytvořen.

5.3.8 SPF

Před samotným zprovozněním SPF chceme zajistit, aby Postfix kontroloval SPF záznamy příchozích emailů, aby případně zjistil podvržené emaily. Před instalací musíme nastavit SPF záznam v DNS.



Edítace záznamu: TXT - .ugcz.eu

Název: .ugcz.eu

TTL: 1800

Typ: TXT

Data: v=spf1 a mx ip4:89.221.220.161 ~all

Upravit záznam

Obrázek 8 – SPF záznam v DNS

Konfigurace SPF

Nejprve musíme stáhnout požadované balíčky, následně přidáme uživatele pro policyd-spf.

```
sudo dnf install epel-release
```

```
sudo dnf install pypolicyd-spf
```

```
sudo adduser policyd-spf --user-group --no-create-home -s /bin/false
```

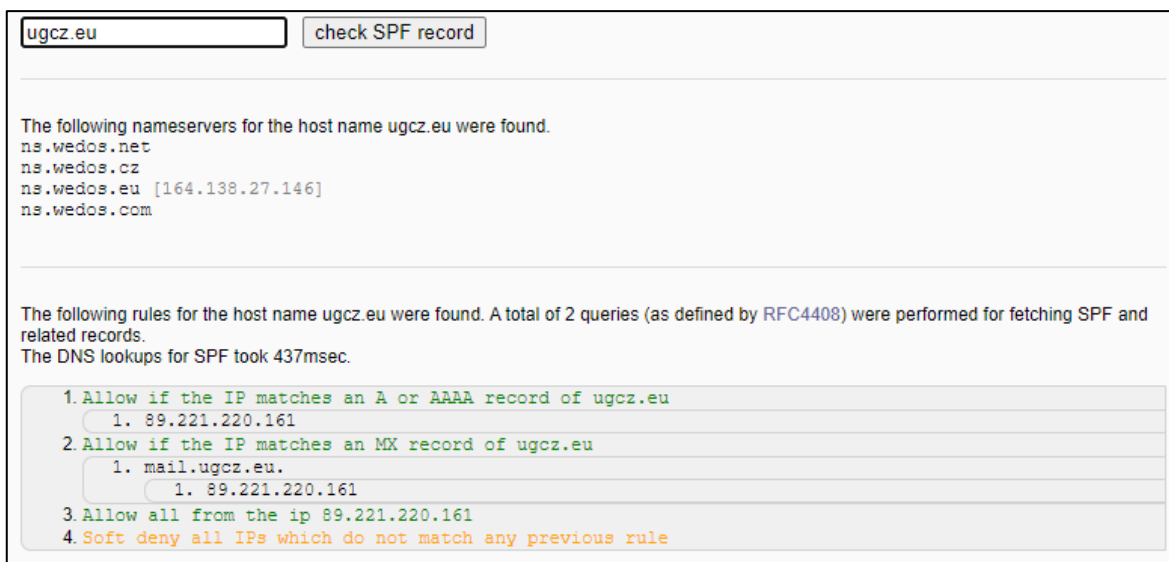
Upravíme soubor `/etc/postfix/master.cf`, kde přidáme požadavek na konec souboru, aby postfix při svém spuštění aktivoval démona zásad SPF. Restart Postfixu.

```
policyd-spf unix - nn - 0 spawn
```

```
user=policyd-spf argv=/usr/libexec/postfix/policyd-spf
```

ID zprávy	<61ec38b3.1c69fb81.e70ae.8bb9SMTPIN_ADDED_MISSING@mx.google.com>
Čas vytvoření:	22. ledna 2022 18:02 (Doručeno za -13 sekund)
Od:	user1 <user1@ugcz.eu>
Komu:	[REDACTED]
Předmět:	Test
SPF:	Výsledek pro IP adresu 89.221.220.161: PASS Další informace

Obrázek 9 – Test odeslaného emailu včetně potvrzení o funkčnosti SPF (z emailového klienta)



Obrázek 10 – Kontrola funkčnosti SPF z webové stránky

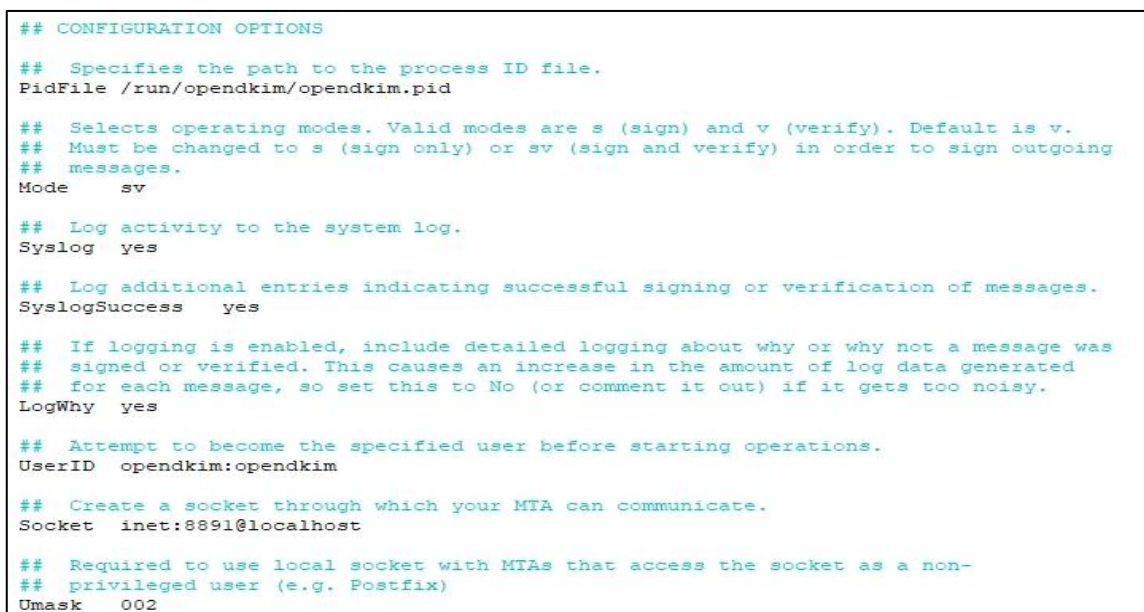
5.3.9 DKIM

Opět prvním krokem je stažení Open DKIM z úložiště souborů EPEL pro Linux.

```
sudo dnf install epel-release
```

```
sudo dnf install opendkim perl-Getopt-Long
```

Následně upravíme soubor `/etc/opendkim.conf`, kde dle obrázku 16 povolíme podepisování odchozích emailů z našeho serveru, to provedeme zakomentování, či odkomentováním řádků dle předlohy.



Obrázek 11 – Upravený konfigurační Open DKIM soubor

Dále vytvoříme tabulky hostitelů, které slouží pro vlastní důvěryhodnost ostatním serverům. Upravíme soubor `/etc/opendkim/SigningTable` následodvně dle obrázku 17, přidáním na konec souboru. Tento krok má zaručit podpis odesílatele z našeho serveru.

```
#example.com default._domainkey.example.com
*@ugcz.eu 20220122._domainkey.ugcz.eu
```

Další úprava bude provedena v souboru `/etc/opendkim/KeyTable`, kde určíme umístění soukromého klíče.

```
20220122._domainkey.ugcz.eu
ugcz.eu:20220122:/etc/opendkim/keys/ugcz.eu/20220122.private
```

Posledním krokem upravíme soubor důvěryhodných hostitelů `/etc/opendkim/TrustedHosts`, kde přidáme řádek s naší doménou (tento krok říká OpenDKIM, že pokud přichází email z naší vlastní domény, nemusí provádět ověření).

```
# OPENDKIM TRUSTED HOSTS
# To use this file, uncomment the #External IgnoreList and/or the #InternalHosts
# option in /etc/opendkim.conf then restart OpenDKIM, Additional Hosts
# may be added on separate lines (IP addresses, hostnames, or CIDR rangers).
# The localhost IP (127.0.0.1) should always be the first entry in this file.
127.0.0.1
::1
#host.example.com
#192.168.1.0/24
*.ugcz.eu
```

5.3.10 Privátní a veřejný klíč

Vygenerování privátního a veřejného klíče je zásadní pro DKIM, který jednak podepisuje odchozí zprávy a ověřuje příchozí. Vytvoříme si vlastní složku pro doménu a následně pomocí generátoru získáme klíč.

```
sudo mkdir /etc/opendkim/keys/ mail.ugcz.eu
sudo opendkim-genkey -b 2048 -d mail.ugcz.eu -D /etc/opendkim/keys/ mail.ugcz.eu -s
20220122 -v
```

Následně Open DKIMu nastavíme oprávnění jako vlastníka klíče, aby do něj mohl zapisovat a číst.

```
sudo chown opendkim:opendkim /etc/opendkim/keys/ -R
```

Zveřejnění veřejného klíče

Zveřejnění klíče provedeme v záznamu DNS dle obrázku 20. (soukromý klíč není vhodné veřejně vystavovat, jelikož slouží pro kontrolu veřejného klíče).



Obrázek 12 – Veřejný klíč zobrazený v záznamu DNS

5.3.11 Propojení Postfix a Open DKIM

Provedeme editaci souboru Postfixu `/etc/postfix/main.cf` dle přiloženého obrázku 21 přidáním řádků.

```
# Milter configuration
```

```
milter_default_action = accept
```

```
milter_protocol = 6
```

```
smtpd_milters = inet:127.0.0.1:8891
```

```
non_smtpd_milters = $smtpd_milters
```

Následně přidáme Postfix uživatele do Open DKIM skupiny a zrestartujeme Postfix.

```
sudo gpasswd -a postfix opendkim
```

```
sudo systemctl restart postfix
```

5.3.12 DMARC

Pro funkční DMARC je potřeba mít nakonfigurované a funkční metody DKIM a SPF a jejich záznamy a díky nim si vytvoříme DMARC záznam. Tím je nastavení kompletní.



The screenshot shows a web interface for editing a DNS record. The title bar reads "Editace záznamu: TXT - _dmarc.ugcz.eu". The form contains the following fields:

- Název:
- TTL:
- Typ:
- Data:

There is a "návod" (help) icon in the top right and an "Upravit záznam" (edit record) button at the bottom right.

Obrázek 13 – Nastavení DMARC záznamu

ID zprávy	<61ec4165.1c69fb81.c690f.7822SMTPIN_ADDED_MISSING@mx.google.com>
Čas vytvoření:	22. ledna 2022 18:40 (Doručeno za -12 sekund)
Od:	user1 <user1@ugcz.eu>
Komu:	[REDACTED]
Předmět:	tewst
SPF:	Výsledek pro IP adresu 89.221.220.161: PASS Další informace
DKIM:	Výsledek pro doménu ugcz.eu: 'PASS' Další informace
DMARC:	'PASS' Další informace

Obrázek 14 – Ověření funkčního DMARC

5.3.13 SpamAssassin

Pro zprovoznění SpamAssassina nejprve službu stáhneme, aktivujeme a spustíme. Následně nainstalujeme spam filtr balíčky z úložiště EPEL, aktivujeme službu a nastavíme automatické spuštění při spuštění serveru.

```
sudo dnf install spamassassin
```

```
sudo systemctl enable spamassassin
```

```
sudo systemctl start spamassassin
```

```
sudo dnf install epel-release
```

```
sudo dnf install spamass-milter
```

```
sudo systemctl start spamass-milter
```

```
sudo systemctl enable spamass-milter
```

Následně zeditujeme soubor `/etc/postfix/main.cf`, kde na konci souboru upravíme řádky, které nastaví pro Open DKIM a DMARC spolupráci se SpamAssassinem.

```
# Milter configuration
```

```
milter_default_action = accept
```

```
milter_protocol = 6
```

```
smtpd_milters =inet:127.0.0.1:8891,unix:/run/spamass-milter/spamass-milter.sock
```

```
non_smtpd_milters = $smtpd_milters
```

Předposledním krokem je odkomentování a přepsání řádku dle obrázku v souboru `/etc/sysconfig/spamass-milter`, tento krok slouží pro odmítnutí emailu, pokud bude jeho skóre vyšší, než 8.

```
## Override for your different local config if necessary
#SOCKET=/run/spamass-milter/spamass-milter.sock

## You may add configuration parameters here, see spamass-milter(1)
##
## Note that the -x option for expanding aliases and virtusertable entries
## only works if spamass-milter is run as root; you will need to use
## spamass-milter-root.service instead of spamass-milter.service if you
## wish to do this but otherwise it's best to run as the unprivileged user
## sa-milt by using the normal spamass-milter.service
EXTRA_FLAGS="-m -r 8 -R SPAM_ARE_NOT_ALLOWED_HERE -i 127.0.0.1 -g sa-milt"
```

Obrázek 15 – Nastavení skóre pro blokaci

Nakonec zrestartujeme služby Postfix a Spamass Milter pro aplikaci vytvořených změn.

```
sudo systemctl restart postfix spamass-milter
```

5.3.14 Nastavení a použití blacklist a whitelist

Pro implementaci blacklistu a whitelistu budeme editovat soubor `/etc/mail/spamassassin/local.cf`. Jako příklad pro nastavení blokace a povolení adres a domén povolíme adresu `rig***@google.com` a zablokujeme doménu `@seznam.cz`.

```
Whitelist_from rig***@google.com
```

```
Blacklist_from *@seznam.cz
```

Následně soubor uložíme, otestujeme, zda konfigurace neobsahuje syntaxové chyby a zrestartujeme SpamAssassina.

```
Sudo spamassassin -lint
```

Sudo systemctl restart spamassassin

```
Received: from unknown (::ffff:84.246.165.117)
  by email.seznam.cz (szn-ebox-5.0.103) with HTTP;
  Sun, 27 Feb 2022 11:38:16 +0100 (CET)
From: <[REDACTED]@seznam.cz>
To: <user1@ugcz.eu>,
  <user2@ugcz.eu>
Subject: qffwqf
Date: Sun, 27 Feb 2022 11:38:16 +0100 (CET)
Message-Id: <HYO.2exGP.4MaP4P{pNzm.1Y6rIO@seznam.cz}>
Mime-Version: 1.0 (szn-mime-2.1.20)
X-Mailer: szn-ebox-5.0.103
Content-Type: text/plain;
  charset=utf-8
Content-Transfer-Encoding: quoted-printable
```

Obrázek 16 – Doručený email od Mailer Daemon o blokaci zprávy z domény @seznam.cz

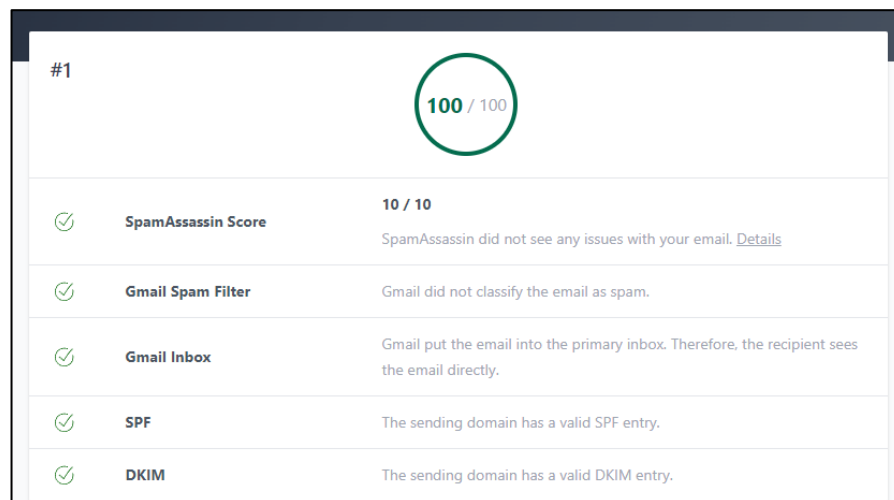
```
Mar 6 13:43:01 mail spamd[1562]: spamd: connection from ::1 [::]:56526 to port 783, fd 5
Mar 6 13:43:01 mail spamd[1562]: spamd: setuid to sa-milt succeeded
Mar 6 13:43:01 mail spamd[1562]: spamd: processing message <3YL.3Ikxd.1DN5j4oGRZa.1Y9AnJ@scif.cz> for sa-milt:985
Mar 6 13:43:05 mail spamd[1562]: spamd: identified spam (102.3/5.0) for sa-milt:985 in 3.9 seconds, 1818 bytes.
Mar 6 13:43:05 mail spamd[1562]: spamd: result: Y 102 - BODY_SINGLE_WORD, DKIM_SIGNED, DKIM_VALID, DKIM_VALID_AU, DKIM_VALID_EF, FREEMAS
Mar 6 13:43:05 mail postfix/cleanup[15717]: A14B91127ABC: milter-reject: END-OF-MESSAGE from mxdl.seznam.cz[77.75.78.210]: 5.7.1 S$
Mar 6 13:43:05 mail postfix/smtpd[15709]: disconnect from mxdl.seznam.cz[77.75.78.210] ehlo=2 starttls=1 mail=1 rcpt=1 data=0/1 qu$
```

Obrázek 17 – Log ze serveru o blokaci emailu z domény @seznam.cz

5.4 Otestování služeb a serveru

V této části jsou přiloženy printscreeny potvrzující funkčnost SpamAssassina, implementovaných metod a funkční odesílání a přijímání pošty v emailovém klientovi.

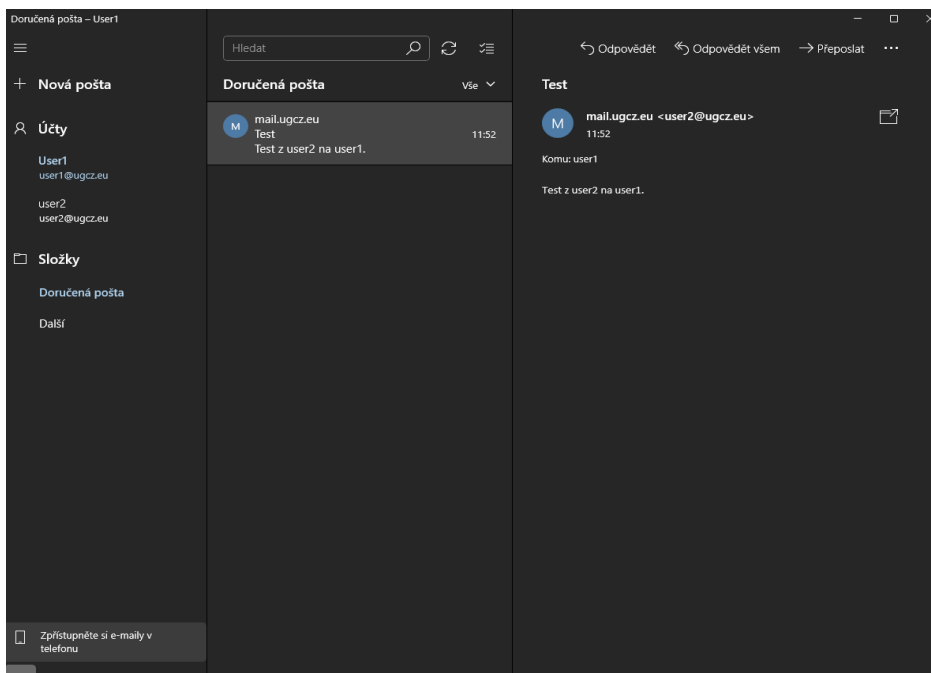
Následující printscreen zobrazuje test z internetové stránky dostupné na stránce <https://www.experte.com/spam-checker>, na které si lze otestovat mnoho dalších funkcí.



Obrázek 18 – Kontrola SpamAssassina, SPF a DKIM

ID zprávy	<61ec4165.1c69fb81.c690f.7822SMTPIN_ADDED_MISSING@mx.google.com>
Čas vytvoření:	22. ledna 2022 18:40 (Doručeno za -12 sekund)
Od:	user1 <user1@ugcz.eu>
Komu:	[REDACTED]
Předmět:	tewst
SPF:	Výsledek pro IP adresu 89.221.220.161: PASS Další informace
DKIM:	Výsledek pro doménu ugcz.eu: 'PASS' Další informace
DMARC:	'PASS' Další informace

Obrázek 19 – Potvrzení funkčnosti SPF, DKIM a DMARC z emailového klienta



Obrázek 20 – Potvrzení funkčnosti odesílání a přijímání pošty

6 Výsledky a diskuse

6.1 Výsledek práce

Výsledkem práce je nakonfigurovaný plně funkční emailový server s pokročilou ochranou proti internetovým hrozbám. Celkově s úplným postupem konfigurace byly splněny všechny požadavky na tuto práci v podobě použití operačního systému CentOS 8, implementace Postfix a Dovecot, nastavení SpamAssassina, implementace zvolených bezpečnostních metod, možné použití blacklistu a whitelistu, použití požadovaných emailových protokolů, získání zkušeností pro budoucí konfiguraci a je ověřeno, že je vybraný operační systém, metody a další rozšíření vhodné pro následnou konfiguraci testovacího serveru do armádního prostředí. Všechny implementované funkce a metody jsou plně funkční a lze emailový server dále upravovat a vylepšovat dle budoucích požadavků. Díky podrobnému rozebrání bezpečnostních rizik, které se mohou v emailu objevit, bude část této teorie použita při bezpečnostním školení uživatelů.

6.2 Diskuse

Hlavní otázkou na tento server je, jak dlouho vydrží být aktuálně zabezpečený. Svět informačních technologií se neustále posouvá vpřed. Náš emailový server je pro současnou dobu vhodně zabezpečený, i když je systém CentOS 8 již bez podpory, ale pro dobu své působnosti jako dočasný emailový server bude plnit svůj úkol, než bude vybrán a pořízen nový, pravděpodobně již i s externí podporou příslušné firmy.

Při volbě jiného operačního systému, který by měl zaručenou podporu na několik dalších let by byla tato konfigurace vhodnější a do budoucna použitelnější, CentOS 8 byl ale vybrán pro svou dlouholetou ověřenou stabilitu a možnosti konfigurace, což je pro armádní prostředí naprosto zásadní a vyhovující. Díky vhodnému zvolení všech částí se konfigurace serveru povedla dle očekávání a téměř bez jakýchkoliv problémů.

7 Závěr

Důležitými kroky pro nakonfigurování tohoto emailového serveru bylo zvolit správný postup implementace všech součástí, vhodné řešení v podobě poskytovatele virtuálního prostředí, aby bylo možné provést veškerou požadovanou konfiguraci, nastavení, veškeré potřebné služby a bezpečnostní politiky pro funkční, a především bezpečný emailový server.

V bezpečnostní otázce pro ochranu serveru byl použit SpamAssassin, Firewalld a pro ochranu emailové komunikace a důvěryhodnost serveru byly zvoleny metody SPF, DKIM, DMARC a naimplementováno šifrování SSL/TLS.

V teoretické části práce byl velmi stručně popsán princip fungování, respektive jeho hlavní součásti pro komunikaci. Podstatnou částí teoretické části byla bezpečnost, kde byly rozebrány metody a bezpečnostní prvky použité v praktické části práce a došlo i na velký rozbor bezpečnostních rizik, se kterými se lze ve světě emailové komunikace setkat.

V praktické části je přesný postup se všemi příkazy a potřebnými informacemi pro konfiguraci a nastavení serveru. Nejprve došlo na základní nastavení prostředí, následně na instalaci a konfiguraci Postfixu. Dále byl nakonfigurován firewall, TLS certifikát a certifikační bot, který je nutný pro získání certifikátu, Apache server a Dovecot. Následně byly vytvořeny testovací účty sloužící pro nastavení serveru, otestování funkčnosti komunikace a po konfiguraci bezpečnostních metod i jejich funkčnost. Následovalo nakonfigurování SpamAssassina a nastavení blacklistu a whitelistu, které jsou jeho součástí. Na závěr nechybí printscreeny potvrzující funkčnost všech zvolených bezpečnostních metod a funkční emailové komunikace z poštovního klienta.

8 Seznam použitých zdrojů

1. *Jak na Internet* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.jaknainternet.cz/page/1750/e-mail/>
2. SYSADMIN. *Mail terminology* [online]. 03.2019 [cit. 2022-02-11]. Dostupné z: <https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mda-smtp-dkim-spf-dmarc>
3. FRUHLINGER, Josh. *What is SSL, TLS? And how this encryption protocol works* [online]. 04.12.2018 [cit. 2022-02-11]. Dostupné z: <https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html>
4. *SSL/TLS certifikáty* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.sslmarket.cz/ssl/certifikaty>
5. GAFETY. *9 tips to protect your business's mail server* [online]. 17.03.2021 [cit. 2022-02-11]. Dostupné z: <https://gatefy.com/blog/tips-protect-your-mail-server/>
6. *What is SPF?* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.agari.com/spf/>
7. *What is SPF?* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.proofpoint.com/us/threat-reference/spf>
8. *SPF* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.cesky-hosting.cz/pro-zakazniky/napoveda/spf.html>
9. *What Is DKIM?* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.sparkpost.com/resources/email-explained/dkim-domainkeys-identified-mail/>
10. RICE, Shane. *DKIM: What is it and why is it important?* [online]. 09.02.2021 [cit. 2022-02-11]. Dostupné z: <https://postmarkapp.com/guides/dkim>
11. TEAM, SendGrid. *What Is DMARC? Understanding DMARC Records* [online]. 04.03.2020 [cit. 2022-02-11]. Dostupné z: <https://sendgrid.com/blog/what-is-dmarc/>
12. DOMANTAS, G. *What is a PTR Record and How to Do Reverse IP Lookup?* [online]. 09.03.2021 [cit. 2022-02-11]. Dostupné z: <https://www.hostinger.com/tutorials/what-is-a-ptr-record-and-how-to-do-reverse-ip-lookup>
13. KRČMÁŘ, Petr. *Co je to reverzní záznam (PTR) a jak ho nastavit?* [online]. 26.06.2017 [cit. 2022-02-11]. Dostupné z: <https://blog.vpsfree.cz/co-je-to-reverzni-zaznam-ptr-a-jak-ho-nastavit/>
14. ZOLA, Andrew. *Spam filter* [online]. [cit. 2022-02-11]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/spam-filter>
15. *What is SpamAssassin? - Meaning* [online]. [cit. 2022-02-11]. Dostupné z: <https://sendpulse.com/support/glossary/spamassassin>
16. *Apache / spamassassin* [online]. [cit. 2022-02-11]. Dostupné z: <https://github.com/apache/spamassassin>
17. *Rspamd* [online]. 21.05.2018 [cit. 2022-02-11]. Dostupné z: <https://alternativeto.net/software/rspamd/about/>
18. GATEFY. *7 most common types of email spam* [online]. 18.03.2021 [cit. 2022-02-14]. Dostupné z: <https://gatefy.com/blog/most-common-types-email-spam/>
19. *Největší emailové hrozby pro firmy* [online]. 17.09.2019 [cit. 2022-02-14]. Dostupné z: <https://www.itsec-nn.com/nejvetsi-emailove-hrozby-pro-firmy/>
20. *Ochrana počítače před ransomwarem* [online]. [cit. 2022-02-14]. Dostupné z: <https://support.microsoft.com/cs-cz/windows/ochrana-po%C4%8D%C3%ADta%C4%8De-p%C5%99ed-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3>

21. BURT, Tom. *New action to disrupt world's largest online criminal network* [online]. 10.03.2020 [cit. 2022-02-14]. Dostupné z: <https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/>
22. *Co je malware?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.mcafee.com/cs-cz/antivirus/malware.html>
23. *Co je spyware?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.avast.com/cs-cz/c-spyware>
24. *Co je to adware?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.avast.com/cs-cz/c-adware>
25. *Co je phishing?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.avast.com/cs-cz/c-phishing>
26. *Co je to Trojský kůň?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.avast.com/cs-cz/c-trojan>
27. *Co je počítačový červ?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.avast.com/cs-cz/c-computer-worm>
28. PAYNE, Kevin a Daphne FOREMAN. *8 Common Bank Scams (And How To Avoid Them)* [online]. 19.02.2021 [cit. 2022-02-14]. Dostupné z: <https://www.forbes.com/advisor/banking/common-bank-scams-and-how-to-avoid-them/>
29. *Banking Scams* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.gfsc.gg/consumers/scams/banking-scams>
30. *SEXTORTION - Vás systém byl napaden virem. Vase zařízení bylo úspesne hacknuto (20210221)* [online]. 21.02.2021 [cit. 2022-02-14]. Dostupné z: <https://www.hoax.cz/scam419/sextortion---vas-system-by-l-napaden-virem-vase-zarizeni-bylo-úspesne-hacknuto-20210221/>
31. *What is a spoofing attack?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.malwarebytes.com/spoofing>
32. DEDENOK, Roman. *Email spoofing: how attackers impersonate legitimate senders* [online]. 03.06.2021 [cit. 2022-02-14]. Dostupné z: <https://securelist.com/email-spoofing-types/102703/>
33. *Nastavení zabezpečeného protokolu POP3S , SMTPS a IMAPS* [online]. [cit. 2022-02-14]. Dostupné z: <https://napoveda.czechia.com/clanek/nastaveni-zabezpeceneho-protokolu-pop3s-smtps-a-imaps/>
34. *What is IMAPS and IMAP over STARTTLS?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.gordano.com/knowledge-base/what-is-imaps-and-imap-over-starttls/>
35. WILSON, John. *SMTPS: How to Secure SMTP with SSL/TLS (Which Port to Use)* [online]. 11.11.2021 [cit. 2022-02-14]. Dostupné z: <https://www.agari.com/email-security-blog/smtps-how-to-secure-smtp-with-ssl-tls-which-port-to-use/>
36. *POP3, POP3S filter* [online]. 28.11.2019 [cit. 2022-02-14]. Dostupné z: https://help.eset.com/eis/12/cs-CZ/idh_config_epfw_scan_pop3.html
37. JELÍNEK, Lukáš. *Stavíme poštovní server – 2 (Dovecot)* [online]. 19.10.2009 [cit. 2022-02-14]. Dostupné z: <https://www.abclinuxu.cz/clanky/site/stavime-postovni-server-2-dovecot>
38. *DOVECOT The Secure IMAP server* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.dovecot.org/>
39. *Courier IMAP Alternatives* [online]. 30.08.2017 [cit. 2022-02-14]. Dostupné z: <https://alternativeto.net/software/courier-imap/>
40. JELÍNEK, Lukáš. *Stavíme poštovní server – 1 (Postfix)* [online]. 12.10.2009 [cit. 2022-02-14]. Dostupné z: <https://www.abclinuxu.cz/clanky/site/stavime-postovni-server-1-postfix>

41. MCDONALD, Alistair, Carl TAYLOR, David RUSENKO, Ian HAYCOX, Magnus BACK, Patrick BEN KOETTER a Ralf HILDEBRANDT. *Linux Email: Set up, maintain, and secure a small office e-mail server*. 2009 [cit. 2022-02-16]. ISBN 9781847198648.
42. *What is Sendmail?* [online]. [cit. 2022-02-14]. Dostupné z: <https://www.proofpoint.com/us/threat-reference/sendmail>
43. KILI, Aaron. *7 Best Mail Transfer Agents (MTA's) for Linux* [online]. 02.08.2021 [cit. 2022-02-14]. Dostupné z: <https://www.tecmint.com/best-mail-transfer-agents-mta-for-linux/>
44. PLESKY, Elvis. *Postfix vs Sendmail vs Exim* [online]. 25.06.2021 [cit. 2022-02-14]. Dostupné z: <https://www.plesk.com/blog/various/postfix-vs-sendmail-vs-exim/>