ANTI-PHISHING STRATEGIJA

ANTI-PHISHING STRATEGY

Džemal Kulašin*

ABSTRAKT

U ovom radu predstavlja se phishing kao jedan od najprominentnijih oblika cyber kriminala, pri čemu se kroz njegovo raščlanjivanje dolazi do projiciranja komponenti anti-phishing strategije. Tako se u radu, kao prva, analizira socijalna komponenta, odnosno djelovanje na ljudske resurse unutar poslovnih (i drugih) sistema te, kao druga, tehnološka komponenta, odnosno primjene odgovarajućih tehnologija u smislu preveniranja kako phishing-a, tako i drugih oblika cyber napada iz kategorije tzv. društvenog inženjeringa.

Ključne riječi: Phishing, društveni inženjering, elektronska pošta

ABSTRACT

In this paper, phishing is presented as one of the most prominent forms of modern cyber attacks, and through its analysis, the components of anti-phishing strategy are projected. Thus, the paper analyzes, firstly, the human component, i.e. the impact on human resources within business (and other) systems and, secondly, the technological component, i.e. the application of appropriate technologies in terms of preventing both phishing and other forms of cyber attacks from the category of so-called social engineering.

Keywords: Phishing, social engineering, e-mail

UVOD

Cyber napadi su iz godine u godinu sve učestaliji i malicioniziji[1], kako zbog tendencija digitalizacije i transformacije na elektronsko poslovanje, tako i pandemijskim uvjetima poslovanja, s obzirom da su se brojne kompanije i institucije različitih profila primorale dijelom preseliti u online môd, stvorivši tako i dodatne sigurnosne ranjivosti. Pritom, posebno je markantno da su glavni vektori cyber napada (i dalje!) iz kategorije društvenog inženjeringa (phishing i sl.), što znači da su ljudski resursi (ili jednostavnije, ljudi) najslabija karika u sistemima zaštite.

Bez sumnje, među najprominentnijim, a ujedno i najštetnijim oblicima cyber napada iz kategorije društvenog inženjeringa su tzv. phishing napadi[2,3]. Brojni pokazatelji i analize ukazuju da se čak 90% zlonamjernog softvera u svijetu isporučuje upravo tehnikama društvenog inženjeringa, gdje apsolutno dominira phishing[4]. Kako se u ovom slučaju radi o informacijsko-komunikacijskim tehnologijama kao sredstvom izvršenja, te kako se napad kategorizira kao društveni inženjering, na određeni način projiciraju se i komponente anti-phishing strategije.

KOMPONENTE ANTI-PHISHING STRATEGIJE

Phishing predstavlja kriminalnu radnju gdje cyber prevarant (eng. cybercrook) šalje e-mail s ciljem da prevarom dođe u

1 Najmalicioniziji oblik cyber napada na kompanije svakako je ransomware, a koji je u prvoj pandemijskoj godini zabilježio porast učestalosti od čak 250%.

2 U 2020. kao godini pandemije, phishing napadi u svijetu porasli su za čak 600%

3 https://cofense.com/solutions/topic/anti-phishing, pristup: 05.02.20222.

4 https://www.gartner.com/reviews/market/email-security, pristup: 03.02.2022.

* - Fakultet za menadžment i poslovnu ekonomiju Univerziteta u Travniku

posjed osjetljivih podataka korisnika kao što su brojevi kreditnih kartica, PIN-ovi, pristupni podaci bankama, matični brojevi itd. Svi ovi podaci korisnika predstavljaju njegov digitalni identitet i ako napadač uspije u namjeri da ih preuzme, može ih zloupotrijebiti na različite načine i time steći značajnu finansijsku dobit, što najčešće i jeste krajnji cilj.

Izražena dvojna priroda phishing napada jasno implicira da anti-phishing strategija mora imati (barem) dvije komponente anti-phishing strategije, a to su:

- Socijalna komponenta, odnosno djelovanje na ljudske resurse unutar poslovnih (i drugih) sistema te
- tehnološka komponenta, odnosno primjena odgovarajućih tehnologija, prvenstveno u smislu preveniranja phishing-a.

Prije same elaboracije pojedinih komponenti anti-phishing strategije, potrebno je osvrnuti se na funkcionisanje phishing napada.

FUNKCIONISANJE PHISHING-A

Već iz konteksta ove kriminalne radnje jasno je da se odnosi na "pecanje" on-line korisnika elektronskim mamcem, te je stoga i nastala karakteristična terminološka odrednica phishing kao korijen riječi fishing (eng. pecanje). Iz terminološke odrednice pecanje otkriva se i ciljanje hakera na nedovoljnu svijest ali i spoznaje korisnika o načinima i tehnikama očuvanja informacijske sigurnosti. Zbog toga se ova vrsta cyber kriminala svrstava u tzv. društveni inženjering[5], jer se koristi varanjem zasnovanim na afektivnim segmentima pojedinca gdje se korist napadaču producira na "slabostima" žrtve u smislu lakovjernosti, ishitrenosti i/ili neznanja.

Za predstavljanje načina funkcioniranja phishing-a korisno je opisati početke ove internet kriminalne radnje. Phishing kao oblik cyber kriminala prvi put se javlja u Americi 1996. godine kao radnja koja označava "upotrebu algoritma za hakovanje AOL sistema za naplatu online vremena". Naime, unos ključnih podataka kreditnih kartica kojima se putem Interneta plaća(la) naknada AOL-u na njihovom serveru bio je izazov za hakere koji nisu mogli "varati" server lažnim podacima te su svjesno razradili indirektnu strategiju putem "pecanja" korisnika. Strategija je podrazumijevala slanje velikog broja nasumičnih e-mail poruka koje su bile potpisane kao "Zaposleni u AOL" sa tekstom koji od korisnika traži da iz nekog vanrednog razloga utipka svoje pristupne podatke (npr. nalog će biti suspendiran, i sl.), čime se otvarao put hakerima za upad u ciljane serverske sisteme.

Način preuzimanja povjerljivih podataka dirigiran je tipom e-mail poruke koja se generira, gdje razlikujemo dva tipična slučaja:

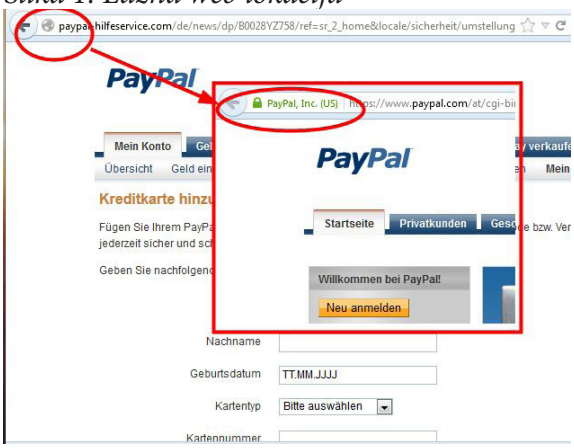
- lažna e-mail poruka i
- klonirani e-mail.

Lažni e-mail sadrži provokativni sadržaj za primatelja (npr. bankarski nalog je pred blokiranjem, i sl.), kako bi se korisnik naveo na ishitrenu reakciju, gdje se često kao prilog (eng. attachment) nalazi i keylogger kao spyware za praćenje rada tipkovnice žrtve. Klonirani e-mail, pak, zloupotrebljava brend kompanije (poput eBay, Amazon, PayPal, VISA, America online i sl.) kako bi se korisnik naveo da utipka (i time "pokloni") svoje podatke na sajtu kojeg uobičajeno koristi za novčane transakcije. Ovaj tip Internet prevare predstavlja (napredniji) oblik phishing-a označen kao pharming[6], što se u ovom kontekstu prevodi kao "uzgajanje žrtve" i "presretanje". Pharming napad je sofisticiraniji, i zahtijeva znatno viši nivo znanja napadača i računarske opreme. Koristi se koncept prevare gdje korisnika "na putu" do web sajta čiji URL utipkava presreće klonirani web sajt na koji sa punim povjerenjem unosi svoje podatke.

5 Pojam se često označava i kao socijalni inženjering

6 Termin je izveden kao veza sa terminom phishing te eng. riječi farming (uzgoj, uzgajanje)

Slika 1. Lažna web lokacija



Izvor: Hanić, H., Sućeska, M., 2008

Ukoliko se DNS (DNS - Domain Name Service, zadužen da pretvara Web i e-mail adrese u numeričke nizove) izmijeni tako da sadrži lažne informacije o tome koja Web adresa odgovara kojem nizu brojeva, svi korisnici koji otipkavaju odgovarajuću (ispravnu) Web adresu bivaju preusmjereni na lažnu. Iako ovaj postupak (nazvan još i DNS poison-ing) nije nov, kompleksnost pharming napada u punoj mjeri otkriva sigurnosne nedostatke Internet protokola, nastale još onda kada je kreiran.

Za sprovođenje manjih pharming napada koriste se posebni virusi upućeni elektronskom poštom koji prepisuju lokalne host fajlove na napadnutim računarima. Host fajl pretvara URL adrese u numeričke nizove koji su razumljivi za računar, tako da ugroženi host fajl uzrokuje da korisnik bude usmjeren ka pogrešnom web sajtu, čak i ako korektno utipka URL adresu legitimne Web lokacije. Takođe, napadač može koristiti i XSS (Cross-site scripting) napad te iskoristiti propuste u dizajnu web stranica za preusmjeravanje žrtvi na lažne web stranice gdje žrtve otkrivaju osjetljive podatke potrebne cyber kriminalcu da dođe do novca ili osjetljivih podataka korisnika.

TEHNOLOŠKA KOMPONENTA ANTI-PHISHING STRATEGIJE

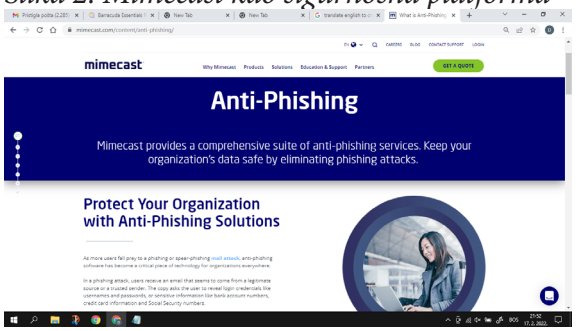
Kao prvi zid odbrane (i) od phishing napada logično se nameće tehnologija, odnosno standardni sigurnosni alati kao temeljni sigurnosni bedem, kao što su antivirusni softver i firewall. Pri tome, podrazumijeva se redovno ažuriranje anti-malware softvera, kao i redovno instaliranje najnovijih zakrpa i instalacija verzija svih ostalih programa u kojima su ispravljeni sigurnosni propusti. Ipak, najuže vezano za zaštitu od phishing (i drugih oblika phishinga, tj. pharming-a i spear phishing-a) je i instaliranje tzv. sigurnosnih ekstenzija za pretraživače (eng. browser) koje koristimo na Internetu. Tako, za browser-e pod aktuelnim operativnim sistemima (Windows, Mac i Linux) postoje različite sigurnosne ekstenzije, a najčešće u upotrebi su sljedeće: Netcraft Toolbar, TrustWatch Toolbar, ScamBlocker, PhishNet, SpoofGuard, Cloudmark itd. Doduše, treba naglasiti da pojedini savremeni browser-i, poput Google Chrome-a, već koristi zaštitni sistem Safe browsing technology koji skenira svaku web lokaciju koju korisnik posjećuje te na određeni način upozorava ako je lokacija sumnjiva. Sigurnosne ekstenzije prikazuju se kao dodatni toolbar-i u pretraživačima skenirajući web promet slično Safe browsing technology-ju, te u slučaju navođenja korisnika na kloniranu web lokaciju ne ponavljaju njen naziv (npr. Ebay.com) već navode "odgovarajuću" IP adresu, što je signal da se radi o kompromitiranoj lokaciji na kojoj ne treba izvoditi bilo kakve transakcije.

No, u tehnološkom smislu, vezano ne samo striktno za zaštitu od phishing-a već i već i svih oblika prijetnji je implementiranje zasebnih softverskih rješenja za sigurnost elektronske pošte (eng. E-mail Security Software). Riječ je, u stvari, o sigurnosnim platformama poznatijim pod akronimom SEG (eng. Secure E-mail Gateway) kao svojevrsnom firewall-u elektronske pošte kojeg implementiraju mnogobrojne organizacije u svijetu. Lista sigurnosnih rješenja prilično je duga, ali su ipak markantnija određena poslovna rješenja, poput:[7]

7 https://www.gartner.com/reviews/market/email-security, pristup: 03.02.2022.

- Proofpoint Email Protection Suite,
- Avanan,
- Mimecast Secure Email Gateway,
- Barracuda Email Security Gateway,
- Cisco Secure Email,
- Trend Micro Cloud App Security,
- FortiMail,
- Symantec Email Security,
- Microsoft Defender for Office 365 i sl.

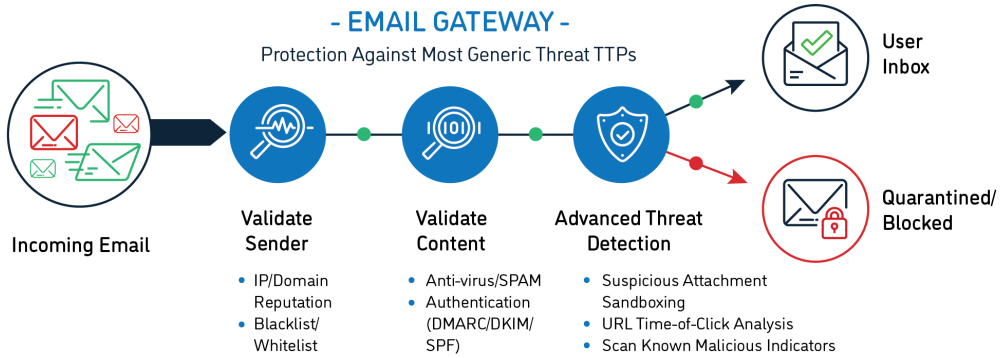
Slika 2. Mimecast kao sigurnosna platforma



Izvor: https://www.mimecast.com

Karakteristično za SEG je da rješenja predstavljaju sigurnosne platforme koje proaktivno i u realnom vremenu skeniraju ulaznu, odlaznu i internu e-poštu u cilju eliminacije (u ovom slučaju, blokiranje ili preusmjerevanje u karantin) ili dozvole prolaska do korisničkog inbox-a (slika 3).

Slika 3. Princip rada SEG platformi



Izvor: https://www.mimecast.com

SEG platforme su, inače, mahom temeljene na SaaS-u (dakle, clouding platforme) čime organizacije oslobađaju obaveza kupovine novog hardvera i (skupog) softvera, izuzev obaveza predvidljivih i prihvatljivijih troškova mjesečne ili godišnje pretplate.

SOCIJALNA KOMPONENTA ANTI-PHISHING STRATEGIJE

Ipak, tehnološka osnova, iako maksimalno važna i nužna, apsolutno nije i dovoljna u zaštiti od phishing-a. Naime, phishing napadi su, kako je istaknuto, dominantno kategorija društvenog inženjeringa te se stoga i zaštita u presudnoj mjeri svodi na korisnike, odnosno na njihovo online ponašanje. Oprez se posebno odnosi na korištenje e-mail servisa, odakle se mahom i generiraju problemi, jer i pored SEG rješenja, brojne maliciozne e-mail poruke, zbog svog socijalnog karaktera, ipak dolaze do odredišne tačke, tj. do korisnika. Dakle, korisnike je potrebno sistemski obučavati u smislu online ponašanja, gdje posebno trebaju pratiti svoj inbox u kojeg svakodnevno stižu brojne e-mail poruke među kojima se kroz sigurnosne filtere "provlače" i sumnjive poruke gdje treba znati adekvatno reagovati. Najvažnije preporuke u edukaciji uposlenika (pri čemu se podrazumijeva i menadžment svih nivoa!) minimalno bi sadržavale set karakterističnih znakova koji ukazuju na potencijalni phishing, i koji se kratko obrazlažu u nastavku.

- E-mail poruka sadrži zahtjeve za osobnim podacima: Legalne kompanije mahom ne traže osobne podatke od svojih korisnika putem e-pošte, već koriste direktne kontakte. Dakle, treba biti maksimalno oprezan sa

e-mail porukama koje traže osobne podatke, iako izgledaju potpuno vjerodostojno.
- E-mail poruka od nepoznatog pošiljaoca: Teorijski, svaku poruku od nepoznatog pošiljaoca treba pretpostaviti potencijalno sumnjivom. Dodatni oprez treba biti ako poruka nema naslov (subject), jer to predstavlja temeljno narušavanje e-mail korespondencije.
- E-mail poruka sadrži očigledne pravopisne greške: Svaku poruku koja sadrži očigledne pravopisne greške ili greške u stručnim finansijskim terminima (ako poruka dolazi od "finansijske institucije", što najčešće i jeste slučaj) treba tretirati sumnjivom. Kodeks nalaže i pravilnu strukturu e-mail poruke ali i konzistentnost sadržaja u smislu da se koriste valjani ekonomski termini, te svako uočeno odstupanje ukazuje na lažni e-mail.
- Hitnost u sadržaju: Lažni e-mail karakterizira provocirajući sadržaj koji iziskuje hitnu reakciju primatelja, odnosno žrtve. Primjer iz jedne otkrivene phishing prevare je sljedeći: "Dragi korisniče banke, ustanovili smo kako je potrebno ažurirati podatke o vašem računu zbog neaktivnosti, prevare ili izvještaja o prevari. Ako ne ažurirate vaše podatke, račun će biti obustavljen. Slijedite ovaj link i potvrdite vaše podatke".
- Prilozi: Mnoge phishing prevare traže od korisnika otvaranje priloga koji zatim mogu na računar "prenijeti" virus ili spyware. Ako se na računar instalira key-logger kao aktuelna vrsta spyware-a, on može "snimati" rad tipki kojima se unosi korisničko ime i lozinku osobnih internetskih računa. Prilog koji se želi pregledati treba najprije spremiti i zatim skenirati korištenjem ažurnog antivirusnog programa prije nego što se otvori. Ovdje može pomoći i ozbiljan e-mail klijent (kakav je npr. MS Outlook) koji automatski blokira određene priloge koji mogu sadržavati viruse; u slučaju da Outlook otkrije sumnjivu poruku, prilozi s bilo kojom vrstom datoteke se blokiraju.
- Lažni linkovi: Prevaranti koji koriste phishing poruke su vrlo sofisticirani kad se radi o stvaranju lažnih linkova i prosječnoj osobi je gotovo nemoguće prepoznati je li veza legalna. Uvijek je najbolje u preglednik ručno unijeti web-adresu ili jedinstveni lokator resursa (URL) za koji se zna da je tačan, a posebno treba izbjegavati popularni Copy - Paste, tj. kopiranje i lijepljenje URL-a iz poruke u preglednik.
- Maska na linku: Iako "link" sadrži čitav ili djelomični naziv prave kompanije, ipak može biti i "maskiran". To znači da link koji se vidi ne vodi na tu adresu već negdje drugdje, obično na lažno web-mjesto.
- Homografi[8]: Na računarima, homografski napad je Internetska adresa koja izgleda kao poznata Internetska adresa, ali je zapravo izmijenjen; npr. www.microsoft.com može izgledati kao www.micosoft.com ili www.mircosoft.com. Svrha ovakvih lažnih web-linkova koji se koriste u phishing prevarama je prevariti žrtvu tako da ih klikne. Cyber kriminalci lažiraju uglavnom nazive domena banaka kako bi prevarile korisnike i uvjerile ih kako posjećuju poznata i povjerljiva web-mjesta, kakvo je svakako web mjesto svoje banke.
- URL sadrži "nemoguću" domenu: Osobe koje šalju phishing poruke često se oslanjaju na činjenice da mnogi e-mail korisnici ne znaju način strukturiranja domena, gdje je zadnji dio domene najbitniji. Npr. domena info.facebook.com je poddomena facebook.com, jer se facebook.com pojavljuje na kraju cijelog naziva domene (na desnoj strani). Na osnovu toga, facebook.zlonamjernadomena.com ne potiče od facebook.com, jer se facebook.com nalazi na lijevoj strani naziva domene, umjesto na desnoj. Prevarant jednostavno kreira poddomenu s imenom facebook ili slično, a rezultirajući naziv domene izgleda ovako:
- facebook.zlonamjernadomena.com.

Na ovaj način prevaranti pokušavaju uvjeriti žrtve da poruka dolazi od digitalnog brenda kao što je Facebook, Microsoft i sl.

- URL lokacije ne sadrži https. Dio https u URL-u web lokacije (npr. bankarske

8 Homograf je riječ koja se piše jednako kao druga riječ, ali ima drugo značenje.

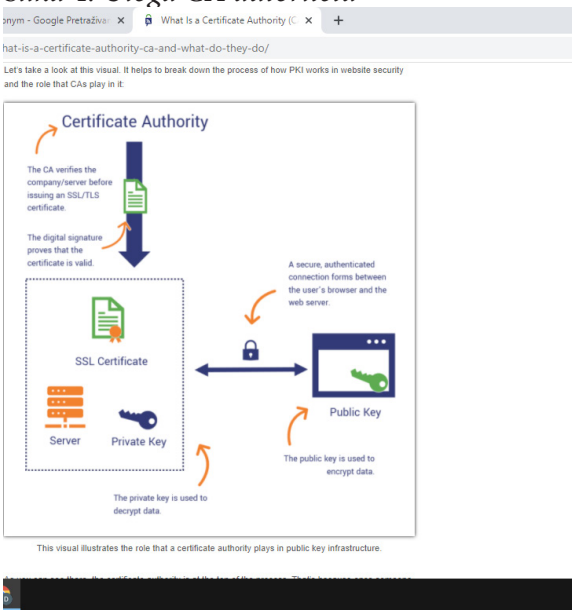
institucije) potvrđuje da se između servera i browsera uspostavlja enkriptirani podatkovni kanal osiguran tzv. SSL sigurnosnim slojem (SSL - Security Socket Layer). Ovaj zaštitni sistem označava se i ikonom katančića, na kojem se može izvršiti i validacija određene lokacije koja treba rezultirati digitalnim certifikatom izdatog od strane odgovarajućeg CA autoriteta (CA - Certification Authority), čija validnost se, između ostalog, dokazuje i terminom valjanosti (Valid from:). U svakom slučaju, ako URL online kompanije gdje se izvode finansijske transakcije) počinje sa http umjesto sa https - znak je da se radi o kloniranoj stranici na kojoj ni u kojem slučaju korisnik ne smije unositi bilo koje osobne poodatke, a posebno brojeve kreditnih kartica ili pristupne podatke (user i password).

Upravo je ova posljednja navedena stavka (URL web lokacije institucije ne sadrži https) ujedno i najvažnija. Naime, SSL sloj (eng. Secure Sockets Layer) nije ništa drugo do (famozni) digitalni certifikat zasnovan na PKI-i[9] koji dokazuje identitet jedne web lokacije (u ovom slučaju, govorili smo o bankama, iako je u suštini sve jednako). Princip je sljedeći:

- na jednoj strani, pretraživač korisnika u realnom vremenu koristi javni ključ određene web lokacije čime odašilje šifrirane poruke,
- na drugoj strani, također u realnom vremenu, ciljana web lokacija koristi svoj privatni ključ za dešifriranje poruka.

Na ovaj način, tj. upotrebom jake kriptografije i realiziranja transfera podataka u realnom vremenu, nema bojazni od otkrivanja povjerljivih podataka cyber kriminalcima. No, treba naglasiti da se apsolutno podrazumijevaju digitalni certifikati pouzdane treće strane, tj. nekog od ovlaštenih CA autoriteta.

Slika 4. Uloga CA autoriteta



Izvor: https://www.thesslstore.com

ZAKLJUČAK

Kako je u radu predstavljeno, u slučaju phishing-a radi se o dvojnoj prirodi napada, gdje se pored IKT-a kao sredstva izvršenja involvira i ljudski faktor, koji se u sistemima pokazuje i kao najslabija karika u sistemima zaštite. Zbog toga smo i projicirali (minimalno) dvije komponente anti-phishing anti-strategije: a) socijalnu komponentu, odnosno djelovanje na ljudske resurse unutar poslovnih (i drugih) sistema te b) tehnološku komponentu, odnosno primjene odgovarajućih tehnologija, u smislu preveniranja phishing-a, ali i drugih oblika cyber napada.

Shodno izloženom, može se zaključiti da tehnološka komponenta anti-phishing strategije ipak nije i dovoljna, jer su phishing napadi dominantno kategorija društvenog inženjeringa, te se i zaštita u konačnici svodi na krajnjeg korisnika. Stoga je u svim organizacijama potrebno provoditi forsirati upravo socijalnu komponentu anti-phishing strategije, što u praksi znači provoditi sistemske i kontinuirane edukacije svih uposlenika, uključujući i sve nivoe menadžmenta. Pritom je svakako fokus na e-mail servisima, jer se i pored implementacije SEG platformi brojne maliciozne e-mail

9 PKI – Public Key Infrastructure, o čemu se kasnije zasebno govori

poruke, zbog svog socijalnog karaktera, ipak "provlače" kroz sigurnosne filtere.

LITERATURA

[1] Hanić, H., Sućeska, M., (2008), Kompjuterski kriminal - pojavni oblici i preventiva, Fakultet
[2] kriminalističih nauka Univerziteta u Sarajevu, Sarajevo
[3] https://fortistelecom.net/cyber-security/anti-phishing-strategy, pristup: 25.02.2022.
[4] https://www.gartner.com/reviews/market/email-security, pristup: 03.02.2022.
[5] https://www.n-able.com/blog/how-secure-email-gateway-can-protect-your-business, pristup: 05.03.2022
[6] https://cofense.com/what-is-a-seg, pristup: 04.03.2022
[7] https://cofense.com/solutions/topic/anti-phishing, pristup: 05.02.20222.
[8] https://www.mimecast.com/content/anti-phishing-software, pristup: 22.02.2022.
[9] https://www.thesslstore.com, pristup: 05.03.2022