



Универзитет „Св. КИРИЛ И МЕТОДИЈ“ во Скопје
**ФАКУЛТЕТ ЗА ЕЛЕКТРОТЕХНИКА И
ИНФОРМАЦИСКИ ТЕХНОЛОГИИ**

СЕМИНАРСКА РАБОТА

Предмет:

БЕЗБЕДНОСТ И ЗАШТИТА НА КОМЈУТЕРСКО КОМУНИКАЦИСКИ СИСТЕМИ И МРЕЖИ

Тема:

„БЕЗБЕДНОСТ НА ЕЛЕКТРОНСКА ПОШТА”

Ментор:

Проф. д-р Данијела Ефнушева

Изработиле:

Ангела Настовска 98/2022

Борјан Петревски 106/2022

Моника Стоилковска 112/2022

СОДРЖИНА

I. ВОВЕД	4
II. ИСТОРИЈА НА ЕЛЕКТРОНСКА ПОШТА - Од научна фантастика до секојдневие.....	5
II.I Првите идеи и експерименти 1950 – 1965	5
II.II Почеток на мрежна е-пошта	6
II.III Стандардизација на протоколи и формати (1980-ти).....	7
II.IV Демократизација и достапноост на е-пошта (1990-ти)	8
III. БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ И ПРВИ НАПАДИ	9
III.I Први познати злоупотреби и напади.....	9
III.II Еволуција на заканите фишинг, малициозен софтвер и социјален живот	10
III.III Географско и техничко потекло на нападите	10
III.IV Последици и влијание врз довербата	10
IV. СТРУКТУРА И ФОРМАТ	12
V. ТЕХНИЧКА АРХИТЕКТУРА И ФУНКЦИОНАЛЕН МОДЕЛ ОСНОВА ЗА БЕЗБЕДНОСНА АНАЛИЗА	14
V.I Архитектура на интернет пошта според RFC 5598	14
VI. ВИДОВИ ЗАКАНИ	20
VI.I Фишинг	20
VI.II Спеар-фишинг.....	22
VI.III Бизнис компромитација на електронска пошта (BEC).....	23
VI.IV Рансомвер преку е-пошта	23
VI.V Злонамерни прилози и измама со адреса (Malicious Attachments и Email Spoofing).....	24
VII. ОСНОВНИ ЦЕЛИ НА БЕЗБЕДНОСТА.....	27
VIII. МЕХАНИЗМИ ЗА ЗАШТИТА ОД Е-MAIL НАПАДИ	29
VIII.I Secure/Multipurpose Internet Mail Extensions (S/MIME)	29
VIII.II Pretty Good Privacy (PGP)	31
VIII.II.I Шифрирање на е-пошта пораки	33
VIII.II.II Верификација со дигитален потпис	33

VIII.II.III	Шифрирање на датотеки	34
VIII.III	Sender Policy Framework (SPF)	34
VIII.IV	DomainKeys Identified Mail (DKIM).....	35
VIII.V	Domain-based Message Authentication, Reporting & Compliance (DMARC).....	37
VIII.VI	BIMI (Brand Indicators for Message Identification).....	38
VIII.VII	AI Spam Filtering	41
IX.	СТУДИИ НА СЛУЧАИ И ПРАКТИЧНИ ПРИМЕРИ ОД ОБЛАСТА НА САЈБЕР – БЕЗБЕДНОСТА	43
IX.I	Фишингот како закана во сајбер-безбедноста: Случајот со Yahoo breach.....	43
IX.II	Фишинг закани кон Gmail и одбранбените механизми на Google	45
IX.III	Фишинг напади во банкарскиот сектор во Македонија: Примери од Охридска банка и Комерцијална банка	47
X.	СОВЕТИ ЗА КРАЈНИ КОРИСНИЦИ ПРИ ЗАШТИТА ОД ФИШИНГ НАПАДИ.....	49
X.I	Како да ги препознаете фишинг нападите	49
X.II	Што да направите ако сте цел на фишинг напад	50
X.III	Password менаџери и добри практики за лозинки	51
XI.	ПРЕДИЗВИЦИ И ИДНИ НАСОКИ	53
XI.I	Напредни фишинг техники (deepfake, AI-generated email).....	53
XI.II	Email security automation (SOAR, SIEM поврзување)	54
XII.	ЗАКЛУЧОК	56
XIII.	РЕФЕРЕНЦИ	58

I. *ВОВЕД*

Во ерата на технолошка трансформација, каде што дигиталната комуникација се развива со брзина на светлината, електронската пошта останува непроменет столб на секојдневната размена на информации. Покрај појавата на современи платформи за комуникација, е-поштата продолжува да биде клучен медиум и технолошка алатка со широка примена, од неформални пораки до доверливи деловни и институционални дописи.

Безбедноста на електронската пошта во таков контекст не претставува само техничка дисциплина, туку и прашање од суштинско значење за довербата, интегритетот и стабилноста на глобалната комуникациска мрежа. Како што истакнува Verizon ^[1], „*е-поштата е далеку од застарена – таа е најуспешниот вектор за софистицирани сајбер напади во модерниот свет на закани.*“. Со анализа на статијата добиваме одговор за прашања кои се вечна мистерија и кои не само што го нагласува ризикот, туку и ја дефинираат вистинската тежина на темата.

Спроведени истражувања укажуваат на разновидни пристапи кон заштитата на електронската пошта – од примена на криптографија (S/MIME, PGP) и DNS-базирани механизми (SPF, DKIM), до машинско учење за откривање фишинг и злоупотреби. Сепак, постои очигледна празнина помеѓу теоретската подготвеност и практичната примена на безбедносните мерки, особено во контекст на зголемената употреба на вештачка интелигенција за автоматизирани напади.

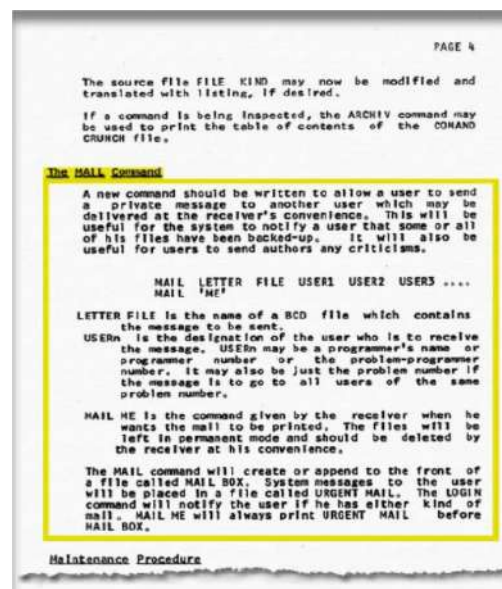
Оваа семинарска работа има за цел да ги истражи токму тие празнини и да обезбеди структурирана анализа на безбедносните предизвици со кои се соочува електронската пошта денес. Преку критички осврт на релевантна литература, споредба на пристапи и разгледување на современи технологии за заштита, ќе се даде јасна слика за важноста и потребата од систематско зајакнување на е-поштата како комуникациска основа во дигиталниот свет.

II. ИСТОРИЈА НА ЕЛЕКТРОНСКА ПОШТА - Од научна фантастика до секојдневие

II.I Првите идеи и експерименти 1950 – 1965

Електронската пошта денес е еден од најчесто користените алати за комуникација во светот кој има длабоки корени кои се протегаат децении наназад. Пред да стане стандардна форма на деловна и лична размена на информации, нејзиниот развој поминал низ етапи на научни иновации, воени истражувања и генијални поединци кои ја поставиле основата за она што денес го нарекуваме „е-маил“.

Во доцните 1950-ти и раните 1960-ти години, кога компјутерите сè уште претставувале привилегија исклучиво на истражувачките институции, воените установи и универзитетските центри, се појавуваат првите замисли за развој на дигитални средства за комуникација меѓу корисници. Во тој историски контекст започнува да се кристализира концептот за испраќање текстуални пораки преку компјутерски системи што во своето време бил оценет како исклучително иновативен и револуционерен пристап. Еден од првите и најзначајни чекори во оваа насока бил направен во 1961 година на Масачусетскиот институт за технологија (MIT), со развојот на системот CTSS (Compatible Time-Sharing System). Оперативен систем кој овозможувал истовремено користење на еден компјутер од страна на повеќе корисници преку терминали, што претставувало вистински пресврт во начинот на интеракција човек–машина. Во рамки на CTSS во 1965 година истражувачите Том Ван Влек (Tom Van Vleck) и Ноел Морис (Noel Morris) ја креирале командата „MAIL“ прикажана на Слика 1 која овозможува еден корисник да остави порака за друг, со тоа што пораката се зачувува во посебна датотека во неговиот директориум. Иако оваа размена била ограничена на корисници на истиот компјутер, сепак преставувала првата практична реализација на концептот на електронско испраќање. Секоја порака во суштина,

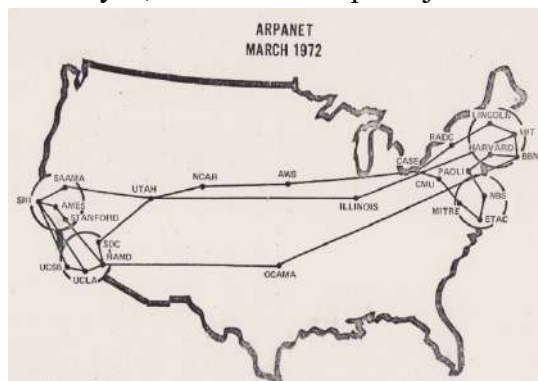


Слика 1. Команда „MAIL“

функционирала како „белешка“ оставена за неког да ја прочита подоцна, што претставува протоформа на она што денес го препознаваме како е-пошта. Ова решение колку и да било технолошки ограничено во тогашните рамки, го трасира патот за идниот развој на меѓусебно поврзани компјутерски мрежи и ја отвора вратата за современите комуникациски платформи. Преку CTSS, не само што се реализира основната идеја на дигитална порака, туку се поставуваат и темелите за важни концепти како што се корисничка автентикација, контрола на пристап до податоци и приватност во дигиталниот простор, што претставуваат аспекти кои денес се клучни во електронската комуникација.

II.II Почеток на мрежна е-пошта

Во годините што следат, ентузијазмот за интеркомпјутерска комуникација се зголемува, особено со развојот на првата глобално распознаена компјутерска мрежа



Слика 2. Географска распределба на ARPANET
март 1972 година

ARPANET (Advanced Research Projects Agency Network), која претставувала експериментален проект финансиран од американската агенција ARPA [2]. Целта на ARPANET е да поврзе различни универзитетски и воени компјутерски системи (слика 2), за побрза размена на информации и ресурси, поставувајќи ја основата за она што подоцна ќе прерасне во Интернетот.

Во рамки на оваа мрежа, клучен историски момент се случува во 1971 година, кога Ray Tomlinson, инженер од компанијата BBN Technologies, ја испраќа првата електронска порака преку мрежа помеѓу два физички различни компјутери. Тој ја модифицира постоечката програма SNDMSG и ја комбинира со CPYNET, што овозможува трансфер на пораки од еден систем до друг преку ARPANET.



Слика 3. Реј Томлинсом и знаком „@“

Иако содржината на првата порака не е документирана (подоцна Tomlinson изјавува дека била нешто безначајно „QWERTYUIOP“), нејзиното значење е длабоко бидејќи таа

претставува моментот на раѓање на модерната електронска пошта. Најголемата иновација во тој чин не е самата испратена порака, туку воведувањето на симболот „@“, кој Tomlinson го користи за да го раздвојува името на корисникот од името на компјутерот. Со тоа, тој го воспоставува денешниот стандардизиран формат на е-адреса `user@host`, кој со децении останува непроменет и препознатлив симбол на дигиталната ера [3]. Симболот @ во англискиот јазик означува „на“ (at), со што јасно се пренесува пораката – „корисник на компјутер“. До 1973 година, е-поштата не само што опстанува како функционалност, туку станува најкористената и најзначајна апликација во рамки на ARPANET, зафаќајќи повеќе од 75% од целиот мрежен сообраќај. Ова е показател за тоа колку корисна и трансформативна станала електронската комуникација во академски и истражувачки кругови. Таа не само што ја забрзува размената на идеи и информации, туку го трансформира начинот на кој се гради научната соработка, проширувајќи ја нејзината употреба во поширок општествен и деловен контекст. Брзиот технолошки прогрес повикува на потребата од подобри алатки за интеракција со пораките. Поради тоа во 1975 година се развива MSG програмата која претставува еден од првите интерфејси за управување со електронска пошта, кој овозможува корисниците не само да испраќаат и примаат пораки, туку и да ги читаат, прегледуваат, архивираат или бришат. Со тоа MSG ја приближува е-поштата до крајниот корисник, воведувајќи концепти на „inbox“ и „message status“, кои подоцна би станал стандарден дел од секоја поштенска платформа во годините што следат. Оваа програма ја проширува електронската пошта од техничка функција во целосно комуникациско искуство, подготвувајќи ја сцената за идниот глобален бум на дигиталната размена на информации.

II.III Стандардизација на протоколи и формати (1980-ти)

Со растечката употреба на е-поштата во академските и воените кругови, се јавува неопходноста од воспоставување на унифицирани протоколи за нејзино функционирање во се поширока мрежна средина. Во таа насока, 1982 година претставува пресвртна точка со воведувањето на SMTP (Simple Mail Transfer Protocol) – протокол кој овозможува ефикасно испраќање и пренос на пораки помеѓу поштенски сервери преку интернет. SMTP станува основата на сите последователни е-пошта системи и овозможува глобална интероперабилност меѓу различни домени и платформи. Паралелно со SMTP, се развива и

стандардизација на форматот на пораките. Преку документите RFC (Request for Comments), IETF (Internet Engineering Task Force) поставува јасни спецификации за структурата на е-поштата – вклучувајќи заглавие (header), тело (body), и MIME екстензии (Multipurpose Internet Mail Extensions), кои од 1988 година овозможуваат прикачување слики, документи, па дури и аудио и видео содржини во формат кој е објаснет во заглавје IV .

II.IV Демократизација и достапност на е-пошта (1990-ти)

Втората половина на 1990-тите години претставува пресвртница во историјата на електронската пошта, бидејќи нејзината употреба излегува надвор од научно



Слика 4. Еволуција на Е-маил

истражувачките и воените кругови, влегувајќи во пошироката јавна и комерцијална сфера. Ова е овозможено преку појавата и експанзијата на World Wide Web и сè поголемата достапност на Интернет сервис провајдери (ISP) кои понудуваат пристапни решенија за домашни корисници. Еден од најзначајните чекори во процесот Демократизација и достапност на е-пошта (1990-ти) е појавата на веб базирани е-пошта сервиси како што се Hotmail (1996), Yahoo Mail (1997) и подоцна Gmail (2004), кои овозможуваат глобално достапна платформа и независна е-пошта преку стандардизиран веб прелистувач. Овие сервиси го елиминираат потребниот технички праг за користење на е-пошта,

проширувајќи ја достапноста кон пошироки категории на корисници. Во корпоративниот сектор имплементацијата на локални поштенски клиенти како Microsoft Outlook, Lotus Notes и Novell GroupWise овозможува длабока интеграција на е-поштата со други деловни процеси и ресурси како што се календарски системи, бази на податоци, споделени документи и организациска интранет комуникација. Со тоа електронската пошта се поставува како централна алатка во рамките на дигиталната трансформација на деловните субјекти поставувајќи го темелот за денешниот концепт на овозможена и подржана комуникација и информациски системи базирани на електронска размена.

III. БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ И ПРВИ НАПАДИ

Со појавата и ширењето на електронската пошта како доминантен медиум за комуникација во академските, деловните и личните сфери, се јавува и зголемена потреба за заштита на интегритетот, доверливоста и достапноста на податоците кои се разменуваат преку овој канал. Покрај првичната намена на е-поштата која била позитивно насочена кон олеснување и забрзување на комуникацијата, со текот на времето таа станува мета на бројни злоупотреби вклучувајќи несакана пошта, фишинг, малициозен софтвер и социјален инженеринг.

III.I Први познати злоупотреби и напади

Еден од најраните документиран напади поврзани со компјутерски мрежи кој индиректно го користел концептот на електронска порака е познатиот Morris Worm од 2 ноември 1988 година, креиран од Роберт Тапан Морис кој имал само 23 години, студент на Универзитетот Корнел во САД. Неговата примарна намера не била деструктивна, но овој компјутерски црв се проширил преку SMTP (Simple Mail Transfer Protocol) механизми и предизвикал сериозно преоптоварување на системите поврзани на ARPANET, што го позиционира како еден од првите алармантни настани поврзани со безбедноста на електронската пошта [4]. Црвот се пренесува од еден уред на друг преку експлоатирање на чести безбедносни слабости во оперативните системи. Првично бил дизајниран за истражување на структурата на интернет врските помеѓу уредите, но наскоро добил сосема поинаков карактер кога биле откриени грешки во кодот. Некои од овие грешки го претворија црвот во опасна мрежна закана, предизвикувајќи непредвидлива и мајорна штета која се шири случајно и неконтролирано [5]. Во почетокот на 1990-тите започнуваат да се појавуваат првите масовни комерцијални пораки испратени без согласност кои денес се познати под терминот несакана пошта. Најистакнат пример е случајот Green Card Spam од 1994 година, кога адвокатска канцеларија во САД испраќа илјадници пораки преку Usenet групи со што се отвора нова димензија на дигитално рекламирање и несакана пошта [6].

III.II Еволуција на заканите фишинг, малициозен софтвер и социјален живот

Во втората половина на 1990-тите и раните 2000-ти години се јавуваат посоефицирани облици на злоупотреба вклучувајќи фишинг напади кои најчесто се претставуваат како легитимни известувања од банкарски институции, онлајн платформи и владини агенции, при што целта е измама на корисниците за да откријат доверливи податоци преку лажни веб страници. При овие напади се користат тактики како лажно прикажување на испраќачот (e-mail spoofing), користење на скриени линкови кои водат кон фалсификувани страници (link obfuscation) и прикачени фајлови кои содржат малициозен код, тројанци, keyloggers или ransomware.

III.III Географско и техничко потекло на нападите

Првичните напади главно потекнуваат од технолошки напредни земји како САД и Западна Европа, каде што постоела развиена мрежна инфраструктура и пристап до информатички ресурси. Со текот на времето, главните извори на фишинг и несакана пошта се префрлаат кон земји со поопуштени регулативи и ограничена правна контрола како што се Русија, Кина, Романија, Нигерија и Бразил. Нападите во голема мера се потпираат на botnets, односно групи на компромитирани компјутери координирани за испраќање на милиони пораки во исклучително краток временски интервал. Мотивациите зад овие напади се разновидни, вклучувајќи финансиски измами, кражба на идентитет и политички мотивирани сајбер најбудувања. Спроведувањето на фишинг кампањи насочени кон финансиски институции или државни органи ја потврдува важноста на електронската пошта како критичен комуникациски механизам.

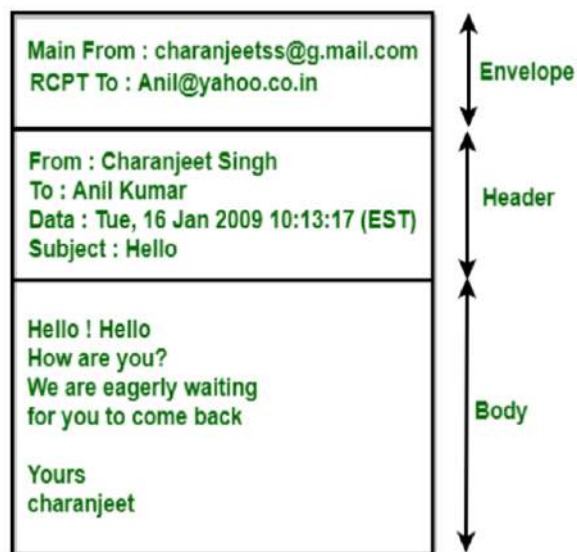
III.IV Последици и влијание врз довербата

Зголемената зачестеност на напади ја доведува во прашање доверливоста и кредибилитетот на електронската пошта како комуникациски медиум. Според податоци од истражувања на глобално реномирани безбедносни компании како Symantec, Kaspersky и Cisco Talos Intelligence Group, околу 85% од вкупниот сообраќај преку е-пошта во одредени периоди може да се класифицира како спам или потенцијална закана. Овој факт ги

принудува организациите и интернет провајдерите да инвестираат во напредни безбедносни решенија и филтри. За да навлеземе детално во безбедноста на е-пошта ќе се разгледаат техничките механизми и протоколи кои се воведуваат како одговор на овие предизвици, вклучувајќи SPF, DKIM, DMARC, TLS енкрипција, антиспам филтри и современи концепти како Zero Trust пристапот во електронските поштенски системи.

IV. СТРУКТУРА И ФОРМАТ

Електронската пошта претставува стандардизиран начин за испраќање и примање на текстуални пораки, кои можат да содржат и мултимедијални прилози. Нејзината структура е дефинирана според протоколи како што се SMTP, IMAP и POP3 преку кои се овозможува интероперабилност помеѓу различни системи и платформи. Разбирањето на структурата на еден е-маил е основа за анализа на безбедноста, автентичноста и потенцијалните злоупотреби. Од Слика 5 форматот на е-пораката се состои од три главни сегменти: заглавје (header), тело на пораката (body) и писмо (envelope).



Слика 5. Формат на Е-порака

Заглавјето содржи мета информации за пораката односно детали кои го дефинираат нејзиното потекло, дестинација и контекст на испраќање [7].

Клучните полиња се:

From: адреса на испраќачот.

To: адреса на примачот.

Cc/Bcc: адреси за копија и скриена копија.

Subject: насловот или темата на пораката.

Date: времето на испраќање.

Message-ID: уникатен идентификатор за пораката.

Received: низата сервери низ кои поминала пораката.

Овие податоци се клучни за форензичка анализа, откривање на фишинг напади и проверка на спуфирани адреси. Безбедносните филтри често ја анализираат токму оваа секција.

Телото на пораката ја има главната содржина на пораката која корисникот ја чита. Може да биде во plain text или HTML формат. Ако се користи HTML, пораката може да

содржи линкови, слики и форматиран текст, но токму тука често се крие малициозен код што ја прави оваа секција подложна на злоупотреба. Поради ова, многу клиенти на е-пошта дозволуваат исклучување на HTML приказ или вградување на sandbox механизми. Токму тука најчесто се формулира социјалниот инженеринг преку лажни известувања, итни пораки или повици на акција.

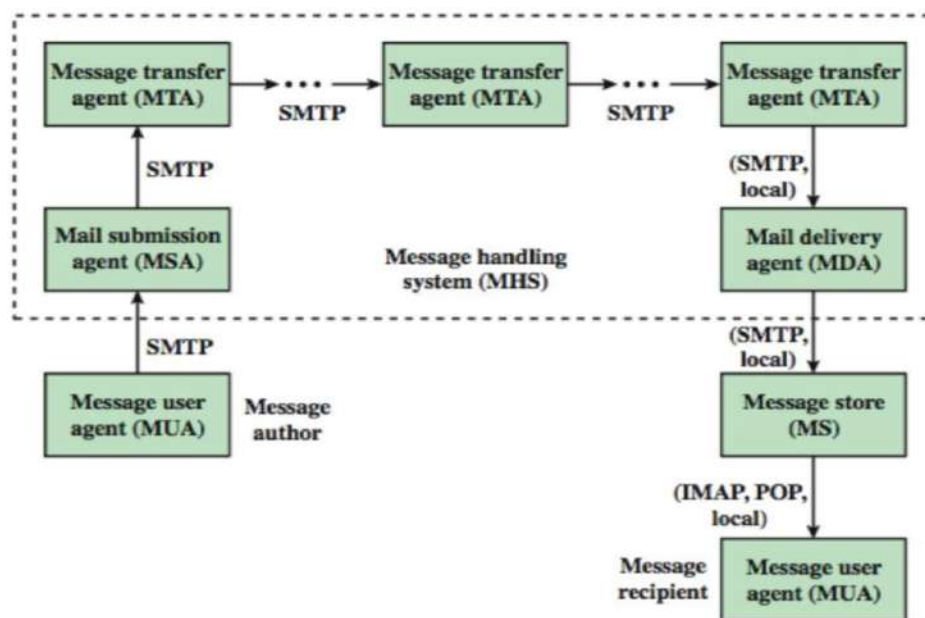
Покрај заглавјето и телото една важна, но често невидлива компонента на е-пораката е т.н. „**Envelope**“ (**Писмо**). Како што е прикажано на слика 5, писмо делот содржи технички информации за преносот на пораката како што се MAIL FROM и RCPT TO. Овие полиња се користат од страна на SMTP серверите за рутирање и испорака на пораката, но не се задолжително прикажани во самата е-пошта што ја гледа корисникот.

V. ТЕХНИЧКА АРХИТЕКТУРА И ФУНКЦИОНАЛЕН МОДЕЛ ОСНОВА ЗА БЕЗБЕДНОСНА АНАЛИЗА

Во контекст на современите закани и растечките безбедносни предизвици поврзани со електронската пошта, суштински е значајно да се започне со систематско разбирање на начинот на кој функционира овој комуникациски систем. Пред да може да се анализираат слабостите и да се предложат ефективни мерки за заштита, мора темелно да се познава техничката основа, архитектурата, протоколите и патот на пораката при нејзиното движење низ мрежата. Заштитата од нападите не може да се заснова само на реактивни мерки, таа бара проактивен пристап кој вклучува детална анализа на секоја точка на можен компромис во процесот на испраќање, пренос, достава и складирање на електронските пораки [8]. Без разбирање на механизмите преку кои функционираат компонентите како што се Mail Transfer Agent (MTA), Mail Delivery Agent (MDA) и DNS-от, невозможно е да се утврдат каде најчесто се случуваат напади и кои заштитни протоколи треба да бидат имплементирани.

V.I Архитектура на интернет пошта според RFC 5598

Вовед во оваа архитектура обезбедува документот RFC 5598, издаден од страна на Internet Engineering Task Force (IETF), кој претставува референтна рамка за дизајн, развој и анализа на инфраструктурата за електронска пошта. Разбирањето на овој архитектонски модел е фундаментално за секоја безбедносна анализа, бидејќи овозможува идентификација на потенцијалните ранливости и критични точки на напад во поштенската комуникација. Документот RFC 5598 го дефинира логичкиот и функционален модел на електронската пошта преку Интернет, вклучувајќи ја улогата на сите релевантни протоколи и компоненти. Овој модел ги опфаќа протоколите SMTP (Simple Mail Transfer Protocol) за пренос на пораки, POP3 (Post Office Protocol) и IMAP (Internet Message Access Protocol) за пристап до поштенски сандачиња, како и MIME (Multipurpose Internet Mail Extensions) за мултимедијални прилози. Според RFC 5598, пораката минува низ повеќе логички и физички модули при своето патување од испраќачот до примачот, што создава повеќе точки на можен компромис од безбедносна перспектива [9].



Слика 6. Интернет архитектура на порака

Mail User Agent, или скратено MUA, претставува крајниот софтверски интерфејс со кој корисникот директно комуницира при користење на системот за електронска пошта. Тоа е апликацијата што му овозможува на корисникот да ги создава, уредува, испраќа и прима електронски пораки. Во пракса, MUA може да биде десктоп апликација како што се



Слика 7. Процес на праќање и примање на Е-пошта

Microsoft Outlook или Mozilla Thunderbird, мобилна апликација или веб базиран клиент како Gmail или Yahoo! Mail. Основната функција на овој агент е да овозможи интуитивен и прегледен начин за управување со електронската пошта, при што корисникот може да внесува текст, да

прикачува датотеки, да специфицира примачи и да ја форматира пораката според потребите. Кога ќе се креира пораката MUA ја иницира комуникацијата со Mail Submission Agent (MSA) за нејзино испраќање користејќи ги стандардните SMTP протоколи. Исто така, за прием на пристигнати пораки MUA користи протоколи како IMAP или POP3 за да се поврзе со Message Store, од каде ги вчитува пораките и ги прикажува на корисникот во

читлив формат. Освен овие функционалности, MUA има значајна улога и во безбедноста на комуникацијата. Бидејќи претставува точка на прв контакт со потенцијално малициозни пораки, оваа компонента е честа цел на фишинг напади, малициозни прилози и напади преку вградени скрипти. Затоа современите MUA решенија се опремени со антифишинг механизми, проверки за валидност на прикачените документи, sandbox системи за отворање сомнителни пораки како и визуелни предупредувања за корисникот. Ваквата синергија помеѓу функционалност и безбедност го прави MUA основна и незаменлива компонента во поштенската архитектура.

Mail Submission Agent е компонентата која ја прима испратената порака од страна на корисничката апликација односно MUA и се грижи таа да биде правилно обработена и проследена до следниот модул во архитектурата – Mail Transfer Agent (Слика 6). Оваа компонента дејствува како посредник кој ги спроведува клучните чекори на проверка и валидација на пораката. Првичната обработка вклучува автентикација на испраќачот преку SMTP AUTH механизам кој овозможува идентификација и превенција од злоупотреба на услугата за испраќање. Понатаму MSA ја проверува синтаксата на е-поштата, нејзината структура и согласноста со стандардите за форматирање, вклучувајќи правила поставени од одредени домени или организациски политики. Откако ќе се потврди дека пораката е легитимна таа се проследува кон MTA за понатамошна испорака [10]. Безбедносната важност на MSA е огромна бидејќи лошо конфигурирана инстанца може да дејствува како потенцијална ранливост што хакерите можат да го злоупотребат за испраќање на спам пораки или дистрибуција на малициозен сообраќај. Стандардна практика е користење на TLS за шифрирање на комуникацијата, дефинирање на дозволени IP опсези, како и примена на политики за ограничување на пристап. Од суштинско значење е администрацијата на MSA да биде одговорно спроведена со цел да се зачува сигурноста и доверливоста на поштенскиот систем.

Mail Transfer Agent (MTA) претставува централна компонента во архитектурата на интернет е-поштата и има клучна улога во преносот на пораки меѓу поштенските сервери. Откако пораката ќе биде креирана од страна на корисникот преку Mail User Agent (MUA) и ќе биде пренесена до Mail Submission Agent (MSA), таа продолжува да се движи низ мрежата токму преку MTA (Слика 6). Тоа делува како поштенски дистрибутер кој ја презема

пораката и го координира нејзиниот пренос до дестинацискиот домен, односно до серверот што му припаѓа на примачот. Функционирањето на МТА се базира на протоколот SMTP (Simple Mail Transfer Protocol), кој овозможува размена на пораки преку IP базирана мрежа. МТА го користи DNS (Domain Name System) за да ја определи IP адресата на поштенскиот сервер на доменот на примачот со проверка на MX (Mail Exchange) записите. Откако ќе го идентификува вистинскиот сервер, МТА воспоставува конекција и ја пренесува пораката. Во повеќето од случаите една порака не оди директно од испраќач до примач, па затоа таа минува низ повеќе МТА сервери особено кога се работи за различни домени, интернационален пренос или филтрирање преку посреднички услуги. Безбедносниот аспект на МТА е од исклучително значење бидејќи токму оваа компонента е честа мета на злоупотреби. Неконфигуриран или слаб МТА може да функционира како отворен релеј (open relay), дозволувајќи неовластени корисници да испраќаат пораки преку него што е една од најчестите причини за појава на спам. Поради тоа МТА мора да биде конфигуриран така што ќе овозможува испраќање пораки само од доверливи извори, а тоа најчесто со помош на механизми за автентикација како SMTP AUTH, филтрирање на IP-адреси и логирање на сообраќајот за мониторинг. Дополнително современите МТА решенија вклучуваат поддршка за криптографски протоколи како што е TLS (Transport Layer Security) кој овозможува шифрирање на комуникацијата меѓу поштенските сервери. Имплементацијата на безбедносни политики како SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) и DMARC (Domain-based Message Authentication, Reporting and Conformance) е тесно поврзана со функцијата на МТА, бидејќи токму на оваа точка се проверуваат или применуваат овие политики за верификација на автентичноста на испраќачот и заштита од spoofing. Конфигурацијата на МТА, исто така, вклучува поставување на редици (queues) за пораки што не можат веднаш да се испратат поради привремени мрежни проблеми или достапност на серверот на примачот. Овие редици периодично се скенираат, а пораките се обидуваат повторно да бидат испратени. Со тоа се овозможува пораките да не бидат загубени во случај на прекини. Во ситуации кога испораката е невозможно да се реализира, МТА генерира и испраќа "bounce" пораки до испраќачот со информации за причината на неуспехот. Може да се заклучи дека сигурниот, правилно конфигуриран и безбедносно зајакнат МТА претставува темел на секоја доверлива е-пошта инфраструктура. Тој е интерфејс помеѓу домените, чувар на интегритетот на пораката и точка на првата линија на

одбрана против сајбер-закани, што го прави суштински елемент во секој безбеден комуникациски систем.

Mail Delivery Agent (MDA) претставува суштински сегмент во системот на пренос на електронска пошта и има централна улога во последната фаза на испорака на пораки до крајниот корисник (Слика 6). Откако пораката ќе ја помине рутата преку Mail Transfer Agent (MTA) таа се предава на MDA кој е одговорен за нејзиното сместување во соодветното поштенско сандаче (mailbox) на примачот, во локалниот или централен поштенски сервер. MDA функционира како мост помеѓу поштенскиот систем и апликацијата што ја користи крајниот корисник за читање и управување со пораките. Задачата на MDA е да ја организира испораката на пораките врз основа на адресата на примачот, правилата на организацијата и состојбата на поштенскиот сервер. Тој управува со процесите на сортирање, филтрирање, проверка и архивирање, осигурувајќи се дека секоја порака пристигнува во вистинското сандаче без дупликации, губење или прекршување на политиките за безбедност. Најчести имплементации на MDA се софтверски системи како Procmail, Maildrop, Dovecot (во комбинација со IMAP/POP3 сервер), или Local Mail Transfer Protocol (LMTP) за испорака од MTA до IMAP сервер. Во однос на протоколите MDA обично не користи SMTP како што тоа го прави MTA, туку директно пристапува до фајл-системот или базата на податоци каде што се складираат пораките. Форматите во кои се зачувуваат пораките можат да варираат, најчесто користени се mbox (една датотека за сите пораки во еден поштенски сандак) и Maildir (посебна датотека за секоја порака, што овозможува побрз пристап и поголема флексибилност). Во контекст на безбедноста MDA има исклучително значајна улога бидејќи е точката каде што пораката ја завршува својата трансмисија и станува достапна за читање од страна на корисникот. Неправилна конфигурација или недоволна контрола може да доведе до потенцијални ранливости, како што се неовластен пристап до поштенски сандаци, особено во случаи кога MDA не е соодветно интегриран со системи за автентикација (LDAP, RADIUS), манипулација со локално складираните пораки, вклучително и промена на содржина или додавање малициозен код, загуба на податоци при преместување, филтрирање или складирање, особено при хардверски проблеми или нефункционални backup системи и фалсификување на заглавја, ако MDA не ја валидира добро структурата на пораката. Поради овие ризици, од суштинска важност е MDA да биде соодветно заштитен преку употреба на техники како што се контрола на пристап до фајлови, шифрирање на поштенските сандаци

и логирање на активностите поврзани со пристап и промени на пораките. Може да се заклучи дека Mail Delivery Agent не е само „крајна станица“ на патот на пораката, туку и чувар на доверливоста, точноста и достапноста на комуникацијата во рамките на поштенската инфраструктура.

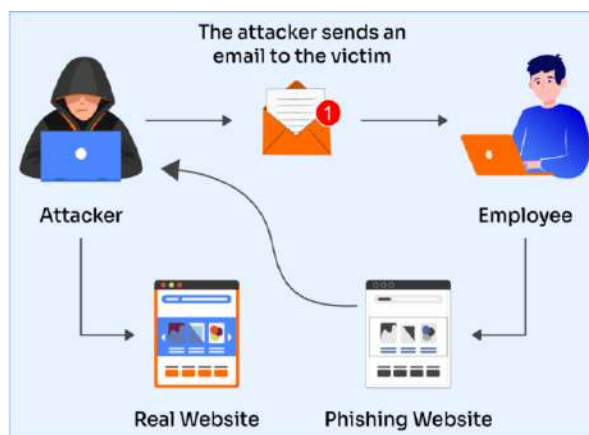
Mail Store (MS) или системот за складирање на поштенските пораки претставува финалната и најстабилна компонента во архитектурата на интернет е-поштата. По успешната достава на пораката преку Mail Delivery Agent (MDA) истата се сместува во Mail Store, каде што се чува сè додека не биде пристапена, прочитана или избришана од страна на крајниот корисник (Слика 6). Оваа компонента е одговорна за долгорочно складирање, структурирање и безбеден пристап до е-поштата и со тоа претставува фундаментална алка во осигурување на интегритетот и достапноста на комуникациските податоци. Најчесто се користат две главни форми за складирање на пораки: Mbox каде сите пораки се сместени во една единствена текстуална датотека, и Maildir каде секоја порака е посебна датотека сместена во структуриран директориум. Пристапот до пораките зачувани во MS се врши преку Mail Access Protocols како што се IMAP (Internet Message Access Protocol) и POP3 (Post Office Protocol v3). IMAP овозможува синхронизирано читање и управување со пораките од повеќе уреди без физичко отстранување на пораката од серверот, додека POP3 презема копија на пораките локално и ги брише од серверот. Притоа загубата, компромитацијата или неовластениот пристап до овие податоци може да има сериозни последици, вклучувајќи кражба на доверливи информации, нарушување на приватноста и правна одговорност. Поради тоа Mail Store мора да биде заштитен со шифрирање на податоци во мирување (encryption at rest), редовно бекапирање, контролиран пристап преку автентикација и авторизација, како и примена на механизми за детекција и превенција на упади (IDS/IPS).

Целосната безбедност на е-поштата не може да се постигне со заштита само на една точка, таа има потреба од end to end стратегија што ги опфаќа сите фази од создавање до читање на пораката со комбинирање на протоколарни, технички и едукативни мерки.

VI. ВИДОВИ ЗАКАНИ

VI.I Фишинг

Закана која претставува една од најчесто користените и воедно најопасните форми на сајбер закани во доменот на електронската пошта [11]. Се работи за форма на социјален инженеринг при која напаѓачот со намера за измама испраќа порака што изгледа релевантно со цел жртвата да настане кон откривање доверливи информации, да превземе малициозен софтвер или да изврши некоја финансиска трансакција. Поради високата ефикасност во реалниот свет, фишингот претставува еден од најчестите иницијални вектори за понатамошни напади врз



Слика 8. Пример за фишинг напад

информациони системи. Овој вид закана може да биде генериран од различни извори вклучувајќи индивидуални напаѓачи или организирани криминални групи. Во последните години сè почесто се користат алатки од типот phishing-as-a-service кои наменски се развиваат за комерцијално дистрибуирање на фишинг напади, што дополнително ја олеснува имплементацијата дури и од страна на технички необучени актери. Во зависност од целта жртвите на фишинг нападите може да бидат индивидуалци, компании, финансиски институции или државни агенции, а во одредени случаи цели земји се таргетирани во рамки на координирани сајбер-офанзиви. Функционирањето на фишингот се базира на психолошки манипулации и технички трикови. Во пораките кои се испраќаат обично се наведува некаква итна потреба за дејствување, како што е ресетирање на лозинка, потврда на идентитет или ажурирање на податоци, со што се предизвикува реакција кај примачот (Слика 8). Линковите вметнати во пораката водат до лажно креирани веб-страници што изгледаат идентично со вистинските каде жртвата ги внесува своите податоци кои веднаш потоа се испраќаат до напаѓачот. Во некои напади фишинг пораките содржат и прикачени фајлови со вградени макроси или извршни компоненти кои автоматски ја инфицираат машината на примачот со малициозен код. Последиците од успешен фишинг напад може да бидат катастрофални и од долгорочен карактер. Во најбенигна форма се манифестираат како

компромитација на еден поединечен кориснички профил, но во сериозни случаи може да доведат до целосно нарушување на интегритетот на корпоративна мрежа, до загуба на доверливи податоци, финансиски измами или правни реперкусии поради нарушување на приватноста согласно закони како што е Општата регулатива за заштита на податоци (GDPR). Во случаи кога жртвата е организација, можат да настанат трајни последици врз угледот, нарушена доверба кај клиентите и внатрешни структурни оштетувања. Дополнително компромитираните сметки често се користат за понатамошна дистрибуција на нови фишинг кампањи, со што се зголемува обемот на заканата. За да се ублажи или елиминира ризикот од фишинг напади неопходна е комбинација од технички и организациски мерки. Основен чекор претставува едукацијата на корисниците со цел да се препознаат сомнителни пораки, необични линкови или прикачени документи. Техничките мерки вклучуваат имплементација на безбедносни протоколи како SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) и DMARC (Domain-based Message Authentication, Reporting and Conformance), кои овозможуваат проверка на легитимноста на испраќачот и спречуваат злоупотреба на домени. Дополнително, користењето на двофакторска автентикација (2FA) значително ја намалува веројатноста за злоупотреба дури и во случај на компромитација на лозинка. Напредните организации инвестираат и во системи за детекција на закани базирани на вештачка интелигенција, sandboxing алатки за анализа на прикачени документи и филтри за е-пошта со високо ниво на прецизност. Во одредени ситуации штетата од фишинг може делумно да се санира преку итна промена на лозинки, известување на засегнати страни или активирање на план за реагирање при инциденти, голем број случаи остануваат неповратно загрозени. Затоа, современиот безбедносен пристап сè повеќе се темели врз принципот „zero trust“, каде што ниту еден канал или корисник не се смета за доверлив во прв момент, туку се вршат континуирани проверки на идентитет, активност и пристап. Фишингот останува еден од најголемите предизвици за информациската безбедност во дигиталната ера, токму поради својата еволутивна природа и способност да се адаптира кон нови технолошки и социјални контексти. За негово успешно неутрализирање потребна е постојана свесност, адаптивна заштита и холистички пристап што ќе го вклучи и човечкиот фактор како активен елемент во безбедносниот еко-систем.

VI.II Спeар-фишинг

Спeар-фишингот претставува таргетирана и значително порафинирана варијанта на класичниот фишинг напад, при што наместо да се испраќаат масовни пораки до случајни корисници, напаѓачот прецизно ја избира својата жртва и ја прилагодува содржината на пораката врз основа на детално истражување и набљудување (Слика 9). Овој пристап се заснова на собирање информации за одредена личност, оддел, организација или конкретен проект, со цел да се изгради комуникација што изгледа



Слика 9. Пример за спeар-фишинг напад

крајно релевантна и персонализирана. Токму затоа, шансите жртвата да ја отвори пораката, да преземе малициозен фајл или да кликне на злонамерен линк се многу повисоки во споредба со класичниот фишинг. Нападите од типот специар-фишинг најчесто се иницирани од актери со повисоко ниво на техничка подготвеност и тактичка прецизност, како што се АРТ (Advanced Persistent Threat) групи, кибер-криминални синдикати или државно спонзорирани хакерски единици. Тие најчесто ги таргетираат клучни лица во



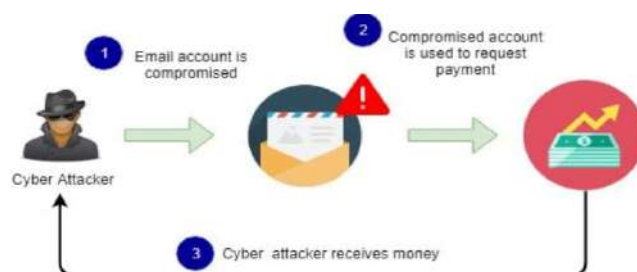
Слика 10. Успешен напад

финансиски трансфери. Преку овој начин можат да резултираат со загуба на високо доверливи податоци, компромитација на целиот информатички систем, значителни финансиски штети, прекин на деловни процеси и уништување на деловен углед. Доколку нападот биде детектиран навремено, можно е делумно санирање преку неутрализација на влезните точки, ресетирање на лозинки, известување на засегнати страни и изолација на инфицирани машини. Поради длабочината на инфилтрацијата и долгорочната природа на таквите напади во многу случаи штетата е тешко да се поврати.

VI.III Бизнис компромитација на електронска пошта (BEC)

Бизнис компромитацијата на електронска пошта (BEC) претставува еден од најпрофитабилните и најперфидните типови на сајбер напади насочени кон организациите, при што напаѓачот се инфилтрира или ја имитира легитимната електронска комуникација на клучни поединци, со цел да иницира измамнички финансиски трансакции или да обезбеди пристап до доверливи информации [13]. За разлика од класичните фишинг напади, BEC не се потпира на автоматски техники или малициозен софтвер, туку на софистицирани психолошки манипулации, при што најчесто не постојат очигледни технички индикатори за нападот. Напаѓачите кои стојат зад ваквите

напади обично се високо организирани криминални групи, често со глобално присуство, добро обучени во кибернетичка и комуникациска манипулација. Во многу случаи, тие користат претходно добиени информации преку фишинг, шпионски



Слика 11. Бизнис компромитација

софтвер или пребарување на јавни извори се со цел за да го мапираат внатрешниот протокол за одобрување на плаќања, како и идентитетите на одлучувачките структури во компанијата (Слика 11). Главна цел на овие напади се директори (CEO), финансиски менаџери или сметководители тоа се луѓе кои имаат надлежност врз финансии или пристап до доверливи податоци. Доколку се забележи BEC напад, итно треба да се прекинат сите трансакции, да се информираат банкарските институции, да се активира интерниот план за одговор на инциденти и да се поднесе пријава до надлежните органи. Во некои случаи може да се обезбеди поврат на средства ако се реагира навремено, но во мнозинството случаи особено кај трансакции во странство, парите исчезнуваат без трага.

VI.IV Рансомвер преку е-пошта

Рансомверот, како форма на малициозен софтвер, претставува една од најдеструктивните и најдоходовни закани во кибер-безбедноста, а е-поштата е еден од примарните канали за неговото распространување. Оваа форма на напад функционира така што корисникот несвесно отвора заразен прилог или кликува на малициозен линк во е-

порака, по што малициозниот код автоматски се извршува и започнува со шифрирање на податоците на системот. Откако енкрипцијата е завршена, жртвата добива



Слика 12. Рансомвер напад

известување, обично преку поп-ап или текстуална датотека дека податоците се заклучени и единствениот начин за нивно отклучување е плаќање на откуп (ransom), најчесто во криптовалути. Напаѓачите кои стојат зад рансомвер кампањи се разновидни, од индивидуални криминалци до

професионализирани групи и државно поддржани актери. Во последните години, сè повеќе се појавува т.н. Ransomware-as-a-Service (RaaS), каде авторите на малициозниот код им овозможуваат на други корисници да го користат рансомверот во замена за дел од добивката. Тоа резултира со масовно ширење на овие закани, каде што жртвите се компании, болници, образовни институции, па дури и владини организации (Слика 12). Прикачените документи често се PDF, Word или Excel фајлови со вградени макроси или пак компресирани архиви кои содржат извршни (.exe) датотеки [14]. Откако ќе се отворат кодот се активира и започнува процес на шифрирање на сите достапни фајлови, вклучително и на мрежни дискови. Последиците од рансомвер напад се сериозни и потенцијално катастрофални. Жртвите можат да загубат критични податоци, да доживеат долг прекин на деловните процеси, да претрпат финансиски штети, оштетување на углед и правни последици поради компромитација на податоци. Рансомверот останува една од најагресивните закани во дигиталната ера, а неговата поврзаност со е-поштата како вектор за напад го прави уште поопасен. Борбата против него бара техничка зрелост, организациска подготвеност и постојана превенција.

VI.V Злонамерни прилози и измама со адреса (Malicious Attachments и Email Spoofing)

Злонамерните прилози претставуваат едноставен, но исклучително ефикасен механизам за компромитирање на системи преку е-пошта. Тие се користат за да се вметне

малициозен софтвер во компјутерот на примачот без потреба од интеракција надвор од отворање на прикачениот документ [15]. Во повеќето случаи, прилозите доаѓаат во форма на Word, Excel, PDF или ZIP документи кои содржат вградени макроси, скрипти или извршни (.exe) фајлови кои штом се активираат, започнуваат процес на инфицирање на системот (Слика 13). Ваквите прикачени датотеки може да иницираат различни типови на злонамерен софтвер – од keyloggers и backdoors до рансомвер или spyware. Еднаш активирани, тие може тивко да преземаат дополнителни компоненти да го следат корисникот или да го вклучат системот во botnet мрежа. Во многу од нападите напаѓачот ги комбинира злонамерните прилози со email spoofing – техника со која се лажира испраќачката адреса така што пораката изгледа како да доаѓа од доверлив извор, на пример од колега, надреден, банка, клиент или владин ентитет со што се намалува веројатноста примачот да ја препознае заканата. Spoofing-от се реализира преку манипулација на SMTP (Simple Mail Transfer Protocol), кој по дифолт не содржи вградена автентикација



Слика 13. Измама со адреси

што го прави ранлив на злоупотреба. Напаѓачот ја поставува „From“ адресата да изгледа легитимно, но всушност пораката потекнува од неавторизиран извор. Овие типови на напади се користат од широк спектар на заканувачи како што се поединечни хакери, криминални синдикати и државно финансирани актери, бидејќи овозможуваат брз влез во системите со минимална интеракција. Целите на ваквите напади се различни, од масовно инфицирање до конкретно таргетиран напади во рамки на поголеми шпионажни или саботажни операции. Особено ризични се сценаријата кога инфицираниот систем има администраторски привилегии или е поврзан со други критични системи. За заштита, најважна е превенцијата. Организациите мора да ги конфигурираат своите системи така што ќе блокираат потенцијално опасни прилози (како .exe, .js, .vbs) да користат email gateway филтри кои скенираат прилози со антивирусни решенија и sandbox алатки кои ги тестираат датотеките во изолирана средина. Дополнително, заштитата од spoofing вклучува правилна конфигурација на DNS-записи преку SPF, DKIM и DMARC, што им овозможува на системите да проверат дали пораката навистина доаѓа од легитимен сервер. Корисниците

треба да бидат обучени да внимаваат на несоодветни домени, грешки во текстот, притисок за итност и необични прикачени датотеки. Покрај тоа штп може да се изолираат и избришат конкретните пораки, откако еднаш ќе се изврши злонамерниот код последиците може да бидат тешко поправливи. Затоа, модерната безбедност не се потпира само на антивирус, туку на проактивен и холистички пристап каде е-поштата се смета за високоризичен комуникациски канал кој бара постојан надзор, мониторинг и обука на човечкиот фактор.

VII. ОСНОВНИ ЦЕЛИ НА БЕЗБЕДНОСТА

Во контекст на информатичката безбедност, постојат четири фундаментални цели кои служат како темел на секоја стратегија за заштита на податоците и системите. Овие цели се доверливост, интегритет, автентификација и достапност кои се познати и како CIAA модел и претставуваат основа за разбирање на безбедносните механизми во секоја дигитална околина, вклучувајќи електронска пошта, бази на податоци, мрежни системи и апликации.

Доверливоста се однесува на заштитата на информациите од неовластен пристап. Целта е да се осигури дека само овластени лица или системи можат да ги читаат или користат чувствителните податоци. На пример при комуникација преку е-пошта доверливоста обезбедува содржината на пораката да не биде прочитана од трети лица, што е особено важно при испраќање на лични, медицински, финансиски или корпоративни информации. Оваа цел се постигнува со употреба на криптографија, енкрипција на податоци, контрола на пристап и автентикациски механизми [17]. Недостаток на доверливост може да доведе до сериозни последици како што се кражба на идентитет, индустриска шпионажа или откривање на доверливи информации во јавноста.

Интегритетот обезбедува точност, потполност и конзистентност на информациите. Тој гарантира дека податоците не се изменети, избришани или оштетени на неовластен начин ниту при складирање, ниту при пренос. Ако некој податок се измени без дозвола, интегритетот е нарушен. Тој е особено значаен кај електронската пошта, каде постои ризик пораката да биде изменета од трета страна за време на преносот. Примена на хеш функции, дигитални потписи и механизми за проверка на интегритет овозможува примачот на пораката да провери дали таа е оригинална и непроменета. Без интегритет, корисниците не можат да се потпрат на вистинитоста на добиените информации.

Автентификацијата е процес преку кој се потврдува идентитетот на корисникот, системот или процесот кој се обидува да пристапи до некој ресурс. Во основа тоа значи проверка на прашањето „дали си оној за кого се претставуваш“. На пример кога корисник се најавува во систем со корисничко име и лозинка тоа претставува најосновен вид на

автентификација. Во поширока примена се користат двефакторска автентификација (2FA), биометриски методи (отпечаток од прст, препознавање на лице), дигитални сертификати и автентикациски токени. Во безбедносен контекст автентификацијата ја спречува можноста за лажна претстава што е клучно при заштита од напади како фишинг или спуфинг. Прецизна автентификација е суштинска за зачувување на довербата во секоја комуникација и заштита на личните податоци.

Достапноста се однесува на тоа информациите и системите да бидат достапни и функционални за овластените корисници секогаш кога се потребни. Безбедноста не значи само заштита од напад, туку и обезбедување на континуирана работа без прекини или падови. На пример ако е-поштата или базата на податоци се недостапни поради напад од типот Denial-of-Service (DoS), тогаш е нарушена целта на достапноста. Оваа цел се обезбедува преку backup решенија, зајакнување на мрежната инфраструктура, контрола на капацитет и заштита од напади кои го преоптоваруваат системот. Достапноста е особено критична за институции како болници, банки и владини установи каде секој прекин може да има сериозни последици.

Овие четири цели не се изолирани една од друга, туку се поврзани и меѓузависни. Заштитата на податоците и дигиталната инфраструктура бара холистички пристап кој ги вклучува сите четири компоненти. Само кога сите се исполнети, може да се зборува за сеопфатна и ефективна безбедност на информациите.



Слика 14. Цели на безбедност

VIII. МЕХАНИЗМИ ЗА ЗАШТИТА ОД Е-MAIL НАПАДИ

Во овој дел ќе се задржиме на механизмите за заштита од напади преку електронска пошта, кои се исклучително важни во современиот дигитален свет. Со оглед на честата злоупотреба на е-mail комуникацијата со ширење на фишинг, малициозен софтвер, спам и други облици на сајбер-напади, потребата од ефикасни и сигурни безбедносни мерки станува сè поголема. За таа цел, се користат различни механизми и практики на кои што ќе обрнеме внимание во овој труд.

VIII.I Secure/Multipurpose Internet Mail Extensions (S/MIME)

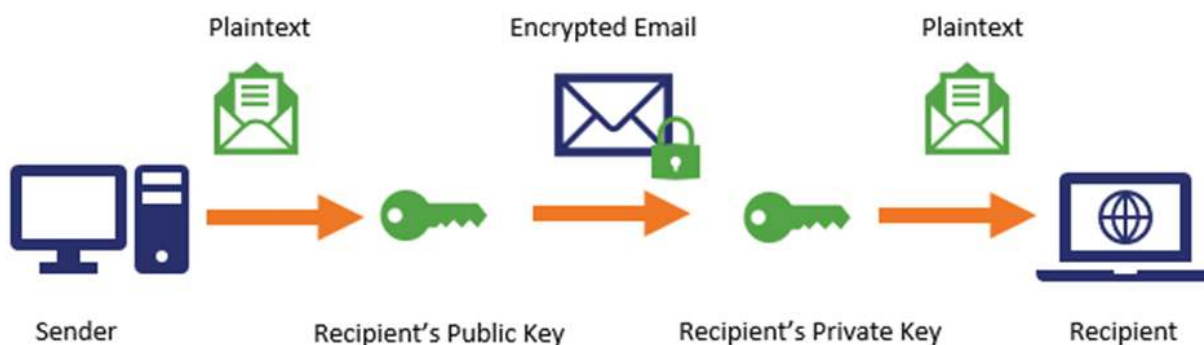
S/MIME претставува стандард кој овозможува шифрирање и дигитално потпишување на е-mail пораки користејќи криптографија со јавен клуч. Со S/MIME, се обезбедува доверливост, автентичност и интегритет на пораките, без разлика на примачот или неговата локација.

S/MIME се базира на принципите на PKI (Public Key Infrastructure) – инфраструктура што користи две клуча: јавен и приватен клуч. Јавниот клуч се користи за шифрирање (заклучување) на пораката и може да се споделува, додека пак приватниот клуч се користи за дешифрирање (отклучување) и мора да остане строго чуван од страна на сопственикот [22] (слика 15).

Со PKI, S/MIME користи дигитални сертификати што содржат јавен клуч и податоци за сопственикот (име, е-mail адреса, организација и сл.). Овие сертификати се издаваат и верификуваат од доверливи трети страни, наречени Certificate Authority (CAs). Тие играат клучна улога во утврдување на валидноста на јавниот клуч и идентитетот на неговиот сопственик.

Со дигитален сертификат, може да се додаде дигитален потпис на е-mail пораките, што претставува дополнително ниво на безбедност. Овој потпис му гарантира на примачот дека пораката е навистина испратена од самиот испраќач бидејќи е потврдена од СА, а не од некој

измамник. Сертификатот дејствува како дигитален печат, кој уверува дека содржината не е променета при преносот. Секоја измена ќе го направи потписот неважечки [22].



Слика 15. Шифрирање и дешифрирање со S/MIME

Процесот на дигитално потпишување порака кај S/MIME има неколку чекори:

1. По составување на пораката и пред нејзино испраќање, се вклучува опцијата за дигитален потпис
2. Се создава хеш од пораката
3. Приватниот клуч се користи за шифрирање на хешот
4. Потписот и јавниот клуч се прикачуваат во пораката при самото испраќање
5. Примачот ја валидира пораката со јавниот клуч и проверува дали хешот одговара на содржината
6. Ако хешот не се совпаѓа, значи пораката е изменета и ќе се појави соодветна нотификација.

Процесот на шифрирање порака кај S/MIME вклучува неколку чекори:

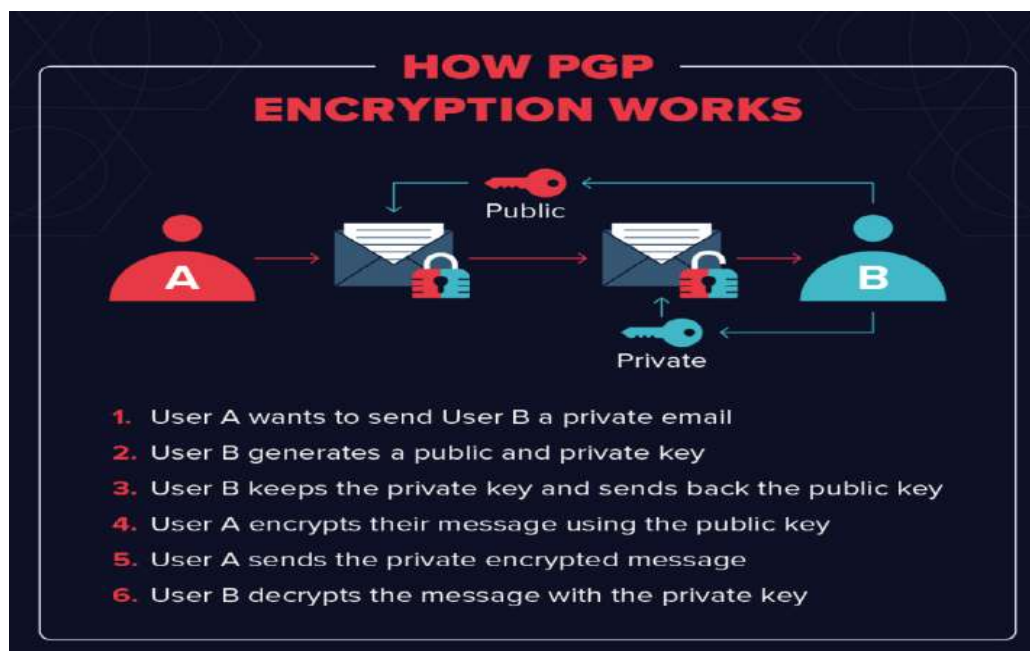
1. Испраќачот го добива јавниот клуч на примачот
2. Пораката се шифрира со симетричен алгоритам.
3. Симетричниот клуч потоа се шифрира со јавниот клуч на примачот.

4. Се испраќаат заедно шифрираната порака (ciphertext) и шифрираниот симетричен клуч во една „пакет“ датотека.
5. Примачот го верификува сертификатот и дигиталниот потпис на испраќачот, користејќи го јавниот клуч и истата хеш функција.
6. Ако е успешна проверката, пораката е автентична и неизменета.
7. Примачот ја дешифрира пораката со својот приватен клуч, користејќи го истиот симетричен алгоритам.
8. Дешифрираната порака се нарекува plaintext, односно оригиналната порака што испраќачот сакал да ја испрати.

VIII. II Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) е систем за енкрипција што се користи за испраќање шифрирани е-mail пораки и за шифрирање на датотеки. Популарноста на PGP се темели на два фактори. Првиот е тоа што, PGP првично бил достапен како бесплатен софтвер (freeware), што овозможило брзо ширење кај корисниците кои сакале дополнително ниво на безбедност при испраќање е-mail пораки. Вториот фактор е тоа што PGP користи комбинација од симетрична енкрипција и енкрипција со јавен клуч, што им овозможува на корисници кои никогаш не се сретнале да си испраќаат шифрирани пораки без да разменат приватни енкрипциски клучеви [23].

PGP има заеднички карактеристики со други системи за енкрипција како што се: Kerberos енкрипција (која се користи за автентификација на мрежни корисници), SSL енкрипција (која се користи за безбедност на веб-страници) и други. PGP користи комбинација од два типа енкрипција: симетрична енкрипција (која содржи ист клуч за шифрирање и дешифрирање) и енкрипција со јавен клуч (која користи два различни клуча: јавен и приватен) [23].



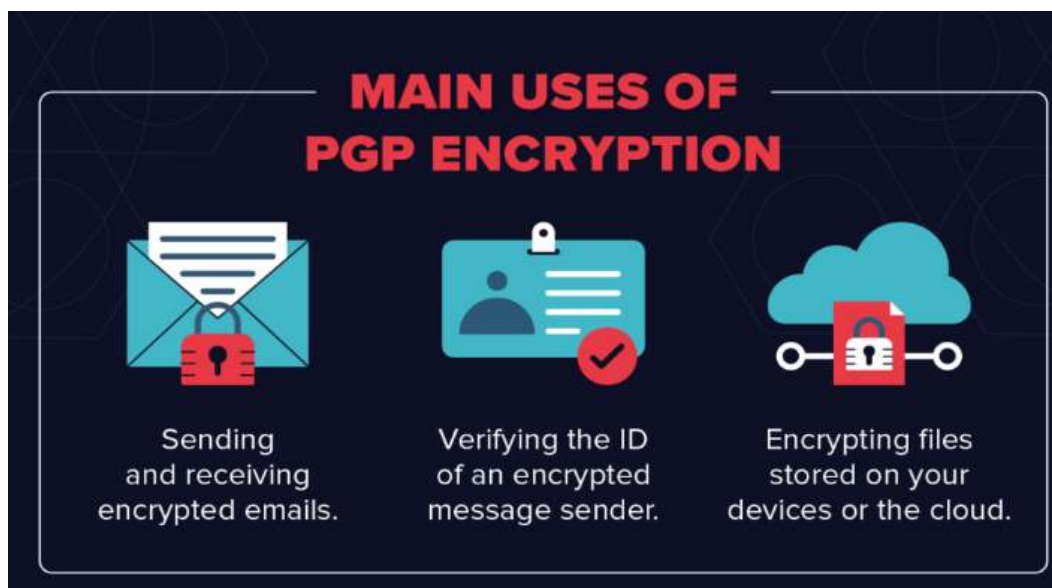
Слика 16. Работа на PGP

Принципот на работа на PGP се состои од неколку чекори прикажани на Слика 16:

1. PGP генерира случаен “session key” користејќи еден од двата главни алгоритми. Овој клуч е бесконечно голем број кој е невозможно да се погоди и се користи само еднаш.
2. Потоа, тој session клуч се шифрира со јавниот клуч на примачот на пораката. Јавниот клуч е поврзан со конкретна личност и секој може да го користи за да ѝ испрати порака.
3. Испраќачот го испраќа шифрираниот session клуч до примачот, кој потоа може да го дешифрира со својот приватен клуч.
4. На крај, користејќи го дешифрираниот session клуч, примачот ја дешифрира самата порака.

Во основа, постојат три главни примени на PGP кои се прикажани на Слика 17:

1. Испраќање и примање на шифрирани e-mail пораки.
2. Верификација на идентитетот на личноста што ја испратила пораката.
3. Шифрирање на датотеки.



Слика 17. Примена на PGP енкрипција

VIII.II.I Шифрирање на е-пошта пораки

Најчеста и најпозната примена на PGP е шифрирањето на електронска пошта. Во своите почетоци, PGP претежно се користел од активисти, новинари и други професионалци кои ракувале со чувствителни или доверливи информации, особено во ситуации каде приватноста и безбедноста биле од критично значење.

VIII.II.II Верификација со дигитален потпис

PGP истотака може да се користи за верификација на e-mail пораки. На пример, ако некој новинар не е сигурен за идентитетот на личноста што му ја испраќа пораката, може да искористи дигитален потпис заедно со PGP за да го потврди тоа.

Дигиталниот потпис работи со алгоритам кој го комбинира клучот на испраќачот со податоците што ги испраќа. Со ова се генерира „hash функција“ - друг алгоритам кој ја претвора пораката во блок од фиксна големина. Таа hash вредност се шифрира со приватниот клуч на испраќачот.

Примачот потоа ја дешифрира таа вредност со јавниот клуч на испраќачот. Ако е изменет дури и еден карактер во пораката, примачот ќе го знае тоа. Тоа може да значи неколку работи а тоа се: испраќачот не е оној за кого се претставува, потписот е фалсификуван или пораката е изменета во текот на преносот.

VIII.II.III Шифрирање на датотеки

Една од значајните примени на PGP, покрај шифрирањето на електронска пошта, е и шифрирањето на локални датотеки. PGP го комбинира симетричното и асиметричното шифрирање за да обезбеди високо ниво на безбедност при заштита на датотеките. Прво, системот генерира случаен симетричен клуч (на пр. преку AES алгоритам), потоа овој клуч се шифрира со јавниот клуч на примачот преку асиметричен алгоритам, најчесто RSA. Шифрираната датотека заедно со шифрираниот симетричен клуч се складира локално на дискот или во облак, а пристапот до неа е можен единствено со соодветниот приватен клуч. Ваквиот пристап овозможува силна заштита на податоци во мирување (data at rest), бидејќи дури и во случај на компромитирање, не е можно нивно дешифрирање без приватниот клуч.

VIII.III Sender Policy Framework (SPF)

Sender Policy Framework (SPF) претставува протокол за автентификација на електронска пошта, чија главна цел е да се спречи фалсификување на адресите на испраќачите (email spoofing) – техника што често се користи во фишинг напади и несакана пошта (spam).

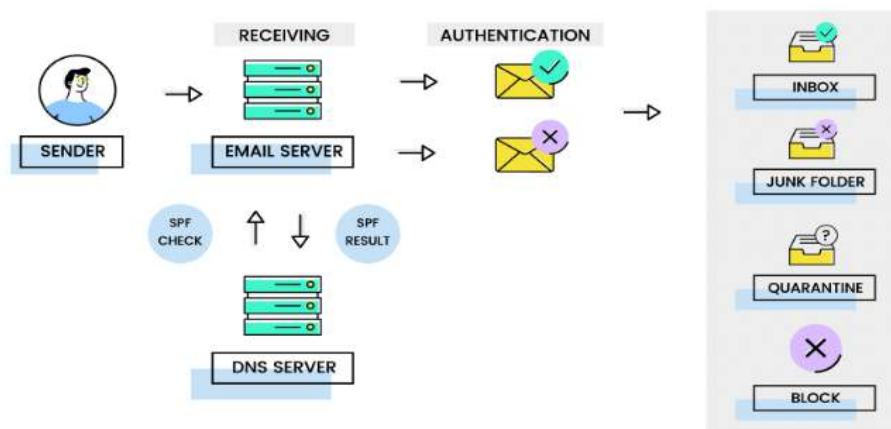
SPF му овозможува на серверот што ја прима пораката да провери дали таа е испратена од овластен сервер за тој домен. Овие информации се дефинирани преку SPF запис, кој се поставува како DNS запис на доменот и содржи список на IP адреси и сервери што имаат дозвола да испраќаат пораки во тој домен. Оваа проверка е особено важна бидејќи напаѓачите често ја лажираат адресата на испраќачот така што изгледа како да доаѓа од доверлива компанија или познат контакт.

Кога серверот ќе прими e-mail порака, го користи SPF протоколот за да провери дали испраќачот е валиден во SPF записот. Доколку проверката е успешна, пораката се прифаќа како валидна. Ако не, се смета за потенцијално фалсификувана (spoofed) и најчесто се одбива или се класифицира како спам.

Иако SPF значајно придонесува за безбедноста на е-поштата, постојат одредени ограничувања. На пример, протоколот дозволува максимум 10 DNS пребарувања за време на проверката, што може да претставува проблем кај сложени SPF записи. Исто така, SPF не обезбедува end-to-end енкрипција и не нуди заштита од напади кои користат домени со

сличен изглед (lookalike domains). Дополнително, ако пораката се проследи (forward) преку сервер кој не е наведен во SPF записот, автентикацијата може да не успее, дури и ако пораката е легитимна.

Затоа, SPF сам по себе не е доволен. Најдобра практика е негово комбинирање со други механизми за автентикација, како што се DKIM (DomainKeys Identified Mail) и DMARC (Domain-based Message Authentication, Reporting and Conformance), со цел да се постигне поефикасна заштита.



Слика 18. Работа на SPF

VIII.IV DomainKeys Identified Mail (DKIM)

DKIM (DomainKeys Identified Mail) е метод за автентификација на електронска пошта кој користи дигитален потпис со цел примачот да може да провери дали пораката навистина е испратена и одобрена [20].

Штом примачот утврди дека пораката содржи валиден DKIM потпис, може со сигурност да се потврди дека содржината на пораката не била изменета при преносот. Во повеќето случаи, DKIM потписите не се видливи за крајните корисници – валидацијата се врши на ниво на сервер.

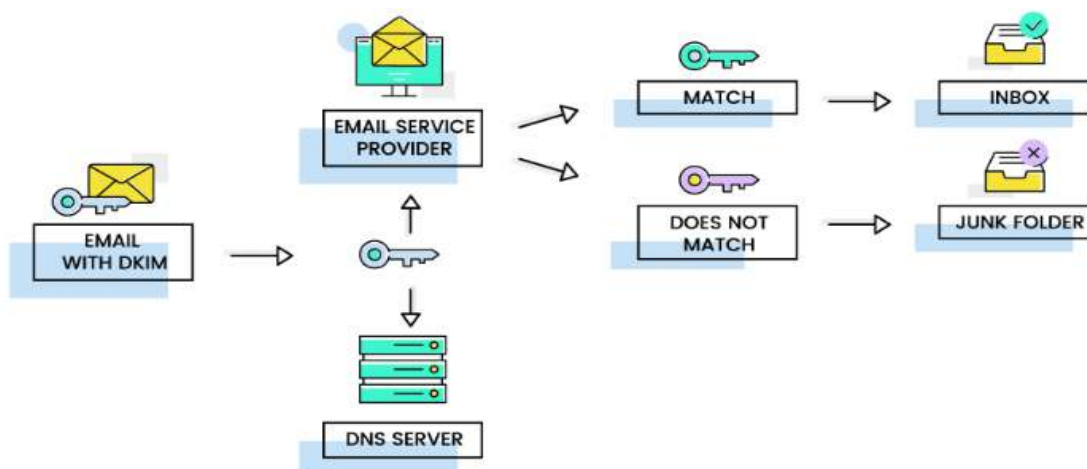
Кога се користи заедно со DMARC и SPF, DKIM овозможува значителна заштита од злоупотреба преку испраќање на малициозни пораки од домени кои се претставуваат како ваш бренд.

DKIM запис е текстуална содржина која се наоѓа во DNS записот на доменот и содржи јавен криптографски клуч. Овој клуч го користат серверите што ја примаат поштата, за да ја проверат автентичноста на DKIM потписот.

Со оглед на тоа што лажирањето (spoofing) на пораки од доверливи домени станува сè поголема сајбер закана, од суштинско значење е да се потврди дека DKIM записот е правилно поставен уште на самиот почеток од имплементацијата. Секогаш кога е можно, се препорачува додавање на DKIM запис во DNS за да се овозможи сигурна автентификација на пораките [20].

DKIM протоколот користи криптографски потпис, односно шифрирано заглавје (header), кое се додава во самата порака. Овој потпис потврдува дека пораката е автентична и дека не била променета за време на нејзиниот пренос. Примачот ја верификува автентичноста на пораката користејќи го јавниот клуч објавен во DKIM записот на DNS-от [20].

Иако протоколот DKIM е корисен, сам по себе не претставува загарантирана заштита од spoofing напади. Потписот не е видлив за обичните корисници и не обезбедува заштита од злоупотреба на „From“ полето во пораката – што е всушност единствената информација што корисниците ја гледаат. Дополнително, приватните клучеви што се користат за потпишување на пораките со DKIM може да бидат украдени од страна на хакери, а управувањето со јавните клучеви може да биде напорна и временски тешка задача.



Слика 19. Работа на DKIM

VIII.V Domain-based Message Authentication, Reporting & Compliance (DMARC)

DMARC (Domain-based Message Authentication, Reporting & Conformance) е напреден безбедносен протокол кој се користи за заштита од e-mail phishing и spoofing. Тој се надоврзува на веќе постоечките механизми за автентификација – SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail) и им овозможува на сопствениците на домени да дефинираат како да се постапува со e-mail пораките кои не ги поминуваат автентикациските проверки. Освен тоа, DMARC овозможува следење и известување преку автоматски генерирани извештаи [21].

Главни карактеристики на DMARC се alignment policy и извештаи (Aggregate & Forensic Reports). Со alignment policy сопственикот на доменот одредува како треба да се постапи со пораките кои не се во согласност со DKIM или SPF и пораките кои имаат несоодветен “From” домен. Додека пак извештаите се делат на Aggregate reports и Forensic reports. Агрегатните извештаи се XML-документи што содржат статистички податоци кои вклучуваат информации како резултати од автентификацијата и начинот на кој пораките се третирали (доставени, одбиени итн.) и се наменети исклучиво за машинска обработка. Форензичките извештаи се копии од e-mail пораки кои не успеале да ја поминат автентификацијата. Тие се корисни за откривање и решавање на проблемите со автентификација, како и за идентификација на малициозни веб-страници и домени [21].

Покрај овие има и дефинирана политика (p=) што одлучува што да се прави со невалидни пораки. Во DMARC записот и постојат три можни вредности прикажани на слика 20:

- p=none (без акција):

Се применува само за следење. Серверот што прима пораки нема да преземе никаква акција врз невалидните пораки, туку ќе испраќа извештаи до зададената адреса.

- p=quarantine (карантин):

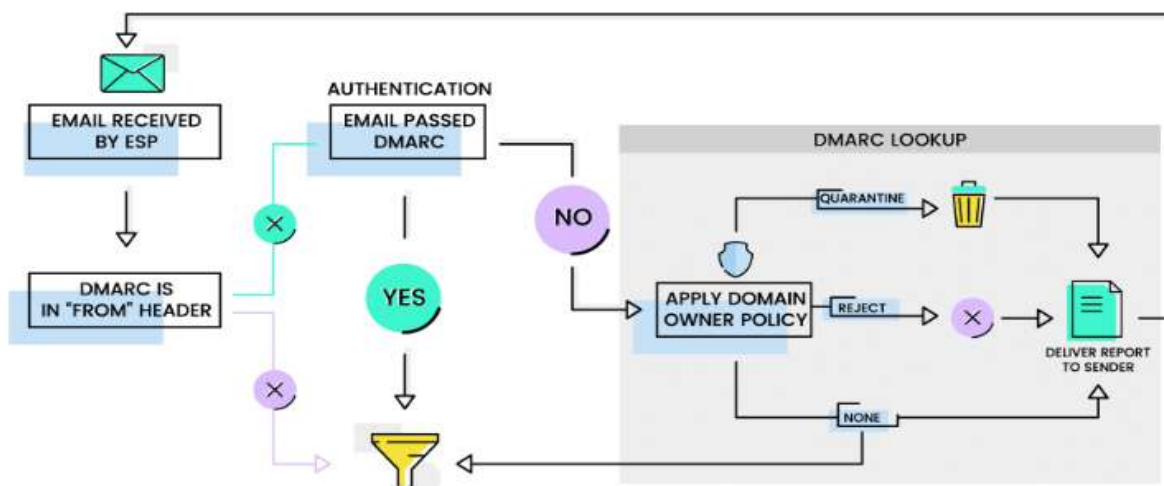
Серверот што прима пораки ќе ги смести невалидните пораки во spam или junk папката. Ова е средна опција која нуди одредена заштита без целосно да се блокираат пораките.

- `p=reject` (одбивање):

Се применува најстрога заштита односно серверот воопшто нема да прифати пораки што не ја поминуваат автентификацијата. Само верификувани пораки ќе стигнат до инбоксот на примачите.

Со оваа политика, домените добиваат контрола врз тоа кој може да испраќа пораки во нивно име и го минимизираат ризикот од фишинг напади и злоупотреба.

DMARC претставува суштински дел од безбедносната инфраструктура за e-mail и е најефективен кога се користи во комбинација со SPF и DKIM. Додека SPF овозможува проверка на овластените IP адреси што испраќаат пораки за еден домен, а DKIM обезбедува криптографска потврда на автентичноста на содржината, DMARC ги поврзува овие две технологии и додава политика за постапување со пораки кои не ја поминуваат проверката.



Слика 20. Работа на DMARC

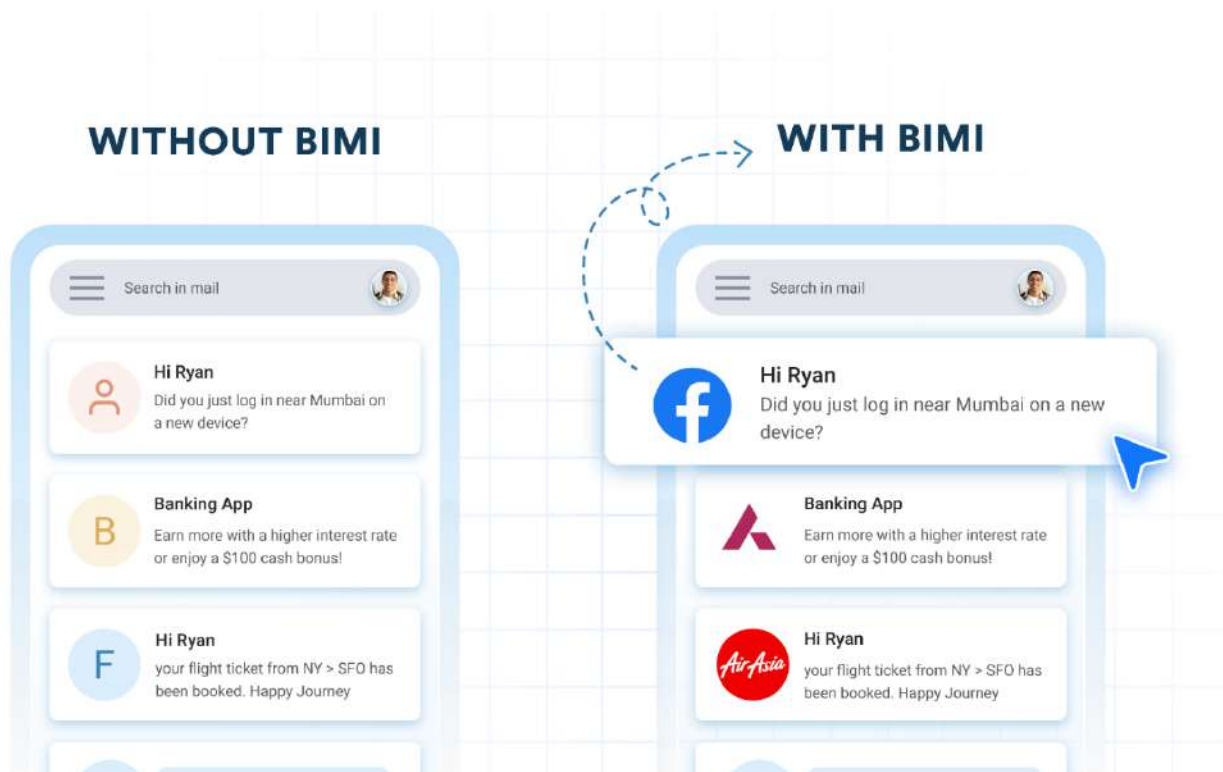
VIII.VI BIMI (Brand Indicators for Message Identification)

Покрај механизмите за автентификација на e-mail кои беа обработени досега, во поново време се појавува и нова, современа технологија наречена BIMI (Brand Indicators for Message Identification).

BIMI претставува напреден метод за унапредување на безбедноста и идентификацијата на испраќачи во електронската пошта. Слично на стандардите SPF, DKIM и DMARC, BIMi се

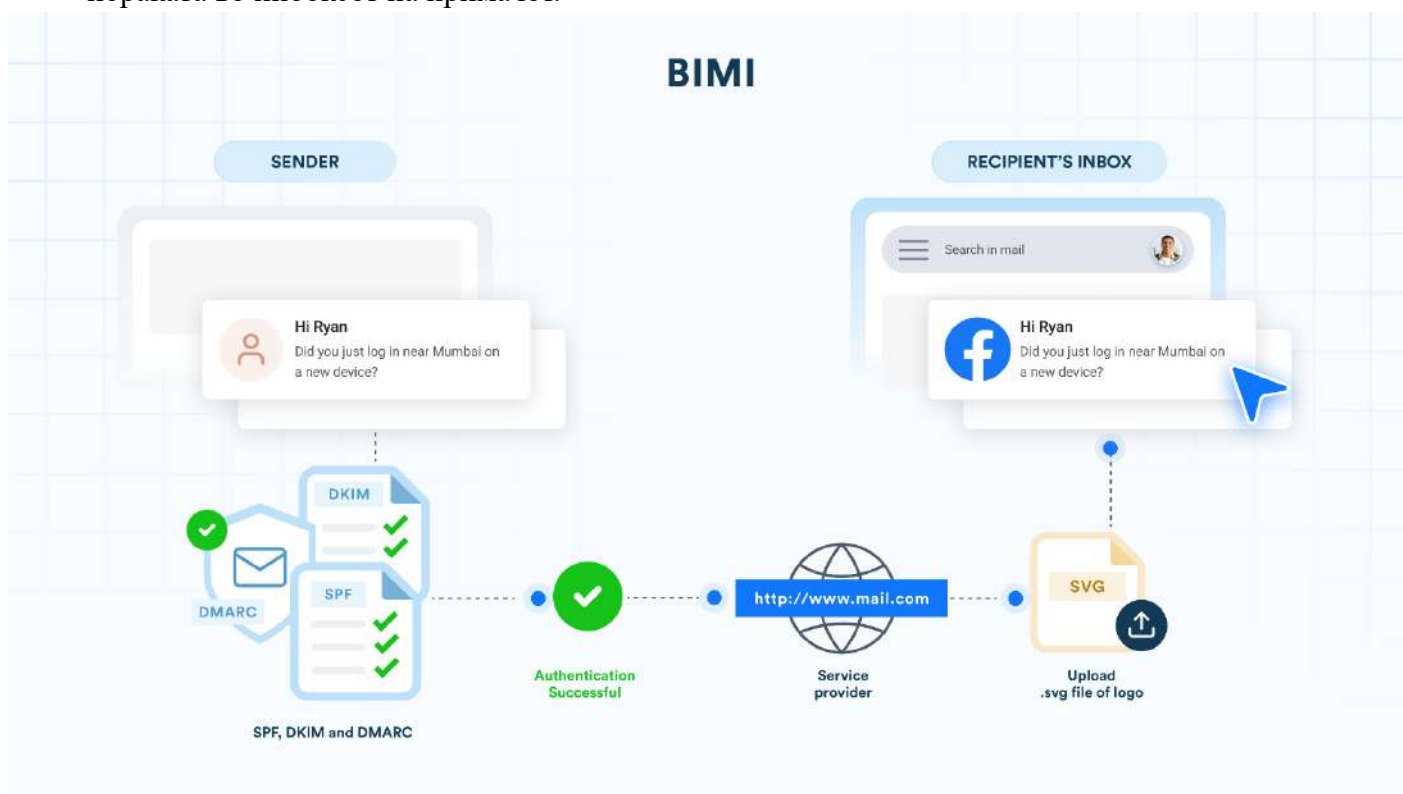
имплементира преку текстуален DNS запис, кој се поставува на серверот на доменот на испраќачот. Работи во синергија со останатите механизми, сигнализирајќи на e-mail клиентите дека пораката потекнува од легитимен и верификуван извор [24].

За разлика од останатите механизми кои се технички „невидливи“ за крајниот корисник, BIMI додава визуелен елемент – верификувано лого на испраќачот, кое се прикажува во инбоксот покрај пораката [24] (слика 21).



Слика 21. Инбокс без/со BIMI

Слично на другите стандарди за автентификација на е-mail, BIMI содржи текстуален запис кој се хостира на серверите на испраќачот. Кога пораката ќе биде испратена, е-mail сервисот на примачот врши DNS пребарување за да го пронајде и валидира BIMI записот. Доколку записот е валиден, тој содржи информација за локацијата на логото на испраќачот. Врз основа на тоа, е-mail клиентот го презема дефинираното лого и го прикажува покрај пораката во инбоксот на примачот.



Слика 22. BIMI процес

Процесот на работа на BIMI се состои од неколку чекори кои се прикажани на Слика 22:

1. Објава на бренд потврда (Brand Assertion)

Сопствениците на домени го објавуваат BIMI записот преку DNS системот, со што го дефинираат логото поврзано со доменот и неговата валидност. Овој чекор ја воспоставува асоцијацијата помеѓу доменот и брендот.

2. Автентикација на е-пошта пораки преку BIMI

При секое примање порака, е-mail провајдерот ја автентифицира пораката за да обезбеди безбедност и приватност. Автентификацијата се извршува врз основа на поставените DNS

записи како SPF, DKIM и DMARC. BIMI функционира како дополнителен слој во овој процес – пораките што не успеваат да ја поминат автентикацијата не се квалификуваат за прикажување на бренд логото и се преместуваат во spam.

3. Пребарување и прикажување на логото

Откако пораката ќе ги помине безбедносните проверки, e-mail клиентот врши DNS пребарување за BIMI запис. Ако постои валиден запис, логото наведено во него се повлекува и се прикажува покрај пораката во инбоксот.

BIMI значително го зголемува визуелниот интегритет на пораката, препознатливоста на брендот и довербата кај примачот. Во ера на сè почести фишинг и измамнички напади, ваквиот пристап придонесува кон посигурна комуникација.

Различни методи за проверка на испраќачите и користење на логоа постојат со години, но првата формализирана спецификација за BIMI е објавена во Февруари 2019 година. Оригиналните креатори оттогаш ја имаат формирано работната група AuthIndicators Working, со цел да се стандардизира и унапреди BIMI технологијата на глобално ниво. Во текот на последните неколку години, групата има добиено поддршка од водечки компании во областа на е-пошта технологијата и комуникацијата, како што се: Google, Yahoo, Fastmail, Mailchimp, Proofpoint, Twilio SendGrid, Valimail, Validity и други [24].

Во овој дел беа разгледани најзначајните механизми за заштита на електронска пошта – S/MIME, PGP, SPF, DKIM и DMARC, кои овозможуваат криптографска заштита, потврда на идентитет, верификација на содржина и поставување политики за одбивање на невалидни пораки. Дополнително, BIMI претставува модерен пристап за визуелна доверба, што го зајакнува брендот и ја олеснува идентификацијата на легитимни испраќачи. Комбинирањето на овие технологии не само што обезбедува техничка заштита, туку и гради доверба помеѓу испраќачите и примачите. Организациите кои ги имплементираат овие механизми покажуваат одговорност кон безбедноста, интегритетот и приватноста на комуникацијата.

VIII.VII AI Spam Filtering

Филтрирањето на несакана пошта претставува клучен елемент во заштитата на електронската комуникација. Со појавата на сè пософистицирани фишинг и спам техники,

традиционалните филтри кои се темелат на клучни зборови, листи со дозволени и блокирани адреси (whitelist/blacklist) стануваат сè помалку ефикасни. Како одговор на овие предизвици, во последните години сè поголем замав земаат AI-базирани филтри кои користат алгоритми за машинско учење за идентификација и блокирање на спам пораки.

AI филтрите се засноваат на анализирање големи количини податоци и препознавање на спам-содржина. Алгоритмите за машинско учење се обучуваат врз основа на податоци од спам и легитимни пораки, при што учат да прават разлика помеѓу нив со висока прецизност. На тој начин, AI е способен да го



Слика 23. Апстрактен приказ на AI Spam Filtering

„разбере контекстот“ на пораките, наместо само да препознава зборови или фрази. Ова му овозможува да открие и нови, досега непознати форми на несакана комуникација [25].

Една од клучните предности на AI филтрите е нивната способност за прилагодување на нови техники на спамери. Додека традиционалните системи мора постојано рачно да се ажурираат, AI алгоритмите се способни самостојно да се прилагодат на нови закани. Ова е особено важно имајќи предвид дека спамерите сè почесто користат вештачка интелигенција за создавање поавтентични и персонализирани пораки, кои тешко се детектираат со класични методи [25].

Иако AI филтрите не обезбедуваат апсолутна заштита, нивната ефикасност значително ја надминува онаа на традиционалните методи, особено кога се комбинираат со други безбедносни механизми како SPF, DKIM и DMARC. Таквиот повеќеслоен пристап овозможува поголема точност и помал број на лажно позитивни или лажно негативни детекции.

Покрај сите предности, AI филтрите се соочуваат и со сериозни предизвици. Еден од главните проблеми е неурамнотеженоста на податочните сетови – ако системот е обучен на примероци кои не ја претставуваат реалната дистрибуција на спам и легитимни пораки, може да дојде до намалување на точноста. Дополнително, спамерите развиваат тактики за избегнување на филтри, што бара постојано дообучување и подобрување на моделите [25].

IX. СТУДИИ НА СЛУЧАИ И ПРАКТИЧНИ ПРИМЕРИ ОД ОБЛАСТА НА САЈБЕР – БЕЗБЕДНОСТА

IX.I Фишингот како закана во сајбер-безбедноста: Случајот со Yahoo breach

Една од најчестите и најопасни закани во областа на сајбер-безбедноста е фишингот — техника на социјален инженеринг преку која напаѓачите настојуваат да измамаат корисници и да дојдат до чувствителни информации. Фишинг-пораките најчесто пристигнуваат преку електронска пошта и често изгледаат како да се испратени од легитимни извори, како што се банки, интернет-провајдери или познати технолошки компании. За навремено препознавање на ваквите напади, од особено значење е добро познавање на структурата на електронската пошта и нејзините заглавија, каде што може да се забележат сомнителни детали поврзани со испраќачот, серверот и времето на испраќање.

Од секојдневието сме сведоци на разни сајбер-напади кои претставуваат сериозна закана за безбедноста на податоците и системите. Еден од најпознатите и најмасовни вакви напади е случајот познат како **Yahoo breach**, кој претставува класичен пример за тоа како безбедносните пропусти и слабата енкрипција можат да резултираат со компромитирање на милијарди кориснички сметки [26].

Нападот се случил во 2013 година, кога напаѓачите успеале да ги компромитираат личните податоци на сите кориснички сметки на Yahoo. На почетокот, компанијата го потценила обемот на нападот, информирајќи во 2016 година дека се погодени околу 1 милијарда сметки. Сепак, во 2017 година Yahoo ја ревидирала оваа бројка, признавајќи дека всушност биле компромитирани сите 3 милијарди кориснички сметки.

Хакерите ја искористиле ранливоста за да добијат пристап до системот и откако го украле кодот за генерирање колачиња (cookies), создавале фалсификувани колачиња кои им овозможувале на корисниците да останат најавени без повторно внесување на лозинки (Слика 24). Овој метод им овозможил на напаѓачите да останат незабележани цели три години, бидејќи фалсификуваните колачиња не активирале безбедносни аларми. За време

на нападот, биле украдени различни видови на податоци: имиња, е-адреси, телефонски броеви, датуми на раѓање, хеширани лозинки, како и одредени нешифрирани информации.

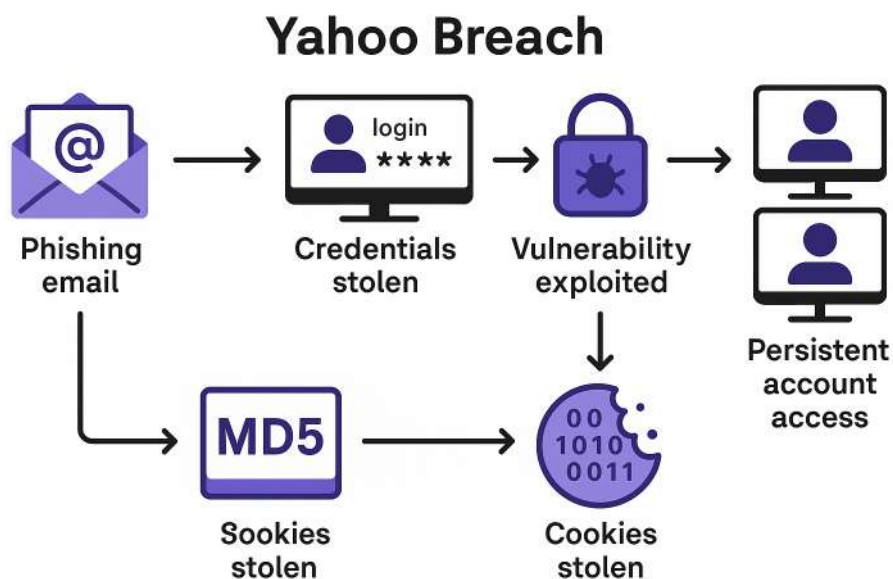
Како главна причина за компромитирањето на лозинките се смета користењето на MD5¹ хеш-функцијата за складирање лозинки — алгоритам кој веќе долго време се смета за застарен и небезбеден.

Овој напад оставил сериозни финансиски последици за компанијата, пред сè поради бројните тужби поднесени од засегнатите корисници. Со цел да го зачува угледот и да спречи идни безбедносни инциденти, Yahoo спроведе низа мерки преку пристапот на StrongDM, кои вклучуваат:

1. **Силна енкрипција и контрола на пристап** — Спроведување на современи стандарди за енкрипција и обезбедување дека само овластени корисници имаат пристап до чувствителни системи.
2. **Мултифакторска автентикација (MFA)** — Зајакнување на безбедноста при најава со барање повеќе форми на автентикација.
3. **Детекција на прекршувања во реално време** — Идентификување и неутрализирање на обидите за неовластен пристап уште во почетната фаза.
4. **Континуирани безбедносни ревизии** — Откривање на потенцијални ранливости и погрешни конфигурации пред тие да бидат злоупотребени од напаѓачите.
5. **Протоколи за автоматизиран одговор** — Брза реакција при појава на безбедносни инциденти, со цел минимизирање на евентуалната штета.

Со воведувањето на овие засилени безбедносни мерки, компанијата значително ја намали можноста за повторување на напади со ваков обем и придонесе кон стабилизирање и обновување на својот углед.

¹ **MD5 (Message Digest 5)** — криптографска хеш-функција развиена во 1991 година од страна на Роналд Ривест. Функцијата генерира 128-битен хеш (32-цифрен хексадецимален излез) од даден влез



Слика 24. Дијаграм на текот на нападот во случајот Yahoo Breach

IX.II Фишинг закани кон Gmail и одбранбените механизми на Google

Освен случајот со Yahoo, слични фишинг напади беа регистрирани и врз корисничките сметки на Gmail, сопственост на компанијата Google. Напаѓачите испраќале електронски пораки од лажни е-адреси кои визуелно и структурно биле речиси идентични со легитимните известувања што Google ги користи при својата официјална комуникација со корисниците.

Во овие пораки најчесто било наведено итно предупредување дека Google наводно добил судска покана со која се бара копија од корисничката сметка. Со оваа тактика, напаѓачите се обидуваа да предизвикаат чувство на страв и итност кај примателот, со цел да го наведат да кликне на прикачен линк кој изгледал како официјална страница за помош на Google.

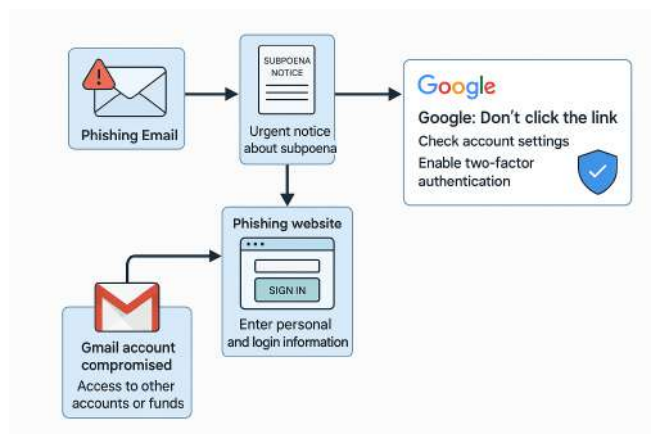
Сепак, зад оваа маска се криела мошне вешта имитација со единствена цел – да го натера корисникот доброволно да внесе лични податоци и информации за најавување. Доколку корисникот паднел во замката, напаѓачите не само што добивале пристап до Gmail сметката, туку преку пристап до содржината на електронската пошта можеле да пронајдат

дополнителни податоци за пристап до други услуги, финансиски сметки, па дури и да извршат финансиски злоупотреби [27] (Слика 25).

Со цел да го минимизира ризикот и да ги заштити своите корисници, Google презеде повеќе активности за подигнување на безбедносната свест. Компанијата објави официјално предупредување до своите 1,8 милијарди корисници да не кликуваат на сомнителни линкови и да внимаваат при отворање на е-пошта со сомнителна содржина. Истовремено, Google им препорача на корисниците да ги проверат безбедносните поставки на своите сметки и да преземат неколку основни мерки за заштита:

1. **Промена на лозинката:** редовно ажурирање на лозинките со посилни и посложени комбинации.
2. **Активирање на двофакторска автентикација (2FA):** дополнително ниво на безбедност, при што покрај лозинката, потребно е и внесување на код испратен на мобилниот телефон на корисникот.
3. **Безбедносни напомени:** Google потсетува дека никогаш не бара лозинки преку е-пошта, ниту иницира телефонски повици со такви барања.

Со ваквиот пристап, Google не само што се обидува да го ограничи влијанието на сајбер-нападите врз угледот на компанијата, туку и активно придонесува кон подигнување на свеста кај корисниците за важноста на навремената заштита од фишинг напади преку примена на соодветни превентивни мерки.



Слика 25. Gmail фишинг - тек на напад

IX.III Фишинг напади во банкарскиот сектор во Македонија: Примери од Охридска банка и Комерцијална банка

Еден од позначајните регистрирани примери на фишинг напади во Република Македонија се случи врз клиентите на Охридска банка, каде што напаѓачите користеле различни методи за компромитирање на лични и финансиски податоци. Во еден од случаите, клиентите добивале електронски пораки од непознат испраќач, при што во пораката бил прикачен RAR² документ кој лажно се претставувал како известување за добиена дознака од странство. Адресата од која била испратена пораката — *ohridska.banka@obsg.com* — визуелно потсетувала на легитимна, но сепак не соодветствувала со официјалната адреса на банката објавена на нејзината веб-страница. Освен преку електронска пошта, нападот се реализирал и преку креирање на лажна веб-страница со повик за учество во наградна игра, каде што од учесниците се барало да достават лични податоци како фотографија од лична карта, број на трансакциска сметка и



Слика 26. Препознавање на фишинг нападите и заштитни мерки

фотографија со бела позадина, овозможувајќи на напаѓачите да приберат чувствителни информации со можност за нивна понатамошна злоупотреба [29] (Слика 26).

Сличен вид на фишинг-активност беше забележан и врз клиентите на Комерцијална банка, каде напаѓачите

² **RAR документ** — формат за архивирање и компресија на датотеки кој овозможува собирање на повеќе датотеки во една компресирана архива со намалена големина.

добил пристап до нивните банкарски сметки и финансиски средства [28]. По добивањето на сознанија за постоењето на овие напади, двете банки презедоа итни мерки за информирање на клиентите, апелирајќи за зголемено внимание при отворање на сомнителни пораки, проверка на легитимноста на веб-страниците пред внесување на било какви податоци и користење на дополнителни безбедносни механизми, како што се двофакторската автентикација и редовна промена на лозинките. Со оваа стратегија не само што се намалува непосредниот ризик, туку се зајакнува и свеста кај корисниците за потребата од внимателно и одговорно управување со личните и финансиските информации во дигиталната средина

Х. СОВЕТИ ЗА КРАЈНИ КОРИСНИЦИ ПРИ ЗАШТИТА ОД ФИШИНГ НАПАДИ

Х.І Како да ги препознаете фишинг нападите

Клучни индикатори за препознавање на фишинг пораки се:

1. **Адреса на испраќачот:**

Потребно е да се провери дали е-адресата е точна и дали потекнува од официјален домен. Лажните е-адреси често имаат дополнителни букви, бројки или домени кои личат на вистинските.

2. **Предмет на пораката:**

Фишинг пораките често користат алармантни наслови за да предизвикаат паника кај корисникот.












3. **Јазик и стил:**

Лажните пораки може да содржат граматички и правописни грешки, чуден стил на изразување, па дури и машински превод.

4. **Линкови:**

Со поставување на глумчето над линкот за да ја видите целната веб-адреса. Доколку не се совпаѓа со очекуваната, потребно е да не се кликува.

5. **Итност:** Пораката бара да преземете итна акција, на пример веднаш да го потврдите налогот, да внесете лозинка или да доставите финансиски податоци.

Comparison: Phishing Email vs. Legitimate Email		
	Phishing	Legitimate
Sender	 support@bank-security-alert.com	 support@bank.com
Subject	 Confirm your account immediately!	 Account statement notification
Content	 Your account will be suspended if you do not respond within 24 hours	 Standard monthly notification
Link	 http://bank-login-verify.com	 https://bank.com/login
Request	 Provide password, SSN, credit card	 No request for personal data
	 Provide password, SSN, credit card	 No request for personal data

Слика 27. Споредба: фишинг порака и легитимна порака

6. **Барање за лични податоци:** Реномирани институции/компаниии никогаш не бараат да им се испрати лозинка, податоци за кредитна картичка или лична карта преку е-пошта.
7. **Сомнителни прилози:** Многу фишинг пораки содржат малициозни прилози (на пример ZIP, RAR, EXE, PDF) кои може да инсталираат вирус или ransomware.
8. **Проверка со институцијата:** Доколку се сомневате, директно контактирајте ја институцијата/компанијата преку официјалните канали, за потврда на автентичноста на пораката [33].

Х.II Што да направите ако сте цел на фишинг напад

Доколку сме станале жртва на фишинг напад, или има сомнеж дека се кликнуло на сомнителен линк, или се доставили лични податоци, неопходно е да дејствува брзо, односно:



Слика 28. Што да направите по фишинг напад

1. **Да се престане со понатамошна интеракција:** Да не се кликнува на дополнителни линкови, да не се отвараат прилози и да не се внесуваат дополнителни податоци.
2. **Промена на лозинки:** Итно да се промени лозинката на компромитираната сметка и на сите останати сметки каде што истата лозинка е користена.
3. **Активирање на двофакторска автентикација:** Да се додаде дополнително ниво на заштита за најавување.
4. **Проверка на активност:** Да се прегледа историјата на најави, промени и трансакции. Доколку се забележи сомнителна активност, истата веднаш да се пријави.

5. **Известување на институцијата/компанијата:** Веднаш да се информира институцијата/компанијата или банката за сомнителната активност. Повеќето институции/компаниии, а особено банките имаат посебни оддели за сајбер безбедност кои се достапни 24/7.
6. **Антивирусно скенирање:** Потребно е секогаш да се скенира уредот со ажурирана антивирусна алатка, за да се провери дали постои злонамерен софтвер - вирус.
7. **Пријавување на нападот:** Потребно е да се информираат локалните институции/компаниии за сајбер-нападот.
8. **Известете ги контактите:** Доколку сопственикот на е поштата се сомнева дека неговата е-пошта била злоупотребена, потребно е веднаш да ги известат сите блиски лица и деловни соработници за да бидат претпазливи [35].
- 9.

X.III Password менаџери и добри практики за лозинки

Управувањето со лозинките е суштински дел од личната сајбер-безбедност. За олеснување на безбедното чување на лозинки се препорачува користење на password менаџери [34].

Главните предности на менаџерите за лозинки се [38]:

1. **Создавање силни лозинки:** Менаџерите автоматски генерираат комплексни, долги и уникатни лозинки за секоја сметка, со што се намалува ризикот од компромитација.
2. **Безбедно складирање:** Лозинките се складираат во силно енкриптирана база на податоци, заштитена со главна лозинка (master password).
3. **Автоматско пополнување:** Го олеснуваат процесот на најавување, автоматски внесувајќи ги корисничкото име и лозинката при пристап до веб-страниците.
4. **Заштита од фишинг:** Менаџерите за лозинки внесуваат лозинка само на вистинските, легитимни веб-страници. Ако страницата е лажна, менаџерот нема да понуди пополнување, со што ви сигнализира дека нешто не е во ред.

5. **Управување со лозинки на повеќе уреди:** Повеќето менаџери нудат синхронизација на лозинките меѓу различни уреди — компјутери, мобилни телефони и таблети.
6. **Известување за компромитирани лозинки:** Некои менаџери нудат и известување доколку некоја лозинка била компромитирана при пробивање на некоја услуга.

Добри практики за лозинки:

1. Да се користат најмалку 12 карактери.
2. Да се комбинираат големи и мали букви, броеви и специјални знаци.
3. Да се избегнуваат употреба на лични информации во лозинките (име, датум на раѓање и сл.)
4. Редовно ажурирање на лозинките.
5. Никогаш да не се споделуваат лозинки со други лица.

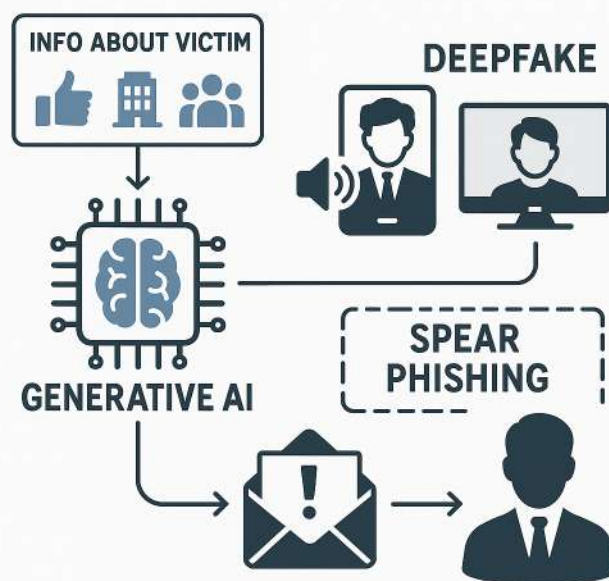
XI. ПРЕДИЗВИЦИ И ИДНИ НАСОКИ

XI.I Напредни фишинг техники (deepfake, AI-generated email)

Современите фишинг напади значително ја надминуваат класичната масовна испорака на лажни пораки кои се препознаваат по правописни грешки и едноставни шаблонски измами. Со појавата и забрзаниот развој на генеративната вештачка интелигенција (Generative AI), напаѓачите сега располагаат со многу понапредни алатки кои им овозможуваат да создадат понапредни фишинг пораки [30]. Овие пораки се прилагодуваат според навиките, стилот на комуникација и интересите, правејќи ги речиси идентични со легитимната електронска порака. Благодарение на пристапот до големи количини на јавно достапни податоци преку социјалните мрежи, јавни регистри и претходно компромитирани бази на податоци, напаѓачите можат да креираат напади што ја експлоатираат конкретната работна функција или тековните активности на жртвата.

Еден од најопасните аспекти на оваа нова генерација напади е примената на deepfake технологиите. Со нивна помош, напаѓачите успеваат да генерираат лажни аудио повици од луѓе на високи позиции, да креираат видеа во кои преку симулација на движење на лицето и говорот се имитира реална личност, како и да испраќаат визуелно и тонски совршено синхронизирани пораки со висок степен на убедливост. Ваквите напади можат да предизвикаат сериозни последици, особено кога се насочени кон вработени со пристап до финансиски или доверливи податоци (Слика 29) [31].

Особено се издвојуваат новите форми на таргетиран фишинг, познат како spear-phishing, каде што фокусот е ставен на индивидуални жртви или помали групи со цел зголемување на веројатноста за успех на нападот. Во овој



Слика 29. Напредни фишинг техники

контекст, моделите како што се GPT-4, Claude и Gemini им овозможуваат на напаѓачите да генерираат хипер-реалистични и контекстуално соодветни електронски пораки, кои изгледаат како да се испратени од легитимни извори. Овие пораки може да содржат лажни понуди за вработување, измамнички инструкции за финансиски трансфери, или симулирани барања од ИТ одделот за ажурирање на лозинки или пристапни информации, со што значително се зголемува опасноста од компромитирање на организациските системи [32].

XI.II Email security automation (SOAR, SIEM поврзување)

Современите системи за заштита на електронската пошта сè повеќе се надградуваат со автоматизирани платформи кои овозможуваат побрзо, поефикасно и попрецизно справување од безбедносните закани. Благодарение на ваквите решенија, организациите се во можност проактивно да ги идентификуваат и елиминираат заканите уште во нивната рана фаза.

Еден од клучните столбови на ваквата автоматизација претставуваат системите за **Security Orchestration, Automation, and Response (SOAR)**. Овие платформи овозможуваат автоматизирана анализа на сомнителните пораки, нивно класифицирање според ниво на ризик, како и иницирање на однапред дефинирани безбедносни процедури за изолација и обработка на инцидентите [36]. Преку SOAR, веднаш по детектирање на потенцијална закана, може да се активира аларм, да се изолира сомнителната порака, да се блокира понатамошниот пристап и да се проследи случајот до безбедносните тимови за дополнителна анализа, со што значително се намалува времето за одговор и ризикот од ескалација.

Покрај SOAR, во рамките на безбедност на електронска пошта сè почесто се применуваат и системите за **Security Information and Event Management (SIEM)**. Овие системи овозможуваат централно собирање, складирање и анализа на логови и настани од различни делови на организациската ИТ инфраструктура, вклучително и од системите за електронска пошта [37]. SIEM платформите овозможуваат корелација на настаните од повеќе извори, со што се зголемува можноста за откривање на сложени напади кои вклучуваат повеќе чекори,

како што се комбинирани фишинг напади, привилегирани злоупотреби или lateral movement³ напади внатре во мрежата.

Преку интегрирање на SOAR и SIEM во заштитата на електронската пошта, институциите/компаниите обезбедуваат побрза реакција, значително намалување на трошоците поврзани со рачно управување и постојана видливост врз актуелните безбедносни ризици. Таквата интеграција станува сè понеопходна, особено во услови кога заканите стануваат посоефистицирани, а бројот на инциденти и обемот на податоци за анализа континуирано расте.

³ **Lateral movement** (буквално: *странично движење*) претставува техника што ја користат хакерите откако ќе стекнат почетен пристап до некој систем или мрежа. Наместо веднаш да го искористат тој пристап, тие се движат „странично“ низ мрежата.

XII. ЗАКЛУЧОК

Електронската пошта, од нејзиното појавување па сè до денес, останува клучен сегмент во дигиталната комуникација и основен инструмент во секојдневното функционирање на деловниот, академскиот и приватниот живот. Иако нејзиниот развој започна како релативно едноставен технички концепт за размена на пораки, денес таа претставува комплексен систем со многубројни функционални и безбедносни предизвици. Со напредокот на технологијата, а особено со брзиот развој на интернетот, електронската пошта прерасна во глобално средство за комуникација, но истовремено стана и една од најексплоатираните платформи од страна на сајбер-криминалците.

Историјата на безбедносни инциденти јасно покажува дека фишингот, спуфирањето, злонамерните прилози и социјалниот инженеринг се најчестите техники што се користат за компромитација на системи и крадење чувствителни информации. Особено загрижувачки е фактот што напаѓачите стануваат сè поиновативни, користејќи напредни алатки како што се генеративна вештачка интелигенција и deepfake технологии за да создадат високо персонализирани и реалистични фишинг пораки. Благодарение на пристапот до огромни количини на јавни податоци, можноста за креирање на целосно убедливи лажни пораки и аудио-визуелни манипулации денес е значително зголемена. Нападите како спер-фишинг, BEC (Business Email Compromise) и рансомвер преку е-пошта веќе се стандардна алатка на напаѓачите.

Одговорот на овие закани не може да се темели само на една технологија или метод. Денешната заштита на електронската пошта се базира на повеќеслоен пристап, кој вклучува комбинација на криптографски стандарди како S/MIME и PGP за заштита на содржината, автентикациски механизми како SPF, DKIM, DMARC и BIMI за потврда на идентитетот на испраќачите, како и системи за автоматска анализа и одговор како што се SOAR и SIEM. Овие системи овозможуваат проактивно следење, детекција и изолација на потенцијални закани уште пред да предизвикаат сериозни последици. Дополнително, употребата на вештачка интелигенција за интелигентно филтрирање на несакана пошта овозможува динамично прилагодување на одбраната во реално време кон новите форми на напади.

Меѓутоа, и покрај сета техничка софистицираност, човечкиот фактор останува најважен елемент во заштитата. Недоволната едукација, слабите лозинки, невнимателното кликување на линкови и отворање на сомнителни прилози сè уште се главните причини за успешноста на многу од денешните напади. Затоа, континуираната едукација на корисниците, градењето на безбедносна култура и внимателното почитување на препорачаните безбедносни практики се подеднакво важни како и техничките решенија.

Безбедноста на електронската пошта претставува динамична и постојано еволуирачка област. Како што технологиите напредуваат, така и заканите стануваат посложени, што налага константна адаптација, инвестиција во нови решенија и развој на вештини. Само ако се комбинираат техничките мерки, правилата во организацијата и одговорното однесување на луѓето, може да се обезбеди сигурна и стабилна заштита на е-поштата, која ќе може да се справи со сегашните и идните закани.

XIII. РЕФЕРЕНЦИ

- [1] <https://www.verizon.com/business/resources/reports/dbir/>
- [2] <https://mk.wikipedia.org/wiki/>
- [3] <https://www.emailonacid.com/blog/article/email-marketing/history-of-email/>
- [4] <https://www.fbi.gov/history/famous-cases/morris-worm>
- [5] <https://www.orange cyberdefense.com/be/blog/legendary-hacks-1-the-morris-worm>
- [6] <http://www.jaedworks.com/shoebox/coleslaw.html>
- [7] <https://www.geeksforgeeks.org/e-mail-format/>
- [8] <https://www.rfc-editor.org/rfc/rfc5598.pdf>
- [9] <https://slideplayer.com/slide/13850137/>
- [10] <https://mailtrap.io/blog/email-infrastructure/>
- [11] <https://www.imperva.com/learn/application-security/phishing-attack-scam/>
- [12] <https://www.sanctionscanner.com/knowledge-base/what-are-phishing-attacks-881>
- [13] <https://www.darktrace.com/cyber-ai-glossary/business-email-compromise>
- [14] <https://www.bbc.com/news/technology-39901382>
- [15] <https://www.kaspersky.com/resource-center/definitions/spoofing>
- [16] <https://www.paubox.com/blog/what-is-a-malicious-email-attachment>
- [17] <https://sprinto.com/blog/cyber-security-goals/>
- [18] <https://www.proofpoint.com/us/threat-reference/spf - SPF>
- [20] <https://www.mimecast.com/content/dkim/>
- [21] <https://www.fortinet.com/resources/cyberglossary/dmarc>
- [22] <https://www.globalsign.com/en/blog/what-is-s-mime>
- [23] <https://www.varonis.com/blog/pgp-encryption>
- [24] <https://www.litmus.com/blog/what-is-bimi-and-why-should-email-marketers-care>
- [25] <https://www.spaceship.com/blog/ai-spam-filtering/>

- [26] <https://www.strongdm.com/what-is/yahoo-data-breach>
- [27] <https://samsungmagazine.eu/mk/2025/05/15/gmail-je-pod-phishing-utokem/>
- [28] <https://4news.mk/izmamnitsi-go-koristat-imeto-na-komertsijalna-banka-za-fishing-napad/>
- [29] <https://kanal5.com.mk/ohridska-banka-predupreduva-za-fishing-napadi-i-zloupotreba-na-licni-podatoci-od-nepoznati-storiteli/a396168>
- [30] <https://www.1kosmos.com/security-glossary/key-distribution-center/>
- [31] <https://ironscales.com/glossary/deepfake-phishing>
- [32] https://www.mailjet.com/blog/deliverability/what-is-phishing/?utm_source=google&utm_medium=cpc&utm_campaign=EU%20%7C%20EN%20%7C%20Search%20%7C%20DSA&utm_id=2090162100&utm_content=183232309907&utm_term=&utm_term=&utm_campaign=2090162100&utm_content=&utm_source=google&utm_medium=cpc&creative=755071011041&keyword=&matchtype=&network=g&device=c&gad_source=1&gad_campaignid=2090162100&gbraid=0AAAAADk4LuqV0uDufPzTwALzCKCwB0e0N&gclid=Cj0KCQjwu7TCBhCYARIsAM_S3NhLyXbocbGIzABzxiTaXp_BksHyYI0A4VNMHWeRX9nflhHRPwwGUM8aAjekEALw_wcB
- [33] https://www.brainkart.com/article/Remote-User-Authentication-Principles_8473/
- [34] <https://www.techtarget.com/searchsecurity/definition/password-manager#:~:text=A%20password%20manager%20is%20a,access%20to%20a%20specific%20service.>
- [35] <https://www.lepide.com/blog/12-steps-to-take-to-recover-from-a-phishing-attack/>
- [36] <https://www.fortinet.com/resources/cyberglossary/what-is-soar#:~:text=SOAR%20stands%20for%20security%20orchestration,custom%2Dfit%20a n%20organization's%20needs.>
- [37] <https://www.ibm.com/think/topics/siem#:~:text=Security%20information%20and%20event%20management%2C%20or%20SIEM%2C%20is%20a%20security,chance%20to%20disrupt%20business%20operations.>
- [38] <https://www.kaspersky.com/resource-center/preemptive-safety/protecting-your-data-online-password-manager>