Sigurnost e-pošte u digitalnom društvu

Brčić, Martina-Matija

Sveučilište u Zadru

Stručni prijediplomski studij

Informacijske tehnologije

Martina-Matija Brčić

Sigurnost e-pošte u digitalnom društvu

Završni rad

Zadar, 2024

Sveučilište u Zadru
Stručni prijediplomski studij
Informacijske tehnologije

Sigurnost e-pošte u digitalnom društvu

Završni rad

Student/ica:
Martina-Matija Brčić

Mentor/ica:
prof.dr.sc. Dino Županović

Zadar, 2024.

Izjava o akademskoj čestitosti

Ja, **Martina-Matija Brčić,** ovime izjavljujem da je moj **završni** rad pod naslovom **Sigurnost e-pošte u digitalnom društvu** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 17. ožujka 2024.

SADRŽAJ

SAŽETAK

Sigurnost e-pošte u suvremenom digitalnom društvu predstavlja složen i vitalan aspekt komunikacije koji zahtijeva duboku analizu i strategije zaštite. E-pošta, kao osnovno sredstvo komunikacije, suočava se s brojnim izazovima i prijetnjama sigurnosti. Ključni protokoli, poput SMTP-a, omogućuju prijenos poruka, ali istovremeno otvaraju vrata za sofisticirane napade poput phishinga, malwarea i spama, čime se ugrožava integritet i povjerljivost podataka.

Edukacija korisnika o sigurnosnim postupcima i tehnologijama koje se koriste u e-pošti igra kritičnu ulogu u prevenciji i odgovoru na prijetnje. Razumijevanje složenih mehanizama autentifikacije, kriptografskih tehnika i mehanizama zaštite podataka presudno je za stvaranje otpornog okvira u digitalnom okruženju. Primjeri stvarnih napada, poput visokosofisticiranih phishing kampanja koje ciljaju na specifične organizacije ili institucije, ističu potrebu za kontinuiranom edukacijom, prevencijom i svjesnošću o sigurnosti.

U konačnici, sigurnost e-pošte zahtijeva holistički pristup koji kombinira tehničke, organizacijske i ljudske resurse kako bi se osigurala zaštita od širokog spektra napada i prijetnji u digitalnom okruženju.

KLJUČNE RIJEČI: sigurnost, protokoli, e-pošta, napadi, edukacija, prevencija

POPIS KORIŠTENIH KRATICA

EOP	Exchange Online Protection
SPF	Sender Policy Framework
DNS	Domain Name System
TXT	Text
DKIM	Domain Keys Identified Mail
MTA	Mail Transfer Agent
DMARC	Domain-based Message Authentication, Reporting and Conformance
MX	Mail Exchange
TTL	Time-To-Live
IP	Internet Protocol
A (record)	Address
AAAA	quad A
CNAME	Canonical Name
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
DANE	DNS-based Authentication of Named Entities
DNSSEC	Domain Name System Security Extension
TLSA	Transport Layer Security Authentication
RRset	Resource Record Set

RRSIG	Resource Record Signature
DS	Delegation Signer
DNSKEY	Domain Name System Key
ZSK	Zone-Signing Key
URL	Uniform Resource Locator
BEC	Business E-mail Compromise
NDR	Non Delivery Report

1. UVOD

U današnjem digitalnom dobu rijetki su oni koji nemaju elektroničku poštu ili se ne koriste istom svakodnevno. Elektronička pošta (odnosno e-pošta, nadalje e-mail) služi prvenstveno za brzu komunikaciju, kreiranje računa na različitim društvenim mrežama, pohranu različitih dokumenata i sl. Zbog povećane potrebe za korištenjem e-maila i korištenjem istog za razmjenu osjetljivih podataka (dokumenata ili potvrda o uplati), povećao se i broj usmjerenih napada na korisnike. Sve češće su krađe identiteta zbog slabih lozinki, provale u društvene mreže, slanje različitih poruka s prijetnjama ili lažnim predstavljanjem najčešće s ciljem dohvaćanja osjetljivih financijskih podataka.

Postoje različite vrste napada koje korisnici svakodnevno doživljavaju, a neke od njih su: spam, scam, različite vrste phishinga, spoofing, malware u e-mailu, i ostali. Kako se poboljšava sigurnost i razvijaju nove tehnologije tako su i napadi sve uvjerljiviji, kompleksniji i sofisticiraniji.

Cilj ovog rada je dati uvid u različite dijelove e-maila i analizirati vrste napada na primjerima iz stvarnog života. Primjeri su uz pisano odobrenje preuzeti na autoričinom trenutnom radnom mjestu te će sve osjetljive informacije biti izbačene. Preuzeti primjeri su iz Microsoft karantene stoga se u radu objašnjavaju servisi dostupni preko Microsoft platforme.

Rad je podijeljen u dva dijela. Prvi dio teorijski objašnjava općenito e-mail, Microsoft i različite e-mail napade, a u drugom dijelu analizirani su stvarni primjeri napada.

2. TEHNOLOGIJE KORIŠTENE U ZAVRŠNOM RADU - MICROSOFT

Microsoft je osebujna platforma koja pruža različite usluge privatnim korisnicima, ustanovama i korporacijama. Neke od usluga su: Outlook (služi za primanje i slanje e-maila), Exchange (poslužitelj za e-mail i kalendar), Microsoft Defender portal (rješenje u oblaku za zaštitu, istraživanje, detekciju, prevenciju različitih prijetnji prema elektroničkoj pošti, identitetu ili uređajima) i mnogi drugi koji nisu relevantni za ovaj rad.

U sklopu Microsoft Defender portala nalazi se tzv. karantena. Karantena je jedan oblik arhive u koju se spremaju opasni ili neželjeni e-mailovi koje je prepoznao Exchange Online Protection (EOP) ili Microsoft Defender. EOP i Defender su dva različita sustava, međutim oba imaju mogućnost prepoznavanja opasnih e-mailova. EOP obuhvaća e-mail, a Defender uključuje kompletan Office 365 (Microsoftov proizvod koji obuhvaća Excel, SharePoint, OneDrive itd.). Oba sustava rade zajedno koristeći različite metode zaštite.

2.1. EOP

EOP se odnosi na rješenje u oblaku koje prepoznaje i filtrira neželjene poruke. Funkcionira tako da štiti svaki mailbox, odnosno poštanski sandučić korisnika koji koristi Exchange uz pomoć zadanih politika, odnosno default policyja.

Uobičajeni tok podataka u EOP:

a. Reputacija - kada dolazni e-mail uđe u EOP, najprije prolazi kroz filtriranje veze koje provjerava reputaciju pošiljatelja. Većina neželjenih e-mailova se zaustavlja na ovoj točki i EOP ih odbija.
b. Zlonamjerni softver - zatim se e-mail pregledava u potrazi za zlonamjernim softverom. Ako se pronađe zlonamjerni softver u e-mailu ili privitku e-maila, dostavlja se u karantenu (ukoliko je organizacija drugačije postavila, na ovom stupnju se e-mail može odbiti, te server šalje automatsku obavijest pošiljatelju). Samo administratori mogu pregledavati i upravljati e-mailovima u karanteni zbog zlonamjernog softvera, ukoliko nije drugačije postavljeno. U tom slučaju se dozvoljava korisnicima da dobiju obavijest o e-mailovima koji su im poslani, a nalaze se u karanteni, te mogu zatražiti „puštanje“ e-mailova ukoliko su prepoznali legitimnu komunikaciju.

c. Transportna pravila - e-mail nastavlja kroz filtriranje politike, gdje se procjenjuje prema pravilima protoka e-maila (poznatim i kao transportna pravila) koja su stvorena. Na primjer, pravilo može poslati obavijest menadžeru kada stigne e-mail od određenog pošiljatelja.
d. Filter sadržaja - e-mail prolazi kroz filtriranje sadržaja (antispam i antispoofing) gdje se štetni e-mailovi identificiraju. Može se konfigurirati akcija koju treba poduzeti na e-mailu na temelju presude filtriranja (karantena, premjestiti u mapu Junk e-mail, itd.). Korisnici dobiju e-mail od Microsofta da im je e-mail dostavljen u karantenu nakon čega mogu pregledati o kojim je e-mailovima riječ i zatražiti da se oni iz karantene prebace u njihov inbox.

Ukoliko je e-mail prošao uspješno kroz sve ove filtere, dostavlja se korisniku. [1]

2.2. POLITIKE

Politike su funkcionalnost koja se može naći u oba sigurnosna sustava (EOP i Defender).

Administratori mogu kreirati prilagođene politike koje mogu imati dodatna pravila kako bi se filtriranje i detekcija poboljšale i prilagodile potrebama. Glavne 3 politike su:

Politika zaštite protiv malwarea – konfigurira se za dolazne i odlazne e-mailove kako bi se spriječilo širenje malwarea. Malware se najčešće nalazi u privitcima stoga se ovdje kao opcija može definirati određene ekstenzije koje će se automatski odbiti ukoliko se nalaze u e-mailu. [2]

Zaštita protiv spama – zasebno se konfiguriraju politike za dolazne i odlazne e-mailove. Postavljanje antispam politike uključuje konfiguraciju alata za filtriranje e-maila, kao što su filteri za blokiranje poznatih spam adresa, detekciju neobičnih obrazaca u porukama ili korištenje lista dozvoljenih pošiljatelja (whitelist) i blokiranih pošiljatelja (blacklist). [3]

Zaštita protiv phishinga - Microsoftove politike protiv phishinga su postavke koje se koriste za konfiguriranje zaštite od phishinga. Ove politike pružaju sljedeće vrste zaštite: zaštitu od spoofinga, zaštitu od lažnog predstavljanja (user i domain impersonation). [4]

S obzirom na pripadajuće politike, u karanteni se automatski dodaju oznake za sumnjive e-mailove, kao i tehnologija koja se koristi za prepoznavanje. Iako je karantena automatizirana i pomoću strojnog učenja prepoznaje moguće opasne e-mailove, jedan dio još uvijek zahtijeva ljudsku intervenciju. Alat ima određene nesavršenosti i često se događaju tzv. lažno pozitivni (false positive) slučajevi, odnosno legitiman e-mail bude prepoznat kao napad. Kako bi se smanjila količina takvih e-mailova još uvijek je potreban ljudski faktor da provjeri karantenu i analizira e-mailove i odluči hoće li se e-mail pustiti do korisnika. U slučaju kada se e-mail pusti do krajnjeg korisnika iz karantene, potrebno je prijaviti Microsoftu pušteni e-mail kao lažno pozitivni slučaj, kako bi se filteri poboljšali.

U antispam politikama oznake su: spam, high confidence spam, phishing, high confidence phishing i bulk.

U antiphishing politikama: spoof, user impersonation, domain impersonation i mailbox intelligence impersonation.

U antimalware i safe attachment politikama oznaka je malware. [5]

3. ELEKTRONIČKA POŠTA

E-mail je metoda komunikacije koju koriste elektronički uređaji kako bi dostavili poruke preko računalnih mreža. [6]

E-mail se sastoji od nekoliko dijelova:

a. Tijelo e-maila, tzv. BODY - odnosi se na nešto što pošiljatelj želi poslati, tekst ili npr. slika, privitak, video, link i sl. Body može biti i prazan. Ukoliko se nešto dodaje, bitno je da veličina ne bude veća od dozvoljene.
b. SMTP omotnica, odnosno envelope - može se povući paralela sa fizičkim pismom. Na njemu se najčešće napiše tko šalje pismo i kome. Tako SMTP omotnica sadrži informaciju odakle dolazi e-mail i kome se šalje. Omotnica zapravo govori e-mail serveru gdje da pošalje e-mail.
c. Zaglavlje e-maila, tzv. HEADER - pruža osjetljive informacije o pošiljatelju i primatelju. Može sadržavati različita neobavezna polja, npr.:

- pošiljatelj, tj. FROM - tko šalje e-mail,
- primatelj, tj. TO - kome se šalje,
- CC - dodatni primatelji,
- BCC - dodatni primatelji koji nisu vidljivi navedenima u TO.

d. Predmet, tj. SUBJECT - kratki opis o čemu je riječ u e-mailu. [7]

3.1. PROTOKOLI ZA AUTENTIFIKACIJU E-MAILA

Protokoli za autentifikaciju e-maila služe za zaštitu od neovlaštenog slanja e-maila. Osim toga, protokoli korišteni zajedno štite primatelja, domenu pošiljatelja i daju povratnu informaciju pošiljatelju o učinkovitosti njegovih politika. Ti protokoli su SPF, DKIM i DMARC.

SPF (Sender Policy Framework) je vrsta DNS TXT zapisa koji sadržava sve servere ovlaštene za slanje e-maila s određene domene. Bez SPF-a, napadač može lako oponašati pošiljatelja i prevariti primatelja da podijeli osjetljive informacije napadaču koje inače ne bi podijelio. Ako IP adresa ili domena pošiljatelja nisu na popisu SPF zapisa, primajući server u većini slučajeva neće dostaviti te e-mailove ili će ih dostaviti u neželjenu poštu. Međutim, krajnja odluka što će se dogoditi ukoliko SPF ne prolazi ovisi o statusu DKIM zapisa i u konačnici DMARC zapisa.

Važno je napomenuti da su SPF zapisi u jednom trenutku imali posvećenu vrstu DNS zapisa. Ta je posvećena vrsta zapisa od tada zastarjela i koriste se samo TXT zapisi.

Primjer SPF zapisa Sveučilišta u Zadru:

naredba:

dig unizd.hr TXT

ispis:

```
"v=spf1 ip4:161.53.27.0/24 ip4:161.53.28.0/24 ip4:161.53.2.69 ip4:31.147.204.135 "
"include:_spf.google.com " "a:mail2.srv.carnet.hr a:hlapic.srce.hr -all"
```

Značenja pojedinih dijelova SPF zapisa:

v=spf1 - ovaj dio govori serveru da se radi o SPF zapisu.

ip4 adrese - e-mailovi poslani s ovih IP adresa podrazumijevaju se kao važeći.

include:_spf.google.com - svi serveri navedeni u Google domeni ovlašteni su za slanje e-mailova s unizd domene.

a:mail2.srv.carnet.hr a:hlapic.srce.hr - ukoliko se e-mail šalje s ovih adresa, bit će označen kao valjan.

-all - tzv. “hard fail” je oznaka koja govori da nema drugih IP adresa ili domena koje mogu slati e-mail, osim onih koje su dozvoljene u ovom zapisu te da takvi pokušaji trebaju biti odbijeni.

Umjesto -all, ovdje se mogu naći: ~all i +all. U prvom slučaju e-mailovi će biti tretirani kao nesigurni ili kao spam, ali će ipak proći, dok je +all najlošija praksa koja se treba izbjegavati. Kada SPF zapis uključuje +all to govori da bilo koji poslužitelj može poslati e-mail u ime pošiljatelja i takva je implementacija najpodložnija napadima. [8]

b. DKIM (Domain Keys Identified Mail) - omogućuje MTA (Mail Transfer Agent) da digitalno potpiše odabrano zaglavlje i tijelo poruke RSA potpisom i uključi potpis u DKIM zaglavlje pričvršćeno na poruku prije prijenosa. DKIM potpis uključuje selektor, koji primatelj može koristiti za dohvaćanje javnog ključa iz zapisa u DNS-u. Ovaj javni ključ se zatim koristi za

provjeru DKIM potpisa preko poruke. Dakle, provjera potpisa osigurava primatelju da poruka nije modificirana tijekom prijenosa - osim dodatnih zaglavlja dodanih od strane MTA-a na putu, koji se ignoriraju tijekom provjere i potvrđuju pošiljatelja poruke domeni koja objavljuje javni ključ. DKIM zapis povezan s domenom example.com sa selektorom “mailkey” pohranjen je na mailkey._domainkey.example.com. Oznaka mailkey se izvlači iz DKIM potpisnog zaglavlja na poruci. Zapis je: “v=DKIM1; p=<kodirani javni ključ>”. Prvi mehanizam identificira ovo kao DKIM zapis. Drugi mehanizam uključuje javni ključ koji će autentificirati potpise koji potječu iz te domene. Ako korespondent primi DKIM potpisanu poruku za koju se tvrdi da je iz example.com, DKIM potpis se izvlači, selektor mailkey i DKIM domena se kombiniraju, a čita se DKIM TXT zapis. [7]

Za provjeru DKIM zapisa potrebno je znati koji se selektor koristi za DKIM. Selektor je dio potpisa koji se nalazi u zaglavlju e-maila.

naredba za provjeru za unizd.hr:

dig mail._domainkey.unizd.hr txt

ispis:

```
mail._domainkey.unizd.hr. 1800 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbmNO9Y9x84eGwK7n
BVBgvXzch3rJjHh+s48M/rww/LY+twG3qEuFo2aJ74EErbQnm3nY2s542vITrhdsGmja
C1kJvxKEDhpBfdQ2SKd1JLEELL3U7cFpjmMR8DeolOQmWC3ZHWEKFsCjswrnQk
pIpcMNvXZUjRYGXOD9mAAZ8zQIDAQAB"
```

Značenje pojedinih dijelova DKIM zapisa:

mail._domainkey.unizd.hr – ime DKIM zapisa

1800 – je TTL. Izražen najčešće u sekundama. Govori o tome koliko DNS zapis vrijedi, odnosno koliko traje u sekundama. Nakon što istekne, ponovno se postavlja.

v=DKIM1 - identifikacija DKIM zapisa kako bi server znao da zapis postoji.

k=rsa - kriptografski algoritam korišten za generiranje potpisa. Ovdje se radi o RSA algoritmu.

p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbmNO9Y9x84eGwK7nBVB gvXzch3rJjHh+s48M/rww/LY+twG3qEuFo2aJ74EErbQnm3nY2s542vITrhdsGmjaC1kJvxK EDhpBfdQ2SKd1JLEELL3U7cFpjmMR8DeolOQmWC3ZHWEKFsCjswrnQkpIpcMNvXZ UjRYGXOD9mAAZ8zQIDAQAB - javni ključ koji se koristi za provjeru DKIM potpisa.

Ovaj zapis omogućuje primateljima e-maila da provjere je li poruka koja dolazi s domene unizd.hr autentična i nije mijenjana tijekom prijenosa. Ako je potpis valjan, to znači da je poruka došla s navedene domene i nije mijenjana nakon što je poslana. Ako potpis nije valjan, to može značiti da je poruka lažirana ili mijenjana nakon što je poslana.

c. DMARC (Domain-based Message Authentication, Reporting and Conformance) - odnosi se na mehanizam povratne informacije koji služi kao obavijest vlasnicima pošiljateljeve domene. DMARC je dio TXT zapisa u DNS-u koji odlučuje što se događa s e-mailom nakon što se provjere SPF i DKIM. U obavijesti se pošiljatelje informira o kvaliteti postavki njihovih SPF i DKIM politika. DMARC ujedno služi i kao informacija primatelju kako bi primatelj znao što poduzeti u slučaju napada. Ukoliko SPF ili DKIM nisu pravilno postavljeni i primateljev server ih odbije, isti taj server šalje automatske poruke pošiljatelju, odnosno DMARC izvještaje o neuspjehu. Prema tim izvještajima pošiljatelj može poboljšati svoje politike. [9]

Uz pomoć online alata MXToolBox pronađen je DMARC zapis za unizd.hr. [9]

v=DMARC1; p=quarantine; rua=mailto:postmaster@unizd.hr; fo=1;

v=DMARC1 - oznaka je u zapisu koja govori da se radi o DMARC zapisu.

p=quarantine - to je oznaka u zapisu koja se odnosi na politike, a koja govori što učiniti u slučaju kada DMARC provjera nije prošla. U ovom slučaju se e-mail pošalje u karantenu. Osim te opcije, postoje još dvije: none i reject. None je opuštena verzija koju je najbolje koristiti u početnoj fazi DMARC implementacije kako bi se promotrile aktivnosti e-maila i autentifikacije. Ta politika ne štiti od napada i ne poduzima se nikakva akcija ukoliko DMARC nije prošao provjeru. Ukoliko je p=reject, onda se e-mailovi koji nemaju postavljen DMARC automatski odbijaju.

rua=postmaster@unizd.hr - rua oznaka u DMARC zapisu odnosi se na URI poštanskog sandučića na koji se šalju agregirani DMARC izvještaji. Ovi izvještaji sadrže statistike o

autentifikaciji e-maila u XML formatu. Važno je napomenuti da domena navedena u rua oznaci mora izričito dopustiti slanje DMARC izvještaja na tu određenu domenu inače pružatelj usluge e-maila neće poslati izvještaje. U rua oznaci može biti dodano više URI-ja odvojenih zarezom. [7]

fo=1 - ova oznaka u DMARC zapisu odnosi se na slanje izvještaja o neuspješnom dostavljanju e-maila. Oznaka fo može imati 4 dodijeljene vrijednosti:

fo=0 - izvještaj se generira ukoliko svi mehanizmi autentifikacije nisu bili uspješni

fo=1 - izvještaj se generira ako bilo koji mehanizam autentifikacije nije bio uspješan

fo=d - izvještaj se generira u slučaju kada DKIM zapis nije bio uspješan

fo=s - izvještaj se generira ukoliko SPF zapis nije bio uspješan. [10]

Uz navedene oznake prikazane na primjeru, postoje i neke druge opcionalne oznake, kao što su: ruf, aspf, adkim, rf i drugi.

3.2. DNS

U smislu DNS-a (Domain Name System) može se govoriti o DNS poslužiteljima i DNS protokolima. DNS poslužitelj se odnosi na server koji sadrži bazu podataka u koju se spremaju imena domena i njihove pripadajuće IP adrese. DNS protokol služi za „prevođenje“ imena domena iz formata bliskoga ljudima u računalni jezik (bitove).

DNS zapis se sastoji od nekoliko elemenata od kojih su najvažniji:

Hostname – npr. www

Tip zapisa (recorda) – npr. MX

Sadržaj – IP Adresa

DNS zapisa ima mnogo, međutim ne koriste se svi iz više razloga – postoje oni koji su zastarjeli, nisu globalno prihvaćeni ili su u eksperimentalnoj fazi. Najvažniji DNS zapisi su:

a. A zapis (address) – zapis IPv4 adrese (npr. 192.0.2.146) koji se dodjeljuje domeni ili poddomeni. Preporuka je da se nikada ne koristi tako da dva različita A zapisa upućuju na istu IP adresu.
b. AAAA zapis – zapis IPv6 (npr. 2001:db8:3333:4444:5555:6666:7777:8888) adrese koji služi za povezivanje IPv6 adrese s domenom od 128 bita.
c. CNAME (canonical name) zapis – zapis koji povezuje jedno ime domene (alias) na drugo, tj. kanonsko ime. CNAME uvijek pokazuje na drugo ime domene, a nikad ne bi trebao direktno na IP adresu.
d. MX zapis (mail exchange) – zapis koji upućuje na server ili servere koje neka domena koristi za razmjenu e-mailova. MX zapis sadrži broj prioriteta, što je broj manji, prioritet je veći, odnosno prije će se dostaviti e-mail s manjim prioritetom. Primjer zapisa za domenu unizd.hr:

```
;; ANSWER SECTION:
unizd.hr.               1800    IN      MX      5 donat.unizd.hr.
```

Unizd.hr je domena za koju je ovaj zapis relevantan, 1800 je već spomenuti TTL, IN je internet klasa, MX je tip zapisa, 5 je prioritet zapisa, a donat.unizd.hr nam govori da će svi e-mailovi poslani na unizd.hr biti usmjereni na taj poslužitelj.
e. TXT zapis (tekstualni zapis) – relevantan za sigurnost e-maila jer se u njemu definiraju SPF, DKIM I DMARC zapisi. [11]

3.3. SMTP

SMTP je tehnički standard za prijenos elektroničke pošte preko mreže. On omogućuje razmjenu podataka između računala i poslužitelja bez obzira na njihovu hardversku ili softversku osnovu, što olakšava široku dostavu e-maila. SMTP je protokol za dostavu pošte, ali ne i protokol za preuzimanje pošte. Da bi primatelj mogao pročitati e-mail, potrebni su posebni protokoli za preuzimanje e-maila s poslužitelja (IMAP i POP).

Rad SMTP-a:

a. Otvaranje SMTP veze: Početak procesa započinje uspostavom TCP veze između klijenta i poslužitelja, a zatim klijent započinje proces slanja e-maila posebnom "Pozdrav" naredbom (HELO ili EHLO).

b. Prijenos podataka e-maila: Klijent šalje poslužitelju seriju naredbi uz stvarni sadržaj e-maila: zaglavlje e-maila (uključujući odredište i predmet), tijelo e-maila i dodatne komponente.
c. Mail Transfer Agent (MTA): Poslužitelj pokreće program MTA. MTA provjerava domenu e-maila primatelja i, ako se razlikuje od pošiljateljeve domene, traži IP adresu primatelja putem DNS-a.
d. Zatvaranje veze: Klijent obavještava poslužitelj kada je prijenos podataka završen, a poslužitelj zatvara vezu. [12]

SMTP protokol sam po sebi nije siguran, stoga je kao sigurnosni dodatak uveden tzv. TLS protokol (Transport Layer Security). TLS je imao više verzija, trenutno je kao standard u uporabi TLS 1.2, ali je sve raširenije korištenje TLS 1.3 verzije. Problematika SMTP-a leži u tome što se koristeći samo SMTP podaci preko interneta šalju kao običan tekst bez enkripcije, osim toga IP adrese na koje se šalje e-mail se komuniciraju preko DNS infrastrukture koja je na internetu javna. Takva DNS infrastruktura je ranjiva i podložna napadima.

3.4. DANE I DNSSEC

DANE – (DNS-based Authentication of Named Entities) služi za validaciju TLS certifikata preko DNSSEC i radi jedino kad je DNSSEC aktivan. Kriptografski sažetak (tzv. hash) vrijednost x509 certifikata ili cijeli certifikat su spremljeni u DNS. Preko te validacije se dokazuje da je vlasnik domene zapravo vlasnik certifikata i da odgovor dolazi od njega. Ovakav proces otežava Man in the middle attack jer napadač treba doći do certifikata, ali ujedno i do dijela DNS zapisa. DANE za SMTP koristi TLSA zapis u DNS-u domene kako bi signalizirao podršku za DANE. Ako nema TLSA zapisa, DNS rezolucija za mail protok radi normalno. TLSA zapis signalizira podršku za TLS i objavljuje DANE politiku za domenu, omogućujući poslužiteljima za slanje pošte da autentificiraju legitimne poslužitelje za primanje pošte. DANE ovisi o DNSSEC-u koji digitalno potpisuje DNS zapise koristeći kriptografiju javnog ključa. Kada se MX, A/AAAA i DNSSEC-povezani zapisi za domenu vrate kao DNSSEC autentični, poslužitelj za slanje pošte traži TLSA zapis koji odgovara MX hostu. Ako je TLSA zapis prisutan i autentičan, vraća se poslužitelju za slanje pošte. [13]

DNSSEC (Domain Name System Security Extensions) je sigurnosni dodatak za DNS koji sprječava lažiranje DNS odgovora. Kada se koristi, DNS odgovori dolaze s digitalnim potpisom

koji potvrđuje da odgovor dolazi od legitimnog DNS poslužitelja i da nije izmijenjen. DNSSEC jamči autentičnost i integritet DNS odgovora. Međutim, korisnik mora provjeriti valjanost digitalnog potpisa kako bi bio siguran u ispravnost DNS odgovora. [14]

Za provjeru DNS odgovora koristi se lanac povjerenja digitalnih potpisa („Chain of trust“). Lanac počinje ključem korijenskih DNS poslužitelja i završava potpisanim DNS odgovorom. Ključ korijenskih poslužitelja je “sidro” ovog lanca, tj. izvor povjerenja za DNSSEC. Kada korisnik sigurno dobije ovaj ključ, može provjeriti valjanost svih ostalih potpisa u lancu.

Za maksimalnu sigurnost potrebno je da se provjera valjanosti potpisa DNS odgovora obavlja na računalu krajnjeg korisnika. To je jedini način da korisnik bude siguran da DNS odgovor nije bio lažiran u bilo kojem dijelu procesa. [15]

Prvi korak u implementaciji DNSSEC-a je grupiranje zapisa istog tipa u jedan set zapisa koji se zove RRSet. Taj set zapisa se potpisuje sa RRSIG (RRset Signature) koji se sastoji samo od potpisa za potvrdu autentičnosti i integriteta podataka. [16]

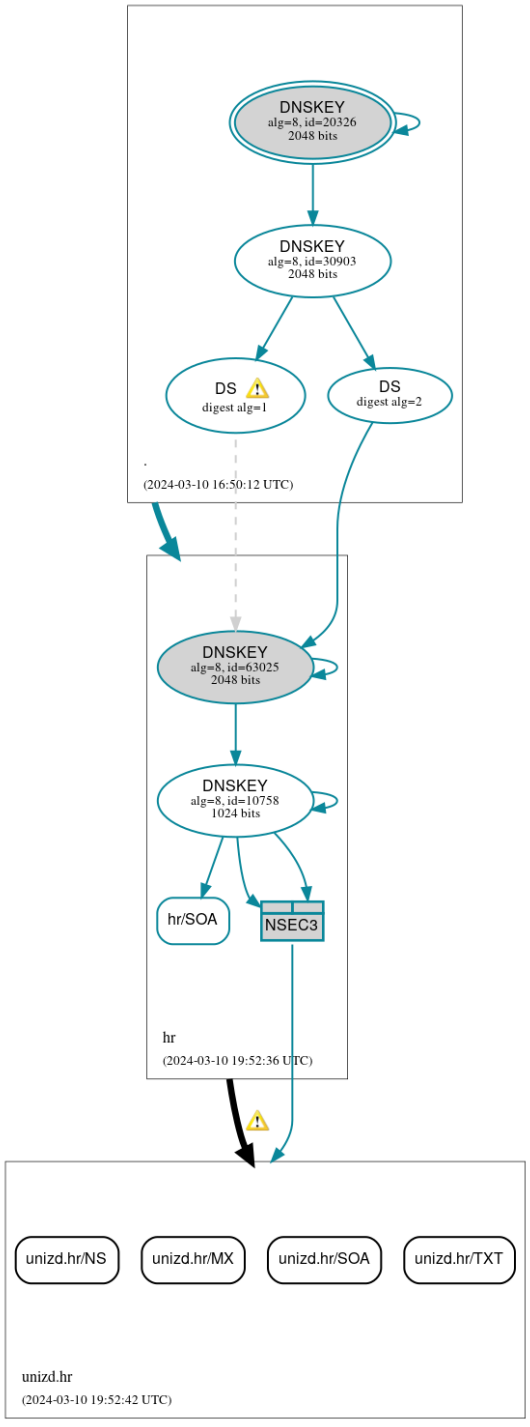
Za postavljanje DNSSEC kriptografskog potpisa potrebno je dodati dodatne DNS zapise od kojih su najvažniji DNSKEY i DS. [17]

DNSKEY zapis sadrži javni ključ koji služi za provjeru potpisa u RRSIG zapisu, a DS zapis sadrži hash DNSKEY zapisa. Svaka DNSSEC zona dodjeljuje skup ključeva za potpisivanje zone (ZSK). Ovaj skup uključuje ključ za potpisivanje RRset zapisa u zoni, tj. ZSK i KSK. KSK služi kao ključ za potpisivanje ključa, tj. DNSKEY zapisa. [18]

DS zapis služi kao veza povjerenja između roditeljske i dječje zone i postavlja se u roditeljsku zonu. Na taj način se omogućuje resolverima da se provjeri autentičnost DNSKEY zapisa u dječjoj zoni, odnosno uspostavlja se već spomenuti lanac povjerenja.

Osim navedenih, postoje još i NSEC i NSEC3 zapisi kojima je glavna svrha dokaz da nešto ne postoji. Ukoliko se pošalje upit na potpisanu zonu za određeno ime koje postoji, ali ne postoji određeni tip zapisa za to ime, vraćeni NSEC zapis koji je potpisan navest će sve tipove zapisa koji stvarno postoje za traženo ime domene. [19]

Na slici je generiran dijagram koji prikazuje lanac povjerenja za domenu unizd.hr. Kada se provjerava valjanost potpisa za unizd.hr, prvo se ide sa unizd.hr na carnet.hr i zatim na root domenu.



[20]

Slika 1 - Primjer DNSSEC za unizd.hr. Izvor: https://dnsviz.net/

4. E-MAIL NAPADI

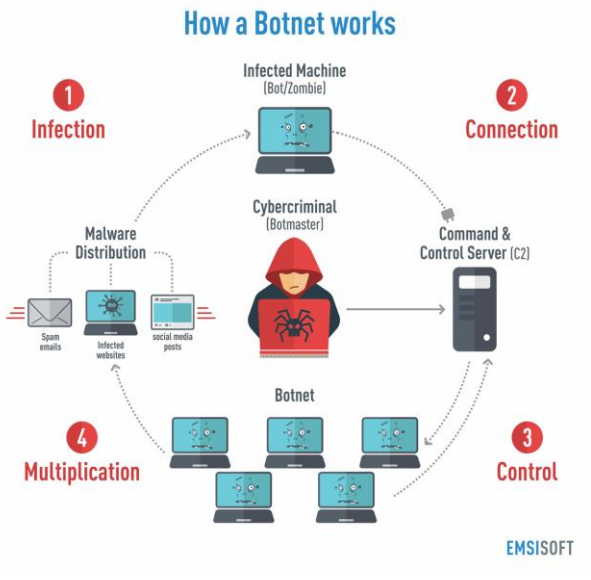
U 21. stoljeću vrlo je česta rečenica da je internet svojim razvojem omogućio mnogo pozitivnih promjena, ali i onih negativnih. E-mail napadi su jedna od tih negativnih promjena koje su se proširile razvojem digitalizacije i interneta. Može se povući paralela sa kriminalom poznatim kroz povijest u smislu dobavljanja nekih resursa ili bogatstva ilegalnim putem. U ovom slučaju se radi o ilegalnim pokušajima nabave osobnih informacija pojedinaca kako bi se te iste zloupotrijebile u različite svrhe. Neke od tih svrha mogu biti: krađa identiteta, bankovne transakcije, put do povjerljivih poslovnih informacija, prodaja na crnom tržištu i mnogi drugi.

Klasifikacija e-mail napada nije jedinstvena, stoga je ovdje kao glavna klasifikacija navedena ona koja će moći biti potkrijepljena stvarnim primjerima iz prakse.

4.1. SPAM

Spam e-mailovi su najčešće poslani odjednom na više e-mail adresa. Takvi e-mailovi u većini slučajeva ne budu identificirani kao opasni, međutim mogu sadržavati zlonamjerne poveznice ili privitke, zlonamjerni softver, mogu služiti za potvrdu privatnog e-maila kako bi korisnik postao žrtva nekog ozbiljnijeg napada i dr. [21]

Iako je prvi spam e-mail poslan još u 70-im godinama 20. stoljeća preko prethodnika današnjeg interneta (ARPANET), pravi izazovi počeli su se javljati 90-ih godina kada je razvoj interneta uznapredovao, a ujedno i botneta. Botnet su zapravo računala kojima upravljaju kibernetički kriminalci bez znanja pravih vlasnika računala. Ta računala korištena su u zlonamjerne svrhe kako bi slala masovne e-mailove i proširila neželjene programe.



[22]

Slika 2 -Botnet. Izvor: https://www.emsisoft.com/en/blog/27233/what-is-a-botnet/

S obzirom na ogroman broj spam e-mailova (čak 90% e-mailova su bili spam), razvila se i potreba za obranom i zaštitom od njih te je tako razvijen način prikupljanja neželjenih IP adresa i blokiranje istih. Ovo bi se moglo smatrati pretečom današnje e-mail karantene.

Način na koji slanje spam e-mailova funkcionira se može objasniti kao:

Sakupljanje adresa e-maila: Pošiljatelji spama prikupljaju adrese e-maila za slanje neželjene pošte. Koriste softver za pretraživanje interneta i prikupljanje adresa iz javnih podataka, a često se podaci prodaju na deep webu ili spammeri međusobno razmjenjuju podatke.

Zamagljivanje sadržaja poruke: Pošiljatelji spama često namjerno pogrešno pišu riječi ili umeću znakove kako bi otežali prepoznavanje njihovih poruka od strane softvera za filtriranje.

Probijanje Bayesovih filtera: Pošiljatelji spama koriste tehniku poznatu kao Bayesovo trovanje, koja uključuje uključivanje nebitnih, nasumičnih riječi u poruke kako bi manipulirali vjerojatnostima riječi i oslabili Bayesovo filtriranje.[1]

Usluge podrške za spam: Postoje razne online aktivnosti i poslovne prakse koje podržavaju napore pošiljatelja spama i omogućuju njihovu operaciju, uključujući obradu narudžbi za robu

[1] Bayesovo filtriranje - je metoda za otkrivanje neželjenih e-mailova temeljena na Bayesovom teoremu. Ova tehnika koristi se za izračun vjerojatnosti da je određena e-pošta spam. Kako bi se smanjio broj lažnih pozitiva Bayesov filtar uči na temelju riječi u naslovu i tijelu poruke, koristeći informacije iz prethodno identificiranih spam i legitimnih poruka. https://guardiandigital.com/resources/blog/email-threats-explained-what-is-spam-email

oglašenu u spamu, hosting web stranica ili DNS zapisa navedenih u spam porukama i proizvodnju spamwarea.

4.2. PHISHING

Phishing je oblik online prijevare gdje napadači koriste socijalno inženjerstvo i tehničke metode za krađu osobnih podataka i financijskih informacija korisnika. Ovo se obično postiže stvaranjem lažnih web-stranica ili slanjem zlonamjernih e-mailova koji izgledaju kao da dolaze od pouzdane organizacije. Cilj je prevariti korisnika da otkrije osjetljive informacije poput lozinki za online bankarstvo ili brojeva kreditnih kartica. Phishing napadi mogu se izvesti putem različitih medija, uključujući telefonske pozive, poruke, web-stranice i e-mailove. Napadači često koriste kombinaciju socijalnih i tehničkih vještina kako bi uspješno izveli ove napade. U ovom radu fokus je na e-mail phishing napadima. [23]

Za phishing napade je karakteristično da se služe pridjevima usmjerenim prema brzini reakcije, hitnoće, opasnosti, odnosno usmjereni su na ljudske emocije. U tim trenucima ljudi ne razmišljaju logički i realno te pokleknu pred fiktivnim pritiskom. Tada oni najčešće kliknu na link čiji se URL ne poklapa s onim u statusnoj traci. Na taj način se u većini slučajeva otvori lažna stranica koja traži od osobe da se unesu neki osobni podaci. Osim navedenih, neke od značajki phishing e-maila su: različito ime pošiljatelja od e-mail adrese, e-mail adresa slična legitimnoj s jednim ili više slova pogrešno napisanih, slike dodane u e-mail slične slikama velikih korporacija koje sadrže neobične URL-ove itd. Karakteristika klasičnog phishinga je da nema ciljanu skupinu nego se šalje velikom broju ljudi.

Phishing se može kreirati na više različitih načina, a neki od općenitih su:

Definiranje ciljeva: Prije pokušaja stvaranja phishing e-maila jasno se moraju definirati ciljevi kampanje.

Provedba detaljnog istraživanja: Da bi se stvorio uvjerljiv phishing e-mail potrebno je proučiti i razumjeti ciljane osobe.

Stvaranje angažirajućeg e-maila: Na temelju provedenog istraživanja kreira se e-mail s određenim specifikacijama. Te specifikacije odnose se na vizualni dio koji bi trebao biti što sličniji stvarnoj kompaniji.

Ugrađivanje tereta: Kibernetički kriminalci često koriste prerušene linkove kako bi prevarili žrtve da kliknu na zlonamjerne phishing web-stranice. Da bi se to postiglo, potrebno je stvoriti phishing poveznice koje snažno nalikuju domeni legitimne usluge. To bi moglo uključivati upotrebu domena koje nalikuju na izvornu, poddomena, pa čak i složenih struktura URL upita koje zamagljuju stvarnu domenu koja se koristi.

Odabir pružatelja e-maila: Odabrani pružatelj e-maila ovisi o potrebama kreatora phishing kampanje. Za slanje manjih količina e-mailova mogu se koristiti poznati pružatelji usluga (Gmail, Yahoo, Microsoft). Međutim, za neke kompleksnije kampanje koriste se infrastrukture koje napadač može sam granularno modificirati.

Kupnja phishing domene: Potrebno je kupiti domenu najsličniju onoj legitimnoj.

Konfiguracija phishing infrastrukture: Kupljenoj domeni je potrebno složiti DNS postavke s protokolima. Ukoliko domena nema postavljen DMARC, SPF ili DKIM, kod ozbiljnih kompanija takav e-mail neće proći do zaposlenika. U startu će biti blokirani zahvaljujući naprednim e-mail filterima i tehnologijama detekcije. [24]

Kod pravilne reakcije na phishing e-mail najveću ulogu ima ljudski faktor. Ljudi su podložni emocionalnim reakcijama te na sadržaj koji sugerira da je nešto hitno ili da su moguće posljedice, mogu ishitreno reagirati. U korporacijama je na vrhu liste najvažnija edukacija zaposlenika. Edukacija se najčešće provodi uz pomoć predavanja, interaktivnih videa i phishing kampanja iz kojih se izvode statistički podaci. Naglasak se stavlja na školsko obrazovanje stoga je sve veća potreba za edukacijom djece i mladih kojih je sve više na društvenim mrežama i u digitalnom svijetu. Najranjivija skupina je starija dobna skupina koja je često meta online prevara.

S obzirom na ciljane skupine i namjenu, phishing e-mailove se može podijeliti na više podskupina. Neke od skupina su:

Spear phishing - ova vrsta napada je pokušaj stjecanja osjetljivih informacija ili pristupa računalnom sustavu slanjem lažnih poruka koje izgledaju legitimno. Usmjerena je na određenu osobu ili skupinu i često uključuje informacije za koje se zna da su od interesa za metu. Poruke se dostavljaju putem e-maila i dizajnirane su da uvjere korisnika da otvori zlonamjernu

poveznicu ili privitak, izlažući metu zlonamjernom softveru. Cilj spear phishinga je stjecanje osjetljivih informacija poput korisničkih imena, lozinki i drugih osobnih podataka. [25]

Whaling - je visoko ciljani phishing napad usmjeren na izvršne dužnosnike na visokim pozicijama, maskiran kao legitimni e-mail. Ovaj oblik phishinga kroz socijalno inženjerstvo dizajniran je da potakne žrtve na sekundarnu akciju, poput pokretanja prijenosa sredstava. Ovakvi e-mailovi složeni su kako bi se približili meti, odnosno najčešće: sadrže personalizirane informacije o ciljanoj organizaciji ili pojedincu, prenose osjećaj hitnosti, izrađeni su s čvrstim razumijevanjem poslovnog jezika i tona. [26]

BEC (Business E-mail Compromise) - ciljana skupina slična je kao kod whalinga (osobe na visokim pozicijama), u ovom slučaju specifično izvršni direktori ili odjel za financije. Od žrtve se uglavnom traži prijenos sredstava ili otkrivanje nekih osjetljivih informacija. Kriminalci iza BEC-a šalju uvjerljive e-mailove koji mogu zahtijevati neuobičajene uplate ili sadrže veze do sumnjivih web-stranica. Neki e-mailovi mogu sadržavati viruse prikrivene kao bezopasne privitke, koji se aktiviraju kada se otvore. [27]

4.3. MALWARE

E-mail se sve više koristi za slanje binarnih datoteka u obliku privitaka. U početku, ovo nije predstavljalo značajan sigurnosni rizik jer su privitci uglavnom bili mali tekstualni dokumenti ili fotografije. Međutim, s porastom uporabe e-maila u svakodnevnoj suradnji organizacija, povećala se veličina i vrste privitaka. Danas se mnogi e-mailovi šalju s privicima poput izvršnih programa, slika, glazbe i zvukova. Razne vrste zlonamjernog softvera, uključujući viruse, crve, trojanske konje i špijunski softver, često se prenose putem privitaka.

Preporuke za sigurnost e-maila uključuju filtriranje potencijalno opasnih vrsta privitaka (npr. .vbs, .ws, .wsc ekstenzije datoteka) na mail serveru ili mail gatewayu, uz provođenje skeniranja zlonamjernog softvera na dozvoljenim vrstama datoteka. Filtriranje bi trebalo uzeti u obzir ne samo ekstenzije datoteka, već i zaglavlje e-maila ili druge identifikacijske aspekte datoteke kako bi se povećala učinkovitost. Važno je, također, razmotriti postavljanje različitih pravila za e-mail koja potječu iznutra nasuprot onih izvana, ili za pouzdane nasuprot nepouzdanih organizacija, iako ovu posljednju opciju može otežati krivotvorenje adresa e-maila. [28]

Neki od načina za zaštitu od e-mail malwarea su:

Skeniranje zlonamjernog softvera - može se provesti na firewallu, mail relayju ili uređaju za mail gateway dok podaci e-maila ulaze u mrežu organizacije, na samom mail serveru i/ili na računalima krajnjih korisnika. Općenito, organizacije bi trebale implementirati barem dvije razine skeniranja zlonamjernog softvera - jedan na razini računala krajnjih korisnika i jedan na razini mail servera ili firewall/mail relay/mail gatewaya - i trebale bi razmotriti implementaciju skeniranja zlonamjernog softvera na svim trima razinama.

Blokiranje pojedinih ekstenzija za privitke – politika se modificira tako da se e-mailovi koji sadrže ekstenzije podložne manipulaciji i umetanju zlonamjernog koda odbijaju.

Filtriranje sadržaja - djeluje na sličan način kao i skeniranje zlonamjernog softvera na firewallu ili mail serveru, s tim što traži e-mail koji sadrži nepoželjni sadržaj, osim zlonamjernog softvera, poput spama ili e-maila s neprimjerenim jezikom. Tipične stavke koje bi bile uhvaćene filterima i moguće radnje na njima mogu biti sljedeće: e-mailovi koji sadrže sumnjiv aktivni sadržaj (npr. ActiveX, JavaScript) očiste se od aktivnog koda i proslijede primatelju, spam e-mail i pokušaji phishinga mogu biti izbrisani ili označeni kao sumnjivi, izuzetno velike datoteke mogu biti zadržane za dostavu izvan radnog vremena. [24]

4.4. E-MAIL SPOOFING

E-mail spoofing je vrsta napada u kojem napadač šalje poruke s lažnom e-mail adresom pošiljatelja.

U e-mail spoofingu, napadači mogu učiniti da e-mail izgleda kao da ga šalje poznata osoba poput kolege, partnera ili menadžera. Spoofing je proces manipulacije poljem "From:" kako bi se stvorio dojam da e-mail dolazi od određene osobe. [29]

Napadači, tzv. spoofers ponekad mogu stvoriti e-mail adresu koja izgleda autentično zamjenjujući samo jedno ili dva slova u imenu tvrtke, poput "Arnazon" umjesto "Amazon", ili drugih zamjena slova koje su teško primjetne.

E-mail spoofing je taktika koja ima za cilj prikupljanje osobnih informacija i podataka od korisnika, preuzimanje njihovih online računa, dostava zlonamjernog softvera ili krađa sredstava. Prema nekim studijama, žrtve često otvaraju e-mail koji izgleda autentično i dolazi od pouzdanog pošiljatelja. Spoofane e-mail poruke uglavnom se ili brišu ili preusmjeravaju u

mapu za neželjenu poštu. Problem počinje kad žrtva bude prevarena da otvori e-mail i klikne na zlonamjernu vezu koja instalira opasni softver u njihov sustav. Iako većina spoofanih e-mailova lako može biti prepoznata i riješena jednostavnim brisanjem, neke varijante mogu imati ozbiljne posljedice. [30]

Motivacije za e-mail spoofing su jednostavne. Obično, napadač će koristiti ovu taktiku kako bi dobio osjetljive informacije poput socijalnih osiguranja, financijskih detalja i sl. Evo nekih drugih razloga za e-mail spoofing: skrivanje pravog identiteta lažnog pošiljatelja, izbjegavanje crne liste za spam, oštećivanje reputacije legitimnog pošiljatelja, planiranje osobne štete, temelj za neki drugi napad, najčešće za phishing.

E-mail spoofing je moguć zbog ograničenja SMTP-a. Ograničenje SMTP protokola je to što ne provjerava je li e-mail adresa u polju "From" stvarna. Napadač može koristiti besplatne online SMTP servere za slanje spoofanih e-mailova. Ako želi spoofati e-mail, jednostavno koristi bilo koji od besplatnih online SMTP servera, sastavi e-mail i unese željenu e-mail adresu u polje "From" prije slanja. Bez obzira na to što ne posjeduje stvarnu e-mail adresu, SMTP server je neće provjeravati.

Spoofane e-mailove moguće je otkriti provjerom e-mail adrese i imena pošiljatelja ili proučavanjem zaglavlja e-maila za SPF i DKIM informacije.

Preporuka za zaštitu od e-mail spoofinga:

a. implementacija SPF-a
b. postavljanje DKIM-a
c. korištenje DMARC-a
d. edukacija zaposlenika
e. branding tvrtke - korištenje konzistentnog brendiranja u marketinškim e-mailovima kako bi se izbjegli uspješni napadi spoofinga. [26]

4.5. USER I DOMAIN IMPERSONATION

Impersonation je lažno predstavljanje koje se često koristi kao phishing. Postoje dvije vrste lažnog predstavljanja.

Lažno predstavljanje domene - domena je registrirana i postojeća, a vrlo je slična pravoj domeni, te često ima i postavljene protokole SPF, DKIM i DMARC. Primjerice, @unizd.hr je legitimna domena, a lažna bi bila vrlo slična, npr. @umizd.hr ili @unizb.com.

Lažno predstavljanje korisnika - jedna od mogućnosti je da postoji djelatnik na Sveučilištu u Zadru Jane Doe s e-mail adresom jdoe@unizd.hr. Napadač mijenja svoje ime u Jane Doe, a e-mail adresa bude prava bez izmjene. Ukoliko primatelj ne provjeri e-mail adresu pošiljatelja, vrlo lako može nasjesti na prevaru. Drugi primjer je kada je e-mail adresa vrlo slična legitimnoj, npr. jboe@unizd.hr. Napadači se najčešće pretvaraju da su direktori kompanija ili da su iz financijskog odjela i zahtijevaju hitno ažuriranje bankovnog računa. [31]

Cilj ovakvog napada je sličan kao i u prethodnim slučajevima - doći do osjetljivih informacija (bankovni računi, lozinke, itd.). Svaki e-mail je potrebno detaljno proučiti i fokusirati se na moguće gramatičke greške, zahtjeve za prijenosom novca, direktorove e-mailove koji nisu uobičajeni, korištenje riječi poput “hitno”, “brzo” ili riječi prijetnje. [32]

Kod ovakvih napada najveći obrambeni faktor je ljudska svjesnost, odnosno edukacija.

5. ANALIZA E-MAIL NAPADA

U ovom dijelu rada analizira se nekoliko pokušaja e-mail napada koji su završili u karanteni. E-mail napadi su učestali u poslovnom okruženju i njihov broj dostiže do nekoliko stotina na dnevnoj bazi. Najčešća meta su direktori, financijski odjel, voditelji ljudskih resursa ili menadžeri.

Dodan je primjer samostalnog pokušaja kreiranja phishing e-maila uz pomoć Kali Linuxa.

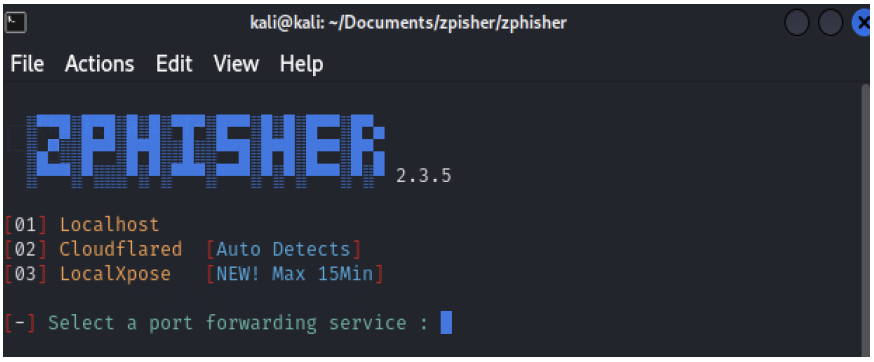
5.1. KALI LINUX – PRIMJER KREIRANJA PHISHING E-MAILA

Kali Linux je open source operacijski sustav na Debian distribuciji. Može se reći da mu je glavna funkcija ethical hacking, pentesting i proširivanje znanja u kibernetičkoj sigurnosti. S obzirom na svrhu, dolazi s različitim alatima predinstaliranima za tu namjenu (čak više od 600). Neki od alata služe za provjeru web-aplikacija kako bi se utvrdili različiti sigurnosni propusti, npr. SQL injection, Denial of service, data encryption, authorization control, password napadi itd.

U Kali Linux programu instaliran je open source tool zvan Zphisher https://github.com/htr-tech/zphisher. U Readme.md fileu se mogu pronaći upute za instalaciju koje su vrlo jednostavne za praćenje. Nakon instalacije i pokretanja programa u terminalu su ponuđene različite opcije za napad:

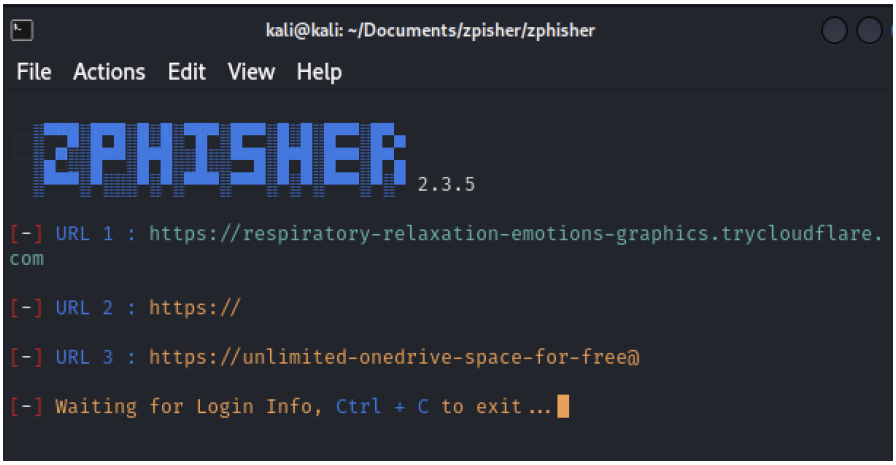
Slika 3 - Zpisher opcije za napad. Izvor: autor. Preuzeto: https://github.com/htr-tech/zphisher

U ovom edukativnom primjeru odabire se Microsoft. Nakon toga se odabire port forwarding service, od ponuđenih opcija odabran je Cloudflare.



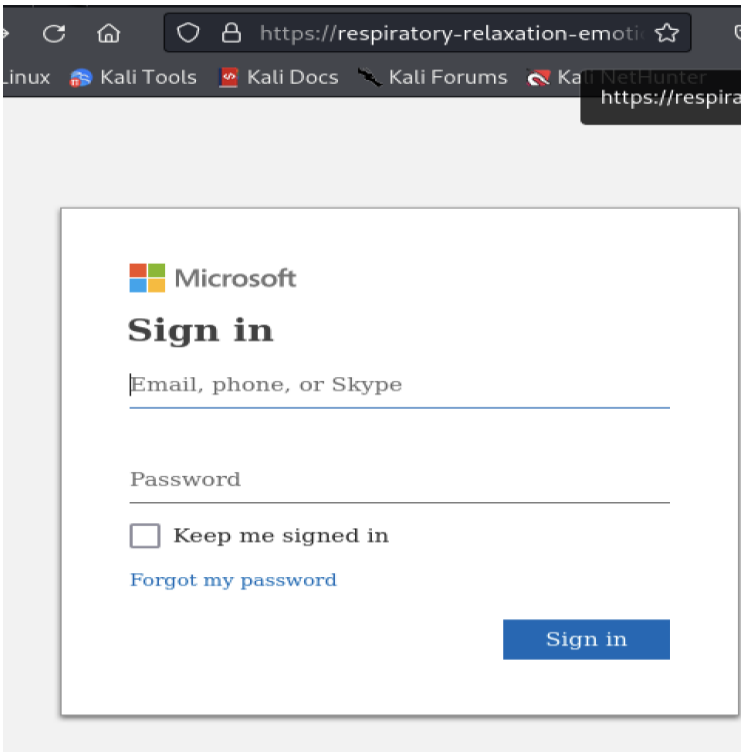
Slika 4 - Port forwarding odabir. Izvor: autor

Nakon odabira Cloudflared dobiju se opcije za URL koji će biti poslan meti. Biramo prvi URL.



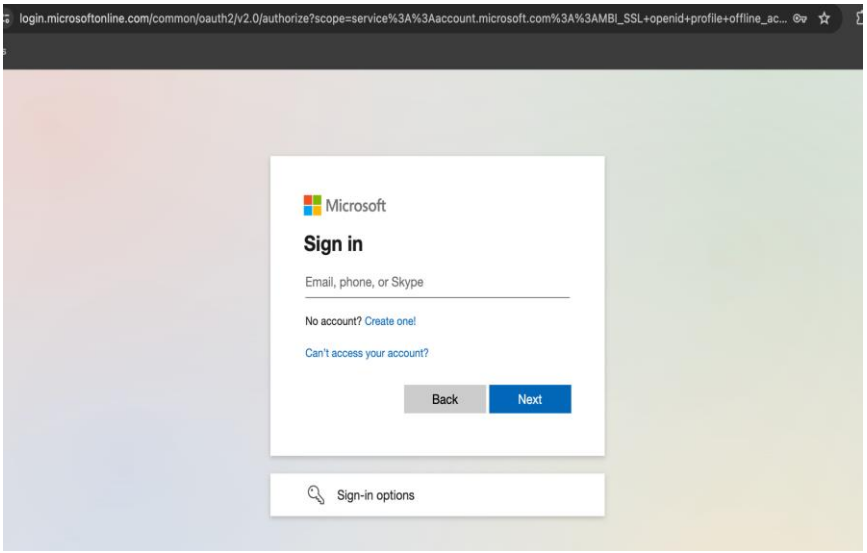
Slika 5 - Odabir URL-a za metu. Izvor: autor

Kada meta otvori URL, dobije sign in prozor vrlo sličan legitimnom Microsoft sign in prozoru. Jedina razlika je URL.



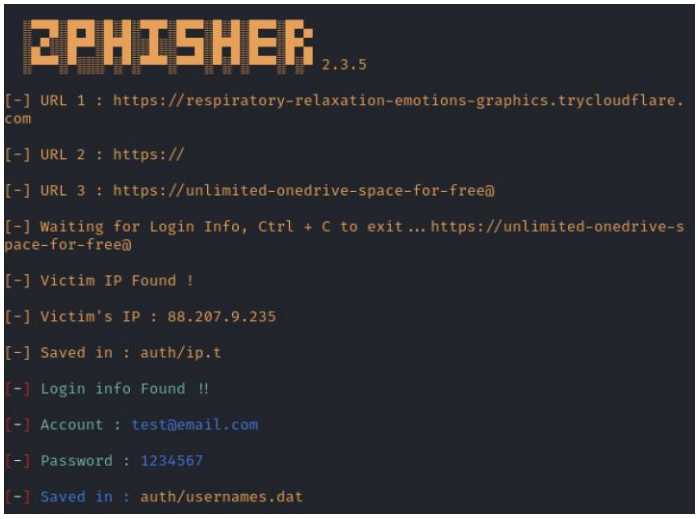
Slika 6 - Lažni sign in prozor. Izvor: autor

Izvorni Microsoft sign in prozor za usporedbu



Slika 7 - Legitiman sign in prozor. Izvor: autor

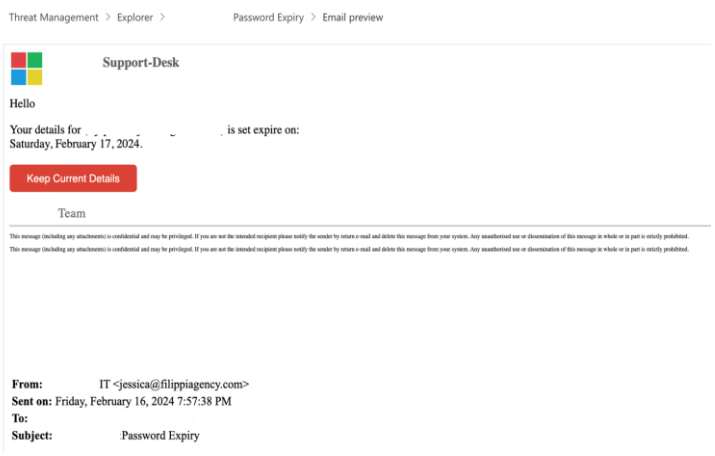
Kada osoba otvori prozor, dobije se public IP adresa uređaja koji koristi, a kada unese podatke, u terminalu se zapišu e-mail adresa i lozinka.



Slika 8 - Prikaz unesenog e-maila i lozinke. Izvor: autor

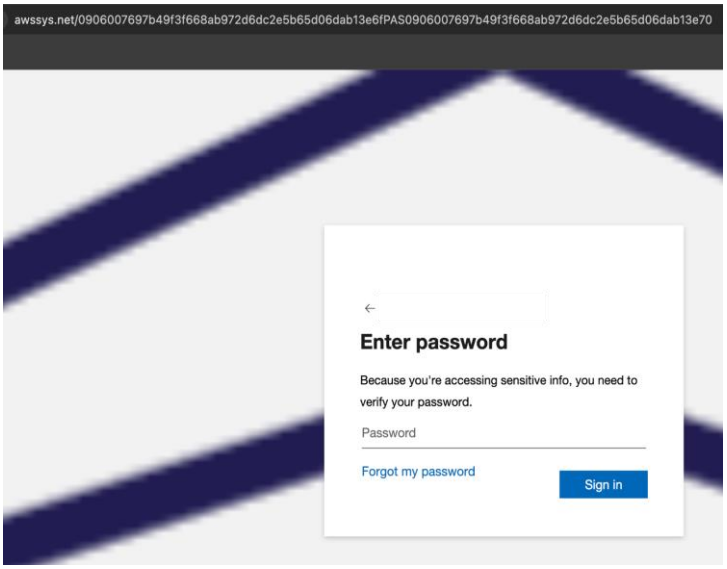
Ovako generirani linkovi se najčešće nalaze u e-mailovima skrivenima unutar slike.

5.2. HIGH CONFIDENCE PHISHING



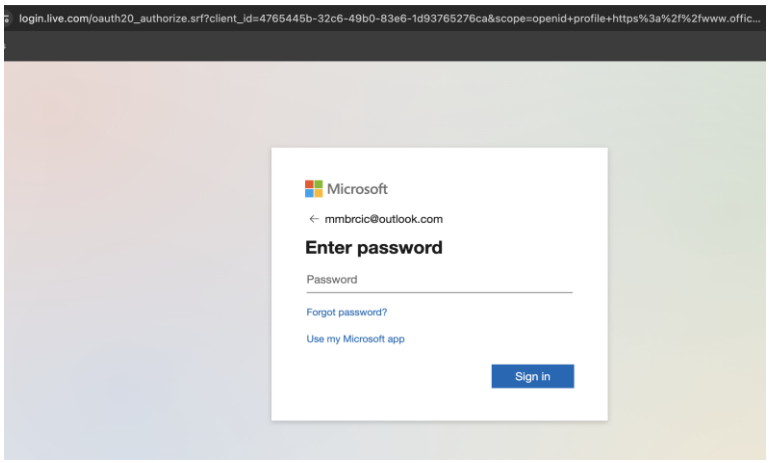
Slika 9 - Primjer high confidence phishing emaila. Izvor: autor

Dodan je primjer jednog pokušaja phishing e-maila koji je završio u karanteni. Na prvi pogled, za neiskusnog promatrača vizualni dojam bi bio da e-mail stiže od Microsofta, odnosno od support tima unutar kompanije. U polju From stoji naziv kompanije kojoj je e-mail poslan, međutim kada se pogleda e-mail pošiljatelja stoji jessica@filippiagency.com, što znači da je upotrijebljena Domain impersonation jer se naziv kompanije koja je meta u ovom napadu i njezine domene nalaze u display name ovog e-maila. Ukoliko se stisne na „Keep current details“ otvori se prozor vrlo sličan legitimnom Microsoft načinu postavljanja lozinke, koji od osobe želi da potvrdi svoju lozinku.



Slika 10 - Primjer lažnog sign in prozora. Izvor: autor

Ako se pogleda u URL, može se vidjeti da prikazani URL nije povezan s uobičajenim URL-om kojeg se dobije od Microsofta prilikom promjene lozinke (https://login.live.com/) te nedostaje originalna Microsoft ikona.



Slika 11 - Primjer Microsoft URL-a. Izvor: autor

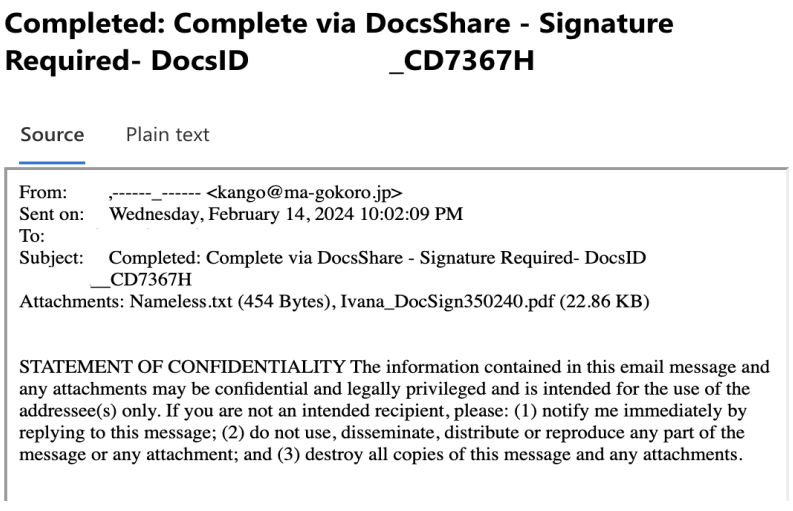
Primarni razlog zbog kojeg je ovaj e-mail završio u karanteni je upravo taj URL koji je Microsoftovim filterima detektiran kao maliciozan, odnosno phishing (URL detonation reputation). URL detonation reputation znači da su Microsoft filteri uz pomoć politika o sigurnim linkovima otkrile zlonamjerni URL u poruci tijekom detekcije unutar sandbox okruženja. Politike koje se odnose na sigurnost URL-a poslanog u e-mailu automatizmom otvaraju URL u sandbox okruženju i proučavaju njegov sadržaj te na temelju rezultata odlučuju o puštanju e-maila ili zadržavanja u karanteni. [33]

```
spf=pass (sender IP is 52.100.172.244) smtp.mailfrom=filippiagency.com; dkim=none (message not signed) header.d=none;dmarc=bestguesspass action=none header.from=filippiagency.com;compauth=pass reason=109
```

U prikazanom dijelu zaglavlja e-maila vidljivo je da je SPF provjera autentičnosti uspješna i da je poslano sa domene filippiagency.com odnosno, da je IP adresa ovlaštena za slanje e-mailova s te domene.

Iako je SPF prolazan, DKIM je označen s none, točnije e-mail nije digitalno potpisan stoga se autentičnost ne može dodatno provjeriti. header.d=none: označava domenu koja je povezana s DKIM potpisom, ali u ovom slučaju, nije navedena nikakva domena (označena je kao "none"), što potvrđuje da poruka nije potpisana DKIM-om. dmarc=bestguesspass action=none header.from=filippiagency.com: DMARC je provjera koja koristi rezultate SPF i DKIM provjera, kao i usklađenost adrese pošiljatelja (header.from) kako bi odlučila hoće li prihvatiti, odbiti ili samo označiti poruku. dmarc=bestguesspass znači da je DMARC provjera prošla na temelju najbolje procjene (vjerojatno zato što SPF provjera prolazi i adresa pošiljatelja odgovara SPF domeni), a action=none znači da DMARC politika ne zahtijeva nikakvu posebnu akciju za ovu poruku. "header.from=filippiagency.com" označava domenu koja je navedena u From polju e-mail headera. compauth=pass compauth je skraćenica za "Composite Authentication", što je ukupni rezultat svih provjera autentičnosti koje je izvršio primateljev poslužitelj. compauth=pass znači da je poruka prošla sve provjere autentičnosti.

5.3. MALWARE



Slika 12 - Primjer e-maila koji sadrži privitak s malwareom. Izvor: autor

Priloženi primjer e-maila je pokušaj prevare preko privitaka dodanih u e-mail. Prvo što se može uočiti je izostanak display name pošiljatelja. Ujedno ovaj e-mail nema tekstualnog sadržaja i

detalja o priloženoj dokumentaciji koja bi primatelju dala potrebne informacije o privitku. Nadodana je izjava o povjerljivosti koja osobi koja ne dolazi iz tehničke pozadine ulijeva jednu dozu važnosti sadržaja e-maila. Kada se pogleda dio iz zaglavlja koji se odnosi na autentičnost:

Authentication-Results: spf=pass (sender IP is 153.127.234.3) smtp.mailfrom=ma-gokoro.jp; dkim=none (message not signed) header.d=none;dmarc=bestguesspass action=none header.from=ma-gokoro.jp;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of ma-gokoro.jp designates 153.127.234.3 as permitted sender) receiver=protection.outlook.com;

može se reći da je slučaj identičan onome iz prethodnog primjera (High Confidence Phish). SPF provjera je prolazna, e-mail nije digitalno potpisan (DKIM), a DMARC bestguesspass znači da ne postoje DMARC TXT zapisi za domenu @ma-gokoro.jp.

S obzirom na nedostatak DKIM-a i DMARC-a ovakav primjer e-maila bi svakako trebao završiti u karanteni. Međutim, primarni razlog zašto e-mail nije dostavljen korisniku je zbog Microsoft tehnologije u pozadini koja je otkrila da je PDF maliciozan, odnosno pripada skupini Malware.

Delivery details

Original Threats
Malware

Latest Threats
Malware

Original location
Quarantine

Latest delivery location
Quarantine

Delivery action
Blocked

Detection technologies
File detonation

Primary Override : Source
None

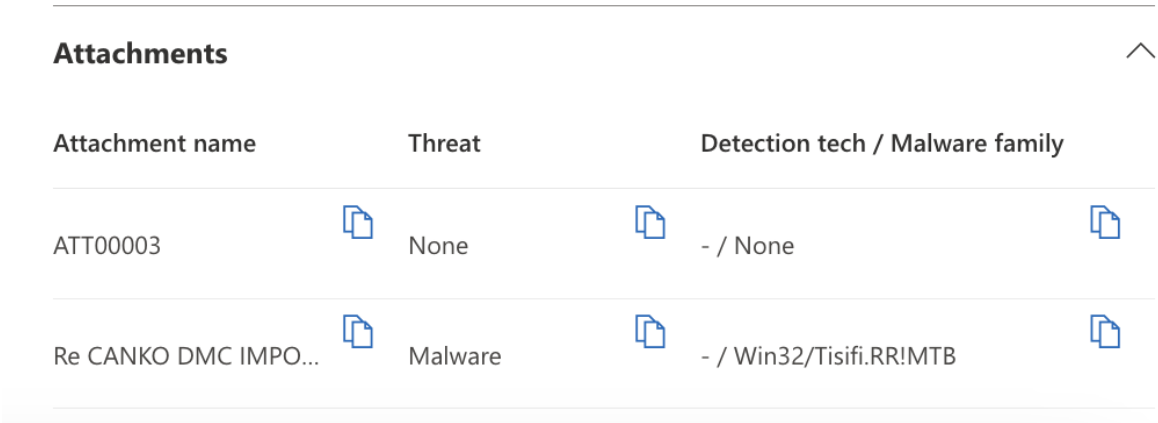
Slika 13 - Primjer za prikaz detalja o malicioznom e-mailu u Microsoft karanteni. Izvor: autor

Tehnologija koja se koristila za detekciju je tzv. File detonation. Ova tehnika svoje provjere vrši tako da se privitak otvori u sigurnom okruženju, tzv. Sandboxu, namijenjenom za testiranje. Otvaranjem se uvidjelo da PDF sadrži maliciozno plaćanje ili mogućnost preuzimanja opasnog koda koji može naštetiti računalu korisnika. [29]

5.4. MALWARE - WIN32

U prethodnom primjeru e-mail je završio u karanteni na način da su Microsoft filteri detektirali potencijalnu opasnost. Međutim, zbog nesavršenosti tehnologija detekcije i filtera (modeli strojnog učenja), mogući su false positive slučajevi. Iz tog razloga se daje izbor administratorima, odnosno pojedincima koji rade na e-mail sigurnosti da na temelju vlastitog znanja i procjene odluče hoće li neki e-mail pustiti do krajnjeg korisnika ukoliko ga filter nije ispravno detektirao.

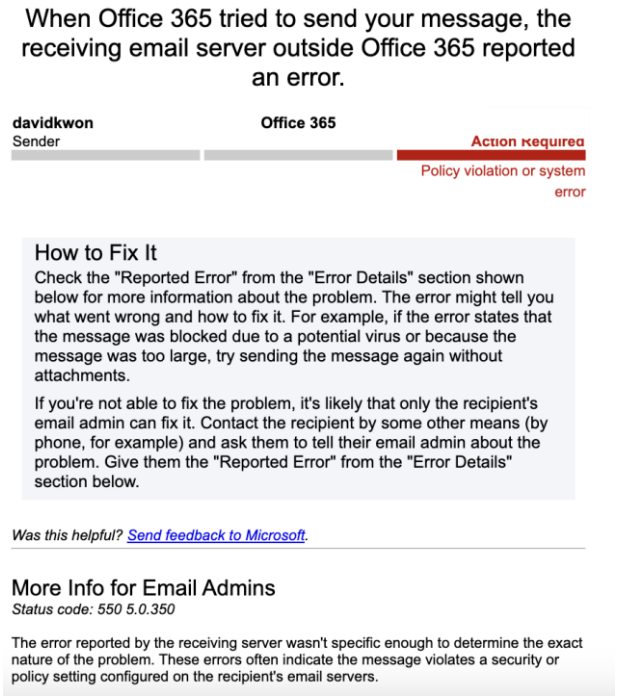
Ovaj primjer se razlikuje od prethodnih jer e-mail nije došao do krajnjeg korisnika, ali nije se ni zadržao u karanteni. E-mail je došao do Microsoft servera, ali ga nije prolongirao dalje. Primarni razlog je taj što sadrži zlonamjerni program (trojanac) /Win32/Tisfi.RR!MTB zamaskiran unutar datoteke dodane u e-mail.



Slika 14 - Primjer za otkrivanje zlonamjernog privitka Win32. Izvor: autor

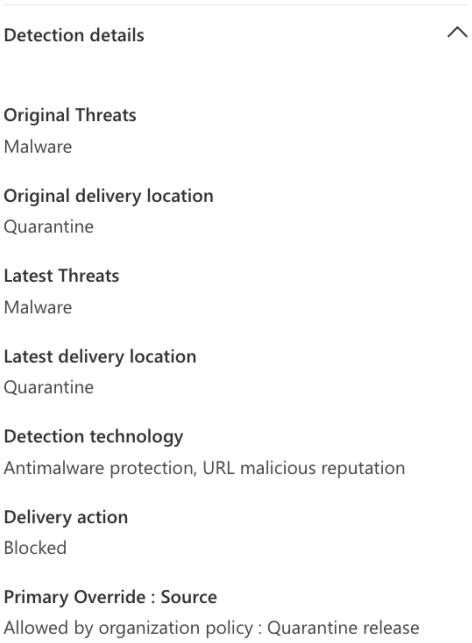
Pošiljatelju se poslao NDR (Non Delivery Report) o detaljima i razlogu zbog kojeg e-mail nije stigao do primatelja. Međutim, ni NDR report nije prošao do pošiljatelja nego je završio u karanteni. Kao što je vidljivo po navedenoj greški, jedan ili više privitaka dodanih u e-mail nisu dozvoljeni od strane organizacije primatelja. Razlog tomu je idući: kompanija ima jasno

definirane politike u kojima su navedeni koji tipovi datoteka su dozvoljeni za primanje/slanje u e-mailu.



Slika 15 - Primjer NDR reporta. Izvor: autor

Microsoft je uz pomoć dvije tehnike detekcije: antimalware protection - identifikacija iz antimalware mehanizama koji se temelje na potpisima i URL malicious reputation - e-mail sadrži URL kojeg su neki drugi izvori detektirali kao prijetećeg, e-mail poslao u karantenu i spriječio da dođe u obliku NDR reporta do napadača.



Slika 16 - Primjer iz Microsoft karantene - detalji o e-mailu. Izvor: autor

5.5. DOCUSIGN PHISHING E-MAIL

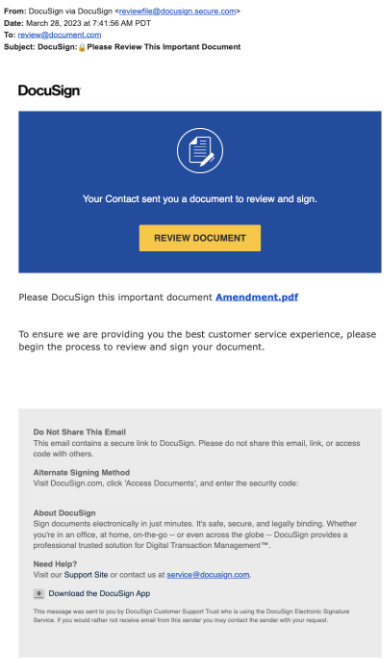
Priložen je primjer jednog učestalog phishing napada - lažirani DocuSign e-mail. DocuSign je platforma koja služi za slanje i elektroničko potpisivanje e-mailova. Lažni DocuSign e-mailovi su tip e-maila koji je vidljiv u karanteni na dnevnoj bazi. Svrha takvih e-mailova je krađa potpisa, osobnih podataka ili podataka kompanije i zloupotreba istih.

Kako bi se uočile razlike između legitimnog i phishing DocuSign e-maila, priložen je primjer preuzet s DocuSign službene web-stranice. Na prvi pogled vizualno (boja i dizajn) oba e-maila izgledaju jako slično. U polju From kao ime je stavljen DocSgn, a pravi e-mail pošiljatelja je: dmainler@exoo.eu.org. Na službenoj stranici DocuSigna objašnjeno je kako legitimni e-mailovi dolaze uvijek sa @docusign.net domene. Ukoliko se fokus stavi na „Review document“ - vidljiv je link koji vodi na URL dallasblackdemocrats, dok legitimni review vodi na “https://www.docusign.net” ili https://eu.docusign.net. Svaki dokument, koji je potrebno potpisati, preko ove platforme dolazi sa jedinstvenim sigurnosnim kodom koji se sastoji od 32 znaka. Razlika je vidljiva i u ovom detalju: kod legitimnog su dijelovi koda odijeljeni s “-”, dok je kod napadačevog skupina znakova spojena. Još jedna bitna razlika je što je kod phishing primjera dodano pod Urgent: High, odnosno, kao što je već spomenuto, izaziva kod primatelja osjećaj hitnosti, žurbe, pritiska, te su u takvim situacijama pogreške češće.

Kada se analiza e-mail header:

spf=pass (sender IP is 54.240.48.102) smtp.mailfrom=amazonses.com; dkim=pass (signature was verified) header.d=exoo.eu.org;dmarc=pass action=none header.from=exoo.eu.org;compauth=pass reason=100

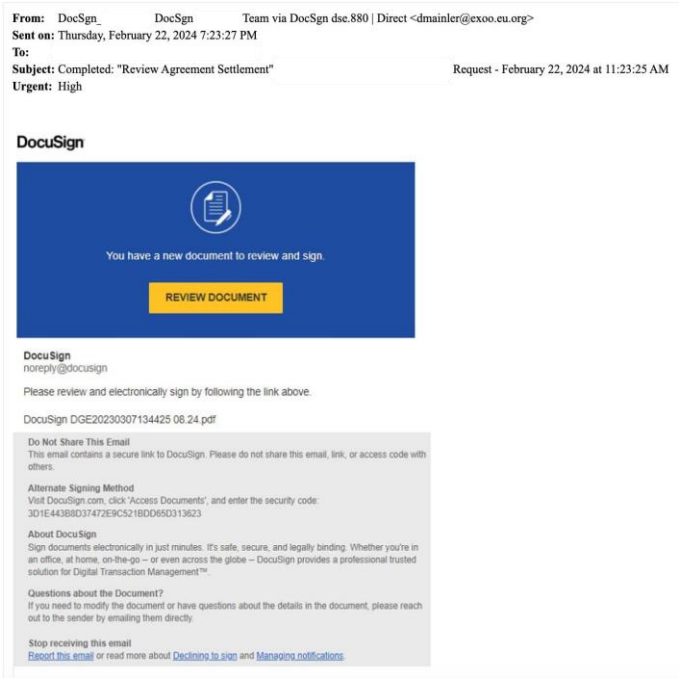
može se zapravo reći kako je ovo dosta uvjerljiv primjer DocuSign pokušaja prevare. Sve 3 provjere autentičnosti su uspješno prošle, čak i dodatna Microsoft provjera zvana composite authentication. Međutim, zahvaljujući testiranju linkova koji se nalaze u e-mailu, ustvrđeno je da su oba zlonamjerna, kao što se i vidi kada se jedan link otvori pa se dobije upozorenje. Ono što se može izdvojiti kao detalj je da u mnogim slučajevima ova dva polja smtp.mailfrom i header.from mogu biti ista, ali u nekim slučajevima mogu biti različita. Primjerice, kada organizacija koristi vanjskog pružatelja usluga e-maila kao što je Amazon SES za slanje e-maila u ime domene (u ovom slučaju, domene exoo.eu.org), adresa e-maila u polju "smtp.mailfrom" bit će adresa pružatelja usluga e-maila (u ovom slučaju, amazonses.com), dok će adresa e-maila u polju "header.from" ostati adresa domene (exoo.eu.org) kako bi korisnici vidjeli pravu adresu pošiljatelja. Ovo se često radi radi transparentnosti i poboljšanja povjerenja korisnika.



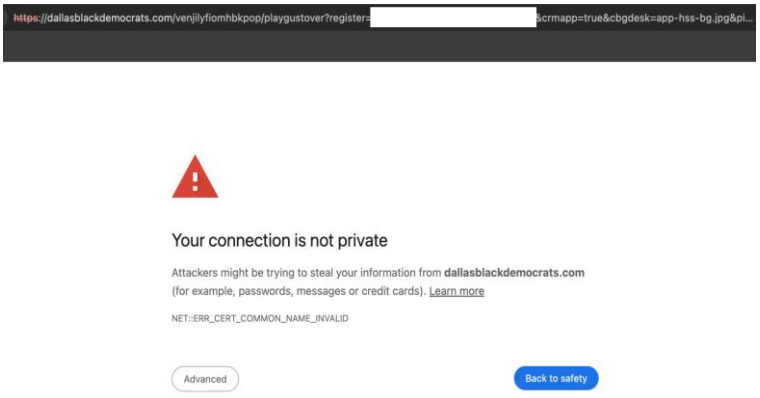
Slika 17 - Primjer DocuSign legitimnog e-maila. Izvor: https://www.docusign.com/trust/security/incident-reporting

Slika 18 - Dodatak na sliku 14. Izvor: isto

DocuSign phishing



Slika 19 - Primjer DocuSign phishing e-maila. Izvor: autor



Slika 20 - Primjer malicioznog URL-a. Izvor: autor

6. EDUKACIJA I PREVENCIJA

Kao najvažniji faktor za pravilnu detekciju i pravovremenu reakciju ističe se edukacija. Ono što kompanije često provode su „Security awareness and training“. Koriste se različiti edukativni video uradci kako bi se uz pomoć animacije pojednostavio i približio uvid u moguće opasnosti i posljedice te kako na njih reagirati.

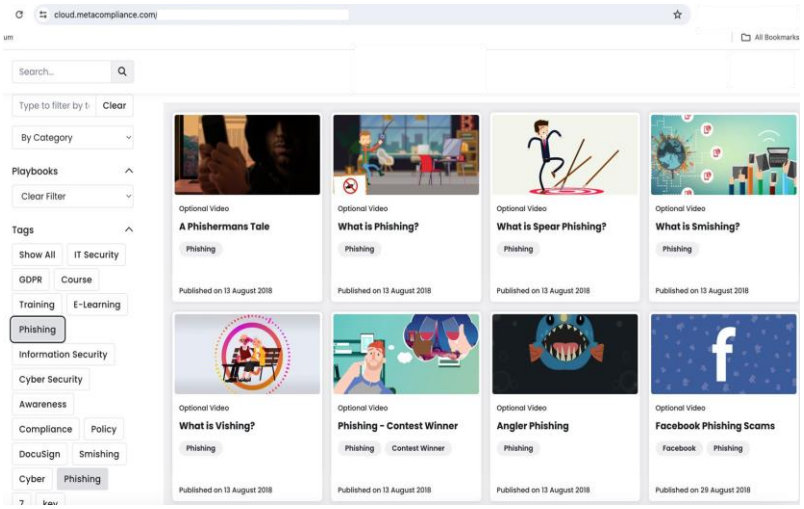
Osim edukacije, često se provodi i „Attack simulation training“, odnosno simulacija (najčešće) phishing e-mailova od strane security i compliance odjela. Ideja takvih treninga je da se korisnicima pošalju e-mailovi phishing sadržaja. Cilj je da se takav e-mail prepozna i pravilno prijavi kao junk ili phishing. Za pravilnu prijavu se najčešće dobije i pozitivna povratna informacija o uspješnoj detekciji. Ukoliko je osoba kliknula na link, otvori se prozor s porukom „You have been phished“ ili sličnog sadržaja, te je takve osobe potrebno iznova educirati. Simulacije se najčešće provode jednom mjesečno, a uspješnost se statistički prati.

Ljudski faktor je glavni element u prevenciji za phishing napade. Uz napredak tehnologije u pozitivnom smjeru dolazi i onaj suprotni napredak, a taj se odnosi na poboljšanje računalnih prijevara, krađa identiteta te kreativnosti i domišljatosti samih kreatora istih.

U svrhu poboljšanja svjesnosti o opasnostima na internetu, kompanije često koriste tzv. MetaCompliance treninge. Njihove platforme pomažu organizacijama u upravljanju rizicima povezanim sa sigurnošću podataka, pružajući alate za obuku zaposlenika, praćenje usklađenosti sa standardima i propisima te provođenje internih kontrola.

Glavni proizvodi MetaCompliance uključuju softver za svijest o sigurnosti, upravljanje usklađenošću, simulacije napada (kako bi se testirala otpornost organizacije na cyber napade), kao i alate za upravljanje incidentima i praćenje promjena u zakonskim zahtjevima. Njihova rješenja usmjerena su na poboljšanje sigurnosne kulture unutar organizacija i osiguravanje da se pridržavaju relevantnih propisa i standarda iz područja sigurnosti informacija i usklađenosti. Ovisno o politikama kompanije, potreba za edukacijom zaposlenika može varirati od one na mjesečnoj bazi, svakih nekoliko mjeseci ili jednom godišnje. Cilj takve edukacije je približiti zaposlenicima jednostavnim jezikom i animacijama opasnosti na internetu te koje korake poduzeti kako bi se obranilo od istih, odnosno spriječile neželjene akcije. Priložen je primjer

izgleda platforme, primjera videa, te oznaka prema kojima je moguće filtrirati videa. Kreira se kampanja tako da se izaberu željeni video uradci te se pošalje obavijest zaposlenicima.

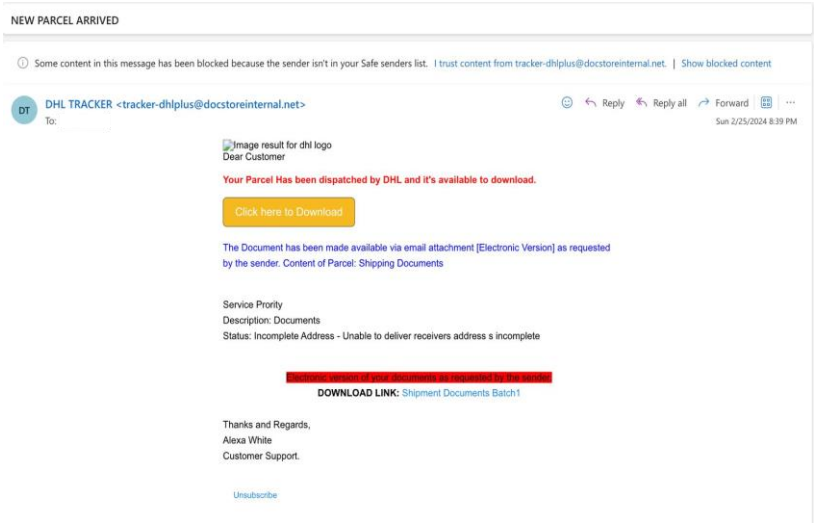


Slika 21 - Primjer edukativnih videa na platformi MetaCompliance. Izvor: https://cloud.metacompliance.com/

Osim edukativnih materijala, kompanije simultano provode i simulacije phishing napada. U sklopu Microsoft Defendera postoji Attack simulation training. Postupak je idući:

a. odabire se tehnika za napad (npr. zlonamjerni URL - phishing, privitak koji sadrži malware, link koji vodi na malware i sl.)
b. odabire se sadržaj e-maila (npr. DHL Parcel Tracker, blokirani Facebook account, OneDrive dokument itd.)
c. uključe se korisnici kojima će biti poslana simulacija
d. odabire se Microsoft trening na koji će biti poslan korisnik ukoliko ne prepozna napad.

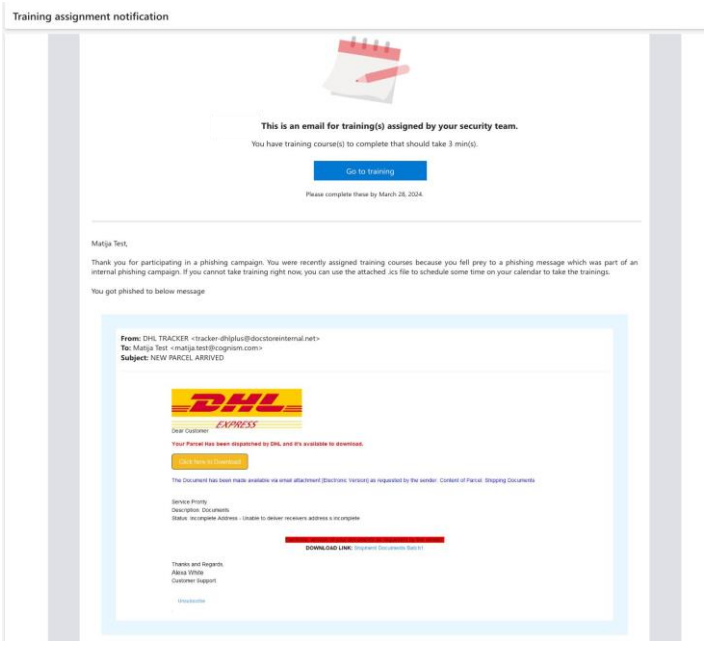
Za potrebe ovog rada, kreirana je testna malware kampanja koristeći lažni DHL tracker koji ima visoku uspješnost od 34% da će primatelj kliknuti. Kada se odabere za download, na korisnikovo računalo se sprema dokument koji sadrži malware.



Slika 22 - Primjer za Microsoft phishing kampanju. Izvor: autor

Nakon odabira za spremanje, dobije se automatski e-mail od Microsofta o treningu koji se dodijelio korisniku jer nije pravilno identificirao phishing e-mail. U suprotnom, korisnik bi e-mail prijavio kao junk/phishing direktno Microsoftu ili MetaCompliance integraciji za phishing.

Za svaku phishing kampanju se automatski izvlače statistički podaci koji pokazuju što je primatelj napravio s primljenim e-mailom (obrisao ga, prijavio, proslijedio, otvorio privitak i sl.).



Slika 23 - Primjer za Microsoft trening. Izvor: autor

7. ZAKLJUČAK

U ovom radu obrađena je sveprisutnost i složenost e-mail napada koji se događaju u današnjem poslovnom i privatnom okruženju. Predstavljeni su alarmantni trendovi u pogledu porasta broja napada, ali i njihove sve sofisticiranije prirode. Kroz proučavanje konkretnih primjera može se uočiti da napadači nisu samo povećali učestalost napada, već su također razvili visoku razinu prilagodljivosti i kreativnosti u svojim strategijama.

Ovi nalazi ukazuju na hitnu potrebu za evolucijom sigurnosnih praksi kako bi se suočile sa sve većim izazovima. Tradicionalni pristupi sigurnosti često su nedovoljni za zaštitu organizacija od modernih prijetnji putem e-maila. Stoga je ključno ulaganje u napredne tehnološke alate koji mogu identificirati i zaustaviti napade u njihovom začetku, kao i u kontinuiranu edukaciju zaposlenika o sigurnosnim rizicima i praksi.

Uzimajući u obzir dinamičnu prirodu sigurnosnih prijetnji, važno je da organizacije usvoje sveobuhvatan pristup prevenciji koji kombinira tehnologiju, obuku i svijest o sigurnosti. Samo integriranim pristupom možemo adekvatno odgovoriti na rastuću prijetnju e-mail napadima i zaštititi organizacije i individue od potencijalnih šteta koje oni mogu prouzročiti.

LITERATURA

[1] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide. [Accessed siječanj 2024].

[2] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure?view=o365-worldwide. [Accessed siječanj 2024].

[3] [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection-about?view=o365-worldwide. [Accessed siječanj 2024].

[4] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide. [Accessed ožujak 2024].

[5] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-end-user?view=o365-worldwide. [Accessed siječanj 2024].

[6] Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/e-mail-security/what-is-e-mail/. [Accessed siječanj 2024].

[7] J. S. Nightingale, "Email Authentication Mechanisms: DMARC, SPF and DKIM," Gaithersburg, 2017.

[8] Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/dns/dns-records/dns-spf-record/. [Accessed siječanj 2024].

[9] "MxToolbox," [Online]. Available: https://mxtoolbox.com/. [Accessed siječanj 2024].

[10] [Online]. Available: https://easydmarc.com/blog/what-are-dmarc-tags-dmarc-tags-explained/. [Accessed veljača 2024].

[11] S. P. Singh, "The Use of DNS Resource Records.," 2012.

[12] Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/email-security/what-is-smtp/. [Accessed ožujak 2024].

[13] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/purview/how-smtp-dane-works. [Accessed veljača 2024].

[14] L. z. s. i. s. Z. z. e. s. i. o. i. F. e. i. r. S. u. Zagrebu. [Online]. Available: https://www.cert.hr/wp-content/uploads/2017/11/DNSSEC_0.pdf. [Accessed ožujak 2024].

[15] [Online]. Available: https://www.catchpoint.com/dns-monitoring/dnssec-validation. [Accessed ožujak 2024].

[16] [Online]. Available: https://simpledns.plus/help/rrsig-records. [Accessed ožujak 2024].

[17] [Online]. Available: https://www.cloudns.net/wiki/article/365/. [Accessed ožujak 2024].

[18] Cloudflare, [Online]. Available: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/. [Accessed ožujak 2024].

[19] [Online]. Available: https://dnsinstitute.com/documentation/dnssec-guide/ch06s02.html. [Accessed ožujak 2024].

[20] [Online]. Available: https://dnsviz.net/d/unizd.hr/dnssec/.

[21] Guardian Digital, [Online]. Available: https://guardiandigital.com/resources/blog/email-threats-explained-what-is-spam-email. [Accessed siječanj 2024].

[22] [Online]. Available: https://www.emsisoft.com/en/blog/27233/what-is-a-botnet/.

[23] Z. Alkhalil, C. Hewage, L. Nawaf and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," 202.

[24] [Online]. Available: https://caniphish.com/blog/how-to-create-a-phishing-email. [Accessed veljača 2024].

[25] [Online]. Available: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf. [Accessed veljača 2024].

[26] National Cyber Security Centre, 6 listopad 2016. [Online]. Available: https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it. [Accessed veljača 2024].

[27] National Cyber Security Centre, 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf. [Accessed veljača 2024].

[28] M. Tracy, W. Jansen, K. Scarfone and J. Butterfield, "Guidelines on Electronic Mail Security," Gaithersburg, 2007.

[29] CrowdStrike, [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/email-spoofing/. [Accessed veljača 2024].

[30] [Online]. Available: https://heimdalsecurity.com/blog/what-is-email-spoofing/. [Accessed veljača 2024].

[31] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-mdo-impersonation-insight?view=o365-worldwide. [Accessed ožujak 2024].

[32] [Online]. Available: https://www.mimecast.com/content/impersonation-attack/. [Accessed veljača 2024].

[33] Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/understand-detection-technology-in-email-entity?view=o365-worldwide. [Accessed veljača 2024].

EMAIL SECURITY IN THE DIGITAL SOCIETY

SUMMARY

Email security in contemporary digital society represents a complex and vital aspect of communication that requires deep analysis and protection strategies. Email, as a fundamental means of communication, faces numerous challenges and security threats. Key protocols like SMTP facilitate message transmission but simultaneously open doors to sophisticated attacks such as phishing, malware, and spam, jeopardizing data integrity and confidentiality.

User education on security procedures and technologies used in email plays a critical role in threat prevention and response. Understanding complex authentication mechanisms, cryptographic techniques, and data protection mechanisms is crucial for establishing a resilient framework in the digital environment. Real-life examples of attacks, like highly sophisticated phishing campaigns targeting specific organizations or institutions, underscore the need for continuous education, prevention, and security awareness. Ultimately, email security demands a holistic approach that combines technical, organizational, and human resources to ensure protection against a wide spectrum of attacks and threats in the digital environment.

KEY WORDS: security, protocols, email, attacks, education, prevention

TABLICA SLIKA