Istraživanje obilježja phishing napada

Starček, Dominik

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:445469

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

ISTRAŽIVANJE OBILJEŽJA PHISHING NAPADA

Diplomski rad

Dominik Starček

Zagreb, rujan 2023.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

ISTRAŽIVANJE OBILJEŽJA PHISHING NAPADA

A STUDY ON FEATURES OF PHISHING ATTACKS

Diplomski rad

Student: Dominik Starček

JMBAG: 0246057122

Mentor: prof. dr. sc. Mario Spremić

Zagreb, rujan 2023.

Sadržaj

SAŽETAK

Informacijski sustavi su svojom pojavom u 20.-om stoljeću značajno unaprijedili proces poslovanja te moderno poslovanje doveli na potpuno novu razinu. Pojavom informacijskih sustava pojavile su se i prijetnje njihovoj sigurnosti. Kao jedna od najozloglašenijih i najopasnijih prijetnji sigurnosti informacijskih sustava izdvojili su se *phishing* napadi. Pojam *phishing* napad označava prijetnju sigurnosti informacijskih sustava i sastoji se od elektroničke pošte koja sadrži poveznicu preko koje se, u slučaju pritiska na istu, na sustav instalira zlćudni kod koji omogućava pojedincu ili organizaciji pristup vrijednim informacijama. Sigurnost informacijskih sustava postala je jedan od imperativa poslovanja u modernom okruženju, te se osim metoda digitalne zaštite podataka počinju razvijati poslovne kulture u kojima je zaštita informacijskih sustava prioritet.

Teorijski dio rada pruža uvid u koncepte informacijskih sustava, sigurnosti informacijskih sustava i *phishing* napada. Temeljni cilj rada je objasniti što su to *phishing* napadi, kako ih prepoznati te kako se zaštititi od njih. U empirijskom dijelu rada bit će prikazana tri odvojena slučaja ovakvih vrsta napada te će se metodom analize slučaja utvrditi njihove sličnosti i posljedice.

Ključne riječi: informacijski sustav, sigurnost informacijskog sustava, *phishing* napadi

SUMMARY

The introduction of information systems in the 20th century has significantly improved the process of business and raised modern business on an entirely different level. However, their introduction also sparked the appearance of threats to their security. One of the most infamous and dangerous of these types of threats is phishing. The term phishing refers to a type of e-mail attack that poses a threat to information system security. The e-mail typically contains a link that, when clicked on, immediately installs malware on the owner's computer, which allows the individual or organization behind this attack access to vital information. Information system security has become crucial for business processes in the modern environment. Digital security alone is no longer sufficient, and modern companies develop workplace cultures that center around information system security.

The theoretical section of this paper provides an insight into the concepts of information systems, information system security, and phishing attacks. The main objective is to clarify what these attacks represent, how to detect them, and how to protect against them. The empirical section of this paper will present three isolated instances of phishing attacks and their analysis using the case study method, which will determine the similarities and consequences of these types of attacks.

Key words: information system, information system security, *phishing* attacks

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.
Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada ne krši bilo čija autorska prava.
Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____
(vlastoručni potpis studenta)

_____
(mjesto i datum

1. UVOD

1.1 Predmet i cilj rada

Jedan od najvažnijih faktora uspješnosti poslovanja danas je intenzivna upotreba tehnologija i informacijskih sustava u poslovanju. Korištenjem informacijskih sustava poslovanje poduzeća postaje konkurentnije, čime postaje izloženo novim vrstama napada: kibernetičkim napadima. Postoje razni oblici kibernetičkih napada, kojima je cilj poduzeću uzeti vrijedne informacije vezane uz informacijske sustave. Vrsta kibernetičkih napada koja će se analizirati u ovome radu su *phishing* napadi. Ciljevi ovoga rada su objasniti što je informacijski sustav i sigurnost informacijskog sustava, objasniti što su *phishing* napadi, koje vrsti *phishing* napada postoje i kako se od njih najbolje zaštititi, prikazati i analizirati studije slučajeva stvarnih te simuliranih *phishing* napada te diskutirati rezultate analize studija slučajeva.

1.2. Izvori i metode prikupljanja podataka

Pri izradi ovog rada korišteni su sekundarni podaci iz stručne i znanstvene literature. Istraživanje se provelo metodom analize tri odvojene studije slučajeva. Na temelju provedenog istraživanja diskutirat će se o sličnostima između slučajeva kao i o metodama zaštite koje su bile ili su mogle biti primijenjene.

1.3. Sadržaj i struktura rada

Rad je strukturiran u šest poglavlja. U uvodu rada objašnjavaju se predmet i cilj rada, svrha istraživanja, izvori i metodologije kojima su se podaci prikupljali i obrađivali te je prikazan način strukturiranja rada. U drugome poglavlju objašnjeno je što su to informacijski sustavi, kako su nastali i razvijali se kroz povijest te koja je njihova uloga u modernom svijetu. U trećem se poglavlju definira i objašnjava sigurnost informacijskih sustava, navode se vrste sigurnosti i detaljnije se prikazuju sve komponente i razine informacijske sigurnosti. Četvrto poglavlje predstavlja uvod u glavni problem ovog rada, a to su *phishing* napadi. Kroz poglavlje je detaljnije objašnjeno što su *phishing* napadi, koje vrste *phishing* napada postoje i zašto se u modernom svijetu smatraju jednom od najopasnijih kibernetičkih prijetnji. U ovome se poglavlju pojašnjavaju i metode obrane od ovakvih vrsta napada te vještine potrebne kako bi se ovakvi napadi u potpunosti izbjegli. U petom su poglavlju analizirana tri slučaja stvarnih ili simuliranih *phishing* napada na temelju kojih je donesen zaključak.

2. INFORMACIJSKI SUSTAV

2.1. Definicija informacijskog sustava

Pojam informacijski sustav označava sustav čije su sastavnice niz komplementarnih komponentni koje svojim usklađenim djelovanjem prikupljaju, obrađuju, pohranjuju i distribuiraju podatke koji su nužni za uspješno provođenje poslovanja (Spremić, 2017). Njihova uporaba vidljiva je u gotovo svim aspektima ljudskog života. Informacijski sustavi koriste se kod aktivnosti kao što su pružanje osobnih usluga (za izdavanje računa), u tehnološkom sektoru (programiranje i analiza podataka) te menadžmentima organizacija (kao alat za organiziranje i skladištenje vrijednih informacija). Kontinuiranom evolucijom i pravovremenom implementacijom novih informacijskih sustava isti mogu postati kompetitivne prednosti organizacije.

2.2. Povijest informacijskih sustava

Počeci informacijskih sustava sežu do 60-ih godina 20.-og stoljeća. Kako je nemoguće opisati ovoliko dugu povijest na jednostavan način, razvoj informacijskih sustava kroz vrijeme raščlanio se na epohe s jasno definiranim granicama koje pojednostavljuju pregled informacijskih sustava. Epohe se mogu podijeliti na : prvu epohu informacijskih sustava koja je trajala od 60-ih do 70-ih godina prošloga stoljeća; druga epoha koja je trajala od 70-ih do 80-ih godina prošloga stoljeća; treća epoha koja je trajala od 80-ih do 90-ih i četvrta epoha koja traje od 90-ih godina do danas (Hirschheim, Kleim, 2010).

Prva epoha informacijskih sustava počinje uvođenjem treće generacije računala (Hirschheim, Kleim, 2010). Autori Hirschheim i Kleim (2010) trećom generacijom računala primarno smatraju model računala 360 poznate američke tvrtke IBM. Prema Pejić-Bach i Spremić et al. (2020), temelj ovakvih računala predstavljao je integrirani sklop koji je omogućavao računalima paralelan rad više programa odjednom i unos podataka pomoću tipkovnice. Karakteristika ove epohe je snažan fokus na razvoj i pomicanje od jednostavnog automatiziranja osnovnih poslovnih procesa prema uspostavi kontrole procesne funkcije podataka, a samim informacijskim sustavima u ovome periodu su najčešće upravljali menadžeri računalnih operacija koji su odgovarali direktoru računovodstva te su se intenzivno primjenjivali u inženjerstvu, računovodstvu, bankovnim poslovima i vojsci (Hirschheim, Kleim, 2010). Velik broj zaposlenika u ovom periodu nije bio sposoban razumjeti koncepte integracije između tehnologije i organizacija te se pojavio strah da će i pojedinci koji posjeduju znanje i vještine koje su potrebne za poslove upravljanja informacijskim sustavima s vremenom početi obavljati svoj posao manje efektivno iz zato što su informacijski sustavi postajali sve kompleksniji u kratkom periodu. U nastojanju da se riješi ovaj problem, akademske institucije u Sjedinjenim Američkim Državama i u Europi formirale su komitete koji su organizirali tečajeve i kurikulume koji su pojedincima služili kao edukacijske smjernice koje su ih

pripremale za karijeru informacijskih analitičara i dizajnera računalnih sustava (Hirschheim, Kleim, 2010).

Autori Hirshhcheim i Kleim (2010) navode kako je drugu epohu razvoja informacijskih sustava obilježio je izum osobnih računala. Uvođenjem nove tehnologije mnoge organizacije su počele transformirati svoje poslovanje u tehnološkom smjeru jer su troškovi osobnih računala bili znatno manji nego kod *mainframe* računala koja su se koristila u prvoj epohi. U ovome periodu nastao je koncept kompetitivne prednosti kojega je stvorio Michael Porter (Hirschheim, Kleim, 2010). Prema ovome konceptu smatralo se da, ako bi menadžment organizacije iskoristio sve mogućnosti koje su informacijski sustavi pružali, isti bi mogli postati jedna od kompetitivnih prednosti organizacije (Hirschheim, Kleim, 2010).

Treću epohu informacijskih sustava obilježava radikalan razvoj *hardwarea*, *softwarea* i telekomunikacija te razvoj TCP/IP protokola za računalne mreže (Hirschheim, Kleim, 2010). Informacijski sustavi u organizacijama počinju dobivati vlastite odjele kojima upravlja šef informativnog odjela (eng. *chief information officer*) te su organizacije počele usklađivati svoje korporativne strategije s IS strategijama (Hirschheim, Kleim, 2010). Unatoč tome što se ovaj period smatra periodom nastanka Interneta, tek će u četvrtoj epohi Internet iz korijenja promijeniti informacijske sustave (Hirschheim, Kleim, 2010).

Četvrtu epohu razvoja informacijskog sustava karakteriziraju najznačajnije promjene u tehnologiji i primjeni tehnologije u poslovnom okruženju (Hirschheim, Kleim, 2010). Rapidan razvoj Interneta omogućuje korištenje novih načina komunikacije i poslovanja koje nisu bila moguća u prošlosti te omogućuje širenje znanja i informacija diljem svijeta a organizacije u ovome periodu počinju mijenjati poslovne strategije tako da maksimalno iskoriste tehnološki napredak kako bi pružile još kvalitetnije te individualizirane usluge klijentima (Hirschheim, Kleim, 2010). Konkurencije u modernom tehnološkom okruženju dosežu nove razine te organizacije opremaju svoje zaposlenike novim mobilnim i računalnim tehnologijama kako bi zaposlenici mogli raditi izvan formalnog radnog vremena te održavati organizaciju relevantnom na tržištu (Hirschheim, Kleim, 2010).

Pojavom raznih programa pretraživanja, kao što su Google ili Yahoo, iz korijena se mijenja način kako pojedinci ili organizacije pristupaju informacijama, a razvoj socijalnih mreža i socijalnog umrežavanja revolucionira komunikacije i interakcije između pojedinaca (Hirschheim, Kleim, 2010).

Razvojem informacijskih sustava postepeno se počinu pojavljivati zloćudni programi i prijevare koje se pomoću njih provode. Jedna od takvih vrsta kibernetičkih prijetnji su *phishing* napadi. *Phishing* napadi prvi put se pojavljuju sredinom 90-ih godina dvadesetog stoljeća kao program pod nazivom *AOHell,* koji je bio prvi automatizirani sustav za krađu osobnih podataka i podataka kreditnih kartica korisnika (Rekouche, 2011). *Phishing* napadi detaljnije će biti analizirani u kasnijim poglavljima.

2.3. Pregled informacijskih sustava

Osnovni zadaci i ciljevi informacijskih sustava su provođenje poslovnih transakcija, bilježenje istih i pohranjivanje podataka te izvještavanje o stanju poslovanja. Informacijska i digitalna tehnologija predstavlja oslonac radu informacijskih sustava u bržem i efikasnijem provođenju poslovnih transakcija. Sastavnice koje čine informacijsku strukturu poslovanja su *hardware*, *software*, *dataware*, *netware*, *orgware* te *lifeware* (Spremić, 2017).

Hardware je dio informacijskog sustava u koji ubrajamo svu fizičku opremu koja vrši input i output podataka te njihovo obrađivanje i skladištenje. Kvaliteta pojedinih dijelova hardwarea direktno utječe na kvalitetu informacijskog sustava a samim time i na konkurentnost u poslovnom okruženju (Stair, Reynolds, 2014).

Softwareom se smatraju računalni programi kojima upravljamo računalima i podijeljeni su na dvije skupine: sistemski *software* i aplikacijski software. Sistemski *software*, kao što je Microsoft Windows ili macOS, upravlja i regulira pokretanjem računala kao i pristupu sistemskim resursima te upravlja računalnom memorijom i podacima. Aplikacijski *software* korisnicima omogućuje izvršavanje specifičnih zadataka kao što je kreiranje financijskih tablica, crtanje grafova, komuniciranje unutar organizacije ili čitanje tekstualnih dokumenata (Stair, Reynolds, 2014).

Dataware je pojam koji označava organiziranu kolekciju činjenica i informacija o klijentima, zaposlenicima, inventaru ili konkurentima. Kroz vrijeme količina podataka se povećava i analogno tome povećavaju se i troškovi održavanja skladištenja podataka, kao i sigurnosti istih (Stair, Reynolds, 2014).

Netware i telekomunikacije su transmisije signala koje nam koriste za telekomunikaciju. Elektroničke transmisije mogu se vršiti putem žičanih, bežičnih i satelitskih transmisija. U modernom okruženju pojedinci i organizacije diljem svijeta koriste kanale telekomunikacije koje im omogućuju rad od doma ili na putu. Kvaliteta kanala telekomunikacije ima izravan učinak na kvalitetu poslovanja pojedinca i organizacija (Stair, Reynolds, 2014).

Orgware ili procedure su koraci kojih se pojedinci moraju pridržavati kako bi ostvarili rezultate. Poštovanje procedura omogućuje brža obavljanje posla, niže troškove te bolje korištenje ljudskih resursa (Stair, Reynolds, 2014).

Lifeware je pojam koji se odnosi na ljudske resurse koji koriste informacijske sustave. Smatra se najosjetljivijom od svih komponenti informacijskog sustava (Stair, Reynolds, 2014).

Phishing napadi smatraju se podvrstom socijalnog inženjeringa kojima je temeljni cilj napasti korisnika informacijskog sustava i krađa povjerljivih podataka (Khonji, Iraqi, Jones, 2013).

2.4. Primjeri informacijskih sustava

Pojava informacijskih sustava predstavljala je novi korak u razvoju tehnologije i isti se počinju upotrebljavati u gotovo svim sferama ljudskog života. Jedna od temeljnih sfera primjene informacijskih sustava je u procesu poslovanja (Pejić-Bach, Spremić et al. 2020).

Prema autorima Pejić-Bach i Spremić et al. (2020), poslovanje je proces koji obuhvaća aktivnosti poput izvršenja poslovnih procesa, upravljanja poslovanjem, aktivnostima komunikacije i suradnje unutar poslovnog sustava te komunikacije s njegovom okolinom. Kombiniranjem faktora poslovanja i mogućnostima koje pružaju informacijski sustavi stvoreni su poslovni informacijski sustavi kojima se unaprjeđuje provođenje poslovnih aktivnosti uz puno manje financijske troškove.

Poslovni informacijski sustav može se definirati kao „informacijski sustav koji obrađuje podatke i informacijski podupire aktivnost u poslovnom području“ (Pejić-Bach, Spremić et al. 2020). Poslovni informacijski sustavi dijele se na (Spremić, 2018):

- Sustav za obradu transakcija – transakcijski sloj sustava.
- Sustav za potporu upravljanju – menadžerski sloj sustava.
- Sustav za komunikaciju i suradnju – komunikacijski sloj sustava (Spremić, 2018).

Sustav za obradu transakcija (eng. *Transaction Processing System*) je dio informacijskog sustava koji funkcionira kao potpora izvršnom podsustavu organizacije te iste povezuje podatkovnim tokovima (Pejić-Bach, Spremić et al. 2020). Transakcijski informacijski sustavi su automatizirani sustavi koji provode i bilježe rutinske transakcije koje su neophodne za pravilno poslovanje organizacije (Al Mamary, Shamsuddin, Aziati, 2014). Sustavi za obradu transakcija smatraju se najčešćim oblikom poslovnih informacijskih sustava, a najviše korišteni uređaji koji se temelje na istima su POS uređaji, čija je funkcija bilježenje prodane robe (Sousa, Oz, 2014).

Može se reći kako je korištenje sustava za upravljanje transakcija znatno utjecalo na efikasnost poslovnih procesa poput trgovanja. Primjena ovakvih sustava omogućila je potpuno nove metode kupnje proizvoda kao što je online kupnja (e-kupnja), gdje korisnici ne moraju biti fizički prisutni tijekom plaćanja već transakcije provode upravo sustavima za obradu transakcija u koje unose podatke sa kreditnih ili debitnih kartica. Sustavi za obradu transakcija imaju mogućnost pohrane tih podataka za buduću kupnju, što u velikoj mjeri olakšava i ubrzava sam proces kupnje. Ipak, ovakvi sustavi podložni su raznim oblicima kibernetičkih rizika jer pohranjeni podaci mogu biti ukradeni ako je sigurnost sustava ugrožena. Iako se *phishing* napadi ne provode transakcijskim informacijskim sustavima, podaci o transakcijama itekako mogu poslužiti kao alat prilikom navođenja korisnika u otkrivanje informacija, što je prikazano prvom analizom slučaja u zadnjem poglavlju rada.

Razvojem tehnologije i količine podataka koje organizacije moraju analizirati kako bi se uspješno provodio poslovni proces i kako bi ostale relevantne na tržištu pojavila se potreba za sustavima koji bi omogućili pojedincima i organizacijama lakše donošenje informiranih odluka,

što je krajem osamdesetih godina rezultiralo pojavom sustava za potporu upravljanju (Pejić-Bach, Spremić et al. 2020).

Sustav za potporu upravljanju (eng. *Decision Support System*) je dio informacijskog sustava namijenjen menadžmentu organizacije kao pomoć u rješavanju problema i informiranom donošenju odluka (Al Mamary, Shamsuddin, Aziati, 2014). Područje primjene ovakvih sustava su strukturirana poslovna okruženja i neefektivni su u donošenju odluka u područjima gdje je nemoguće na temelju prošlih informacija utvrditi ishod budućih situacija, kao što je upravljanje dioničkim portfeljima ili u medicini (Sousa, Oz, 2014). Sustavi za potporu upravljanju pomažu u donošenju poslovnih odluka koje se dijele na strateške, taktičke i operativne poslovne odluke (Spremić, 2018). Jedna od temeljnih poslovnih odluka koje se koncipiraju na strateškoj razini a provode na nižim hijerarhijskim razinama je implementiranje kulture sigurnosti koja je nužna kako bi se organizacija zaštitila od sve učestalijih *phishing* napada.

Sustav za komunikaciju i suradnju (eng. *Communication and Collaboration System*) je definiran kao dio informacijskog sustava čiji je zadatak omogućiti povezivanje unutar organizacije i vezu organizacije s okolinom (Pejić-Bach, Spremić et al. 2020). Cilj ovog sustava je primjena informacijske tehnologije kojom bi se ostvarilo komuniciranje, potpora suradnji, potpora individualnom radu, upravljanje sadržajima i pretraživanje dokumenata (Pejić-Bach, Spremić et al. 2020). Korištenjem informacijske tehnologije i sustava unaprijedilo je proces komuniciranja do razine gdje se isti može vršiti u realnom vremenu iako je između sudionika velika fizička udaljenost. Najpopularniji primjer sustava za komunikaciju i suradnju su društvene mreže poput Facebooka i X-a (Twittera) koje se mogu koristiti za individualnu i poslovnu komunikaciju te Slack koji se primarno koristi za zaštićenu komunikaciju unutar poslovne organizacije. Društvene mreže i same su postale jednim od medija *phishing* napada, posebice *spear phishing* napada koji su visoko individualizirani i sofisticirani napadi (Bossetta, 2018). Sustavi za komunikaciju i suradnju mogu se smatrati izrazito bitnim čimbenikom funkcioniranja poslovnih organizacija današnjice. Spor protok informacija unutar organizacije i loša komunikacija organizacije sa okolinom značajno mogu smanjiti efektivnost poslovanja iste i time omogućiti konkurentima preuzimanje dijela tržišta. Važnost sustava komunikacije i suradnje posebno se ističe u situacijama kada je organizacija pod kibernetičkim napadima poput *phishing* napada jer pravovremeno reagiranje i komuniciranje o propustima u sigurnosti može spriječiti veću količinu štete.

3. SIGURNOST INFORMACIJSKOG SUSTAVA

Intenzivnom uporabom informacijskih sustava organizacije današnjice stječu konkurentnost na tržištu i poboljšavaju proces poslovanja. Međutim, paralelno uz razvoj informatičkih sustava razvijale su se i nove prijetnje i rizici njihovoj sigurnosti koji se nazivaju kibernetičke prijetnje i rizici.

„Kibernetički rizici su poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće“ (Spremić, 2017).

Karakteristike kibernetičkih rizika su njihova konstantna prisutnost te dvojna narav i dijele se na strateške rizike koji proizlaze iz neimplementiranja digitalnih rješenja koja mogu pozitivno utjecati na poslovanje organizacije, rizike neispravno vođenih provedbi informatičkih programa i projekata, operativne ili transakcijske rizike poput ometanja provedbe poslovnih transakcija i neprekidnosti poslovanja, te infrastrukturne informatičke rizike koji se odnose na funkcionalnost računalne mreže i komunikacijske infrastrukture (Spremić, 2017).

Kibernetičke prijetnje mogu se definirati kao događaji koji mogu nanijeti veću količinu štete informacijskom sustavu i dijelimo ih na unutarnje, kao što je interna prijevara ili krađa resursa, ili vanjske, kao što je hakerski napad ili virus te predstavljaju, uz međudjelovanje organizacija i ranjivost sustava, jedan od tri faktora funkcije procjene kibernetičkih rizika (Spremić, 2017).

Razvojem informacijskih sustava i novih funkcija koje isti pružaju otvaraju se vrata razvoju novih vrsta kibernetičkih prijetnji i rizika. Informacijski sustavi postaju ciljem napada ne samo u organizacijama privatnog već i državnog sektora te posljedice takvih napada mogu biti kobne i za nacionalnu sigurnost. Zbog toga je veoma važno kontinuirano ulaganje u sigurnost informacijskih sustava. Spremić (2017) tako navodi da je broj sigurnosnih incidenata koji su rezultat kibernetičkih rizika u stalnome porastu i povećao se sa 33.4 milijuna 2009. godine do 43 milijuna 2014. godine.

Operacija Aurora niz je kibernetičkih napada koji su se dogodili 2010. godine u privatnim kompanijama u SAD-u kako bi se ukrali njihovi podaci. Jedina kompanija koja je javno priznala da je napadnuta bila je Google, a za napad je optužila Kinu na temelju ukradenih privatnih podataka koji su pripadali kineskom aktivistu. Napad je zbog krađe informacija okarakteriziran kao industrijska špijunaža i predstavljao je prekretnicu u korištenju tehnologije za krađu informacija (Council on Foreign Relations, 2010).

3.1. Definicija sigurnosti informacijskog sustava

Informacijski sustavi organizacija današnjice toliko su međusobno različiti da nije moguće tvrditi da postoje dva u potpunosti identična informacijska sustava (Spremić, 2017). Samim time, provođenje sigurnosti informacijskog sustava predstavlja jedinstven proces za svaku organizaciju i zahtjeva različite pristupe i resurse potrebne za uspostavu iste (Spremić, 2017).

Informacijska sigurnost je skup metoda i tehnika kojim se informacije i informacijski sustavi štite od zloporabe (Whitman, Mattord, 2021). Metode zaštite od prodora informacijske sigurnosti su procedure, edukacije i treninzi dok se standardi zaštite informacijske sigurnosti temelje se na tri komponente informacija; povjerljivosti, integritetu i dostupnosti (Whitman, Mattord, 2021).

Povjerljivost je karakteristika informacije da samo pojedinci s određenim pravima i privilegijama imaju mogućnost pristupiti informacijama, a metode koje se koriste kako bi se sačuvala povjerljivost podataka su klasifikacija informacija, sigurno skladištenje dokumenata, primjena općih sigurnosnih politika i edukacija zaposlenika (Whitman, Mattord, 2021). Narušavanje povjerljivosti podataka može biti fizičko, u slučaju da fizički dokument s vrijednim informacijama nakon uporabe nije uništen (Whitman, Mattord, 2021). ili digitalno ako pristup informacijama nije autoriziran odgovarajućim rolama u sustavu (Spremić, 2017). Integritet je svojstvo informacije da ostane u cjelovitom obliku, da bude točna i da ni na koji neovlašteni način ne bude izmijenjena te se zaštićuje u prijenosu, ako se radi o dinamičkim podacima, ili u mirovanju, ako se radi o statičkim podacima (Spremić, 2017). Dostupnost je definirana kao karakteristika informacije da osigurava pristup informacijama osobama koje su ovlaštene koristiti se tim istim podacima i postiže se primjenom kontrola upravljanja kontinuitetom poslovanja i metodama oporavka poslovanja (Spremić, 2017). Primjerice podaci iz financijskih izvješća moraju biti povjerljivi na način da pristup imaju samo osobe unutar organizacije sa zahtijevanom autorizacijom, kao što je izvršni ili financijski direktor. Ti podaci također moraju imati integriteta tako da niti jedan dio izvješća nije lažiran ili pogrešno izračunat i moraju biti dostupni kada ih autorizirana osoba zatraži.

Temeljem pojmova komponenti informacija lako je uočiti zašto su one toliko bitne za održavanje sigurnosti informacijskog sustava organizacije. Većina poslovnih organizacija povjerljive informacije o poslovnom procesu nastoji zaštititi i pravnim putem pomoću ugovora o tajnosti podataka kako bi sadašnjim ili bivšim djelatnicima onemogućila zloporabu. Nepoštivanjem tih ugovora menadžment organizacije može pokrenuti pravni postupak protiv osobe zaslužne za curenje informacija i pravo na financijsku odštetu.

3.2. Komponente sigurnosti informacijskog sustava

3.2.1. Kontrole rada informacijskog sustava

Uspostavljanje sigurnosti informacijskog sustava dugotrajan je i zahtjevan proces koji je nužan kako bi sustav funkcionirao na visokoj razini i omogućavao nesmetan proces poslovanja organizacije. Proces zaštite informacijskog sustava realizira se planiranjem te izvršavanjem kontrola koje su ugrađene u iste i kojima je cilj uklanjanje kvarova i smetnji koje potencijalno mogu naštetiti njegovom radu (Spremić, 2017).

Informatičke kontrole zaštitni su mehanizmi koji informacijske sustave štite prevencijom, detekcijom i korigiranjem neželjenih događaja (Spremić, 2017). Kako bi se postigla što viša

razina efikasnosti potrebno je uspješno izvršiti što veći broj ispravno izvedenih kontrola čime se znatno smanjuje vjerojatnost izlaganja sustavu vanjskim i unutarnjim prijetnjama, međutim uz kontinuiran razvoj i kompleksnost informacijskih sustava potpunu sigurnost nije moguće postići (Spremić, 2017).

Automatske kontrole su zaštitni procesi informacijskih sustava kojim oni samostalno uklanjaju greške bez značajne angažiranosti korisnika, dok se ručnim kontrolama smatra korisnikovo samostalno otkrivanje prijetnji i njihovo uklanjanje (Spremić, 2017). S obzirom na prirodu *phishing* napada može se zaključiti kako filtar elektroničke pošte djeluje kao automatska kontrola sustava dok se ručna kontrola odnosi na korisnikovo brisanje poruka koje su potencijalni napadi.

Detektivnim kontrolama otkrivaju se propusti, pogreške ili sumnjivosti pri korištenju informacijskog sustava kao što su primjerice pogreške u programskom kodu, pristup sustavu bez potrebne autorizacije ili elektronička pošta sumnjivog sadržaja (Spremić, 2017). Ovim kontrolama može se pristupiti na dva načina: korisnikovom detekcijom i softverskim rješenjima (Khonji, Iraqi, Jones, 2013). Kontrole temeljene na korisnikovoj detekciji u velikoj mjeri ovise o kvaliteti edukacije korisnika u prepoznavanju znakova koji upućuju da se radi o *phishing* napadima dok su softverska rješenja alat koji nadopunjuje korisnika otkrivanjem eventualnih grešaka u njegovoj prosudbi (Khonji, Iraqi, Jones, 2013).

Nakon što se potencijalna prijetnja detektira cilj joj je umanjiti efekt koji ima na sustave pomoću korektivnih kontrola (Spremić, 2017). U slučaju *phishing* napada, korektivnim kontrolama se uništavaju resursi *phishing* napadača brisanjem *phishing* stranica i sadržaja te suspendiranjem računa elektroničke pošte sa koje je napad izveden (Khonji, Iraqi, Jones, 2013).

Preventivne kontrole služe za predviđanje potencijalnih budućih problema stalnim nadgledanjem aktivnosti informacijskog sustava i njihov proces započinje prije samog napada te se vrši metodama poput obrazovanja djelatnika, imenovanjem upravnog odbora za informatiku, podjelama dužnosti i odgovarajućih autorizacija djelatnicima te mnogim drugim aktivnostima (Spremić, 2017). U kontekstu *phishing* napada, preventivne kontrole imaju sličnu ulogu kao i detektivne kontrole; osposobiti pojedinca edukacijama kako bi se povećale vjerojatnosti otkrivanja detalja koji upućuju da se radi o *phishing* sadržaju (Khonji, Iraqi, Jones, 2013).

Fizičke kontrole odnose se na kontrole izvan informacijskih sustava a cilj im zaštiti sve što je materijalno i opipljivo te pripada organizaciji na način da se fizički ograniči pristup prostorima organizacije i postrojenjima u kojima se skladište podaci (Spremić, 2017). Primjerice, korisno je pri uspostavljanju fizičkih zaštita paziti na dizajn ureda i izbjegavati otvorene planove koji olakšavaju neometano kretanje pojedinaca koji nisu osobe od povjerenja, kao što je novi kandidat za posao koji može poslovne informacije prosljeđivati konkurentima. Iako su *phishing* napadi primarno oblik kibernetičke prijetnje, logično je da informacije korištene prilikom njegovog izvođenja mogu biti prikupljene i vanjski suradnici koji djeluju kao industrijski špijuni, zbog čega je bitno uspostaviti propisno autoriziran pristup prostorima organizacije.

Nedostatak velikog broja kontrola je pretjerana usmjerenost na tehnološke aspekte sigurnosti i zanemarivanje utjecaja korisnika na sustav te je bitno je naglasiti holistički pristup upravljanju

sustava koji opisuje utjecaj vodstva organizacije na razinu njene sigurnosti (Spremić, 2013). Spremić (2013) predlaže model nadgledanja sigurnosti informacijskog sustava prikazanog na slici 1. Cijevi ovog modela nadgledanja su:

- Poravnanje strategije sa poslovnim ciljevima.
- Implementiranje procedura upravljanja rizikom temeljenih na poslovnoj analizi.
- Investiranje i očuvanje informatičkih resursa kako bi se mogla isporučiti vrijednost.
- Upravljanje tehnološkim i ljudskim resursima.
- Upravljanje performansima poput ključnih pokazatelja performansa i sigurnosti.
- Integracija procesa osiguranja poput revizije sustava (Spremić, 2013).

Slika 1 - Informatičke kontrole razvrstane prema hijerarhiji

Izvor: Spremić, M. (2013), Corporate IT risk management model: a holistic view at managing information system security risks, u: Spremić M., International Conference on Information Technology, (str. 299-304), Zagreb: Faculty of Economics & Business

Pokretačima poslovanja (eng. *business drivers*) smatraju se načela putem kojih se provodi nadgledanje sigurnosti informacijskih sustava i kojima se definira strateški cilj poslovanja, poduzimaju se mjere kako bi se osigurali poslovni ciljevi, osiguravaju se potrebni koraci za upravljanje rizicima i kontrolira se način na koji se koriste resursi organizacije (Spremić, 2013).

Korporativne kontrole predstavljaju politike kojima se dugoročno definira način poslovanja i kultura sigurnosti u organizaciji te se odnose na sve razine hijerarhije organizacije (Spremić, 2013). Njima se definira koji rizik je organizaciji prihvatljiv i neće prouzrokovati veliku štetu, koji su mjerni pokazatelji sigurnosti, tko je odgovoran ako dođe do propusta u sigurnosti informacijskih sustava te način na koji će se provoditi njegove revizije (Spremić, 2013).

BYOP (eng. *bring your own device*) je primjer korporativne politike informacijske sigurnosti koja pruža zaposlenicima i ostalim autoriziranim korisnicima mogućnost korištenja vlastite tehnologije kao medija pristupa mreži organizacije i izvršenja poslovnih obaveza (IBM, What

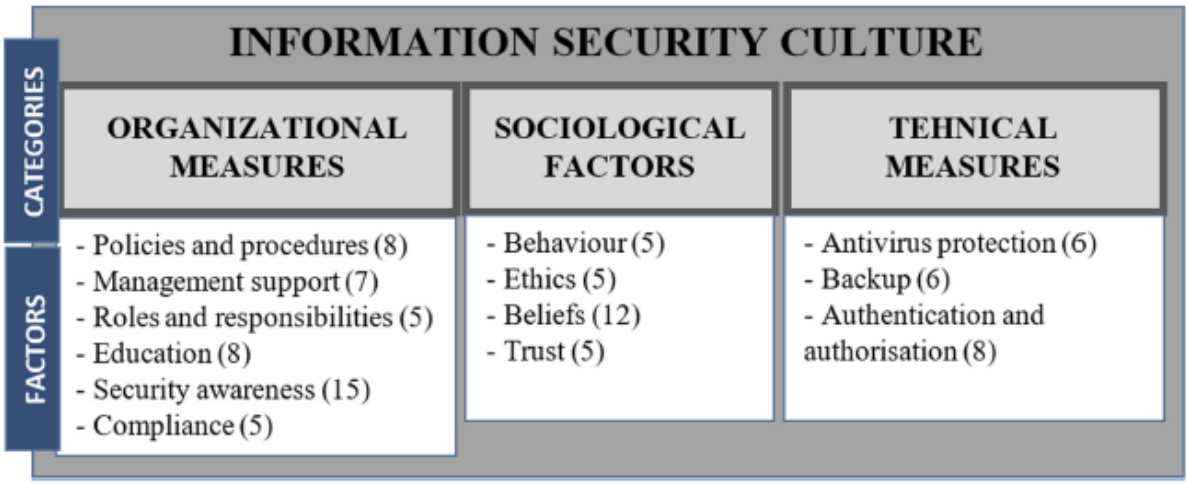
is BYOD (bring your own device)?). Većina BYOP politika unutar organizacije je sastavljena od strane glavnog direktora informatičkog odjela i definira što je: dozvoljena uporaba, koje uređaje zaposlenik može koristiti, koje su sigurnosne mjere, što su privatnost i dozvole, naknade troškova, IT potpora i koje su procedure nakon otpuštanja zaposlenika (IBM, What is BYOD (bring your own device)?). Prednosti uporabe BYOD politika su mnoge, od kojih su najbitnije ušteda troškova, brže zaposlenje i povećana produktivnost zaposlenika dok su negativne strane politike moguće narušavanje privatnosti zaposlenika, limitiran broj novih kandidata za posao, sigurnosni rizici koji se ne rješavaju BYOD politikom te regulacije po pitanjima usklađenosti (IBM, What is BYOD (bring your own device)?). Uvođenje BYOD politike može dovesti informacijski sustav organizacije u opasnost ako nisu uklonjeni sigurnosni rizici njenog implementiranja (Hajdarevic, Allen, Spremić, 2016). Organizacije sa niskom razinom sigurnosne osviještenosti često se oslanjaju na djelatnikovu sposobnost detektiranja prijetnji, što može predstavljati problem u BYOD okruženju ako budu žrtve *phishing* napada jer napadači putem njihovim računala imaju direktan pristup korporativnoj mreži (Flores, Qazi, Jhumka, 2016).

Temeljni zadatak upravljačkih ili administracijskih kontrola je implementacija politika korporativnih kontrola na taktičkoj razini, pri čemu se kontrole mogu provoditi u sukladnosti sa uspostavljenim regulativama (Spremić, 2013). Upravljačke kontrole se tako mogu podijeliti na obvezne ili diskrecijske kontrole, pri čemu se obveznim kontrolama ispunjavaju svi standardi uvriježenih regulacija ali potencijalno neće pružiti svu potrebnu zaštitu informacijskom sustavu, dok se diskrecijske kontrole definiraju korporativnim politikama i podupiru temeljne ciljeve poslovne organizacije ali možda ne ispunjavaju sve standarde regulativa (Spremić, 2013). Regulative koje se najčešće koriste u zaštiti informacijskih sustava su CobiT 5, ISO 27001:2013, PCI DSS, NIST i SANS (Spremić, 2017).

Operativne kontrole ili aktivnosti odnose se na upravljanje informacijskim sustavom organizacije te uključuju kontrole sustava, kontrole pristupa, kontrole prava korisnika itd (Spremić, 2013).

Kultura informacijske sigurnosti je okvir koji se temelji na kontinuiranom održavanju sigurnosnog ponašanja u organizacijama i teško ga je mjeriti empirijskim metodama (Arbanas, Spremić, Hrustek, 2021). Implementacija okvira kulture sigurnosti zahtijeva holistički i višeslojan pristup koji se sastoji od tehnoloških i organizacijskih mjera te sociooloških faktora, kao što je prikazano na slici 2 (Arbanas, Spremić, Hrustek, 2021).

Slika 2 - Koncept okvira kulture informacijske sigurnosti organizacije



Izvor: Arbanas, K., Spremić, M., Žajdela Hrustek, N. (2021), Holistic framework for evaluating and improving information security culture, Aslib Journal of Information Management, 73(5), 699-719.

Prema Laycock, Petrić i Roer (2019) kultura sigurnosti sastoji se od sedam dimenzija kao što su:

- Ponašanje – djela ili aktivnosti koje imaju izravan utjecaj na sigurnost organizacije (Laycok, Petrić, Roer, 2019).
- Stavovi – osjećaji i uvjerenja koja djelatnici organizacije imaju prema protokolima (Laycok, Petrić, Roer, 2019).
- Spoznaje – razumijevanje djelatnika o posljedicama opasnosti proboja sigurnosti (Laycok, Petrić, Roer, 2019).
- Komunikacija – otvorena komunikacija o sigurnosti sustava i prijavljivanje neželjenih događaja (Laycok, Petrić, Roer, 2019).
- Usklađenost – razina pridržavanja zapisanih pravila i procedura (Laycok, Petrić, Roer, 2019).
- Norme – pridržavanja pravila na način da djelatnicima takvo ponašanje djeluje normalno i poželjno (Laycok, Petrić, Roer, 2019).
- Odgovornost – prihvaćanje svojih uloga u sigurnosti organizacije (Laycok, Petrić, Roer, 2019).

Kombinacijom i poštivanjem kontrola rada i kulture sigurnosti sustava stvara se potencijalno moćan alat zaštite informacijskih sustava od kibernetičkih prijetnji poput *phishing* napada. Međutim važno je razviti kvalitetan teorijski koncept na korporativnoj razini upravljanja i adekvatno ga implementirati na nižim hijerarhijskim razinama. Detaljniji pregled ostalih alata kojim se organizacije mogu zaštititi od takvih prijetnji analizirat će se u četvrtom poglavlju.

3.2.2. Zaštitne mjere informacijske sigurnosti

Upravljanje sigurnošću informacijskog sustava dugotrajan je proces koji zahtjeva velike količine ljudskih i financijskih resursa, tim više što kibernetički rizici postaju sve sofisticiraniji. Kontinuiranim razvojem kibernetičkih prijetnji povećali su se zahtjevi za razvojem novih i boljih mehanizama obrane informacijskih sustava od istih. Ti mehanizmi obrane kolektivno se nazivaju zaštitnim mjerama informacijske sigurnosti i zadatak im je spriječiti njihovu krađu, uništenje, oštećenje ili neovlaštenu uporabu (Spremić, 2017).

Kontrole pristupa su metode kojima se nadgleda i ograničava pristup resursima unutar organizacije (Sattarova, Tao-hoon, 2007). Kontrole pristupa sastoje se od politika, subjekta i objekta te se provode u tri koraka (Ballad, Banks, 2011):

- Identifikacija – proces kojim se korisnik identificira sustavu
- Autentifikacija – potvrda korisnikovog identiteta
- Autorizacija – donošenje odluke o davanju pristupa objektu (Ballad, Banks, 2011)

Autorizacija je izrazito bitna stavka kontrole pristupa i definira se kao skup pravila koji opisuju subjekte (korisnike) i objekte (resurse) (Ballad, Banks, 2011). Veće i kompliciranije organizacije mogu imati više stupnjeva autorizacije, primjerice izvršni direktori mogu imati pristup svim osjetljivim informacijama dok djelatnici mogu pristupiti samo informacijama potrebnima za provođenje poslovnog procesa (Ballad, Banks, 2011). Autorizacija može biti korisna obrana od *phishing* napada ako su napadnuti djelatnici koji nemaju potrebnu razinu autorizacije da pristupe vrijednim informacijama. Međutim napadi mogu ciljati i menadžment organizacije sa višom razinom autorizacije zbog čega je potrebno kombinirati više zaštitnih kontrola i mjera na svim hijerarhijskim razinama.

Kriptografija je tehnika zaštite podataka koja povjerljive informacije pretvara u tajni, neautoriziranim osobama nečitljiv (šifriran) sadržaj (Kessler, 2015). Kod provođenja kriptografije važno je obratiti pozornost na komponente kriptografskog procesa. Proces kriptografije čini 5 komponenti (NIST, 2004):

- Autentifikacija podataka – provodi se kriptografskim algoritmom i utvrđuje je li se podacima prethodno manipuliralo (NIST, 2004). Kriptografski algoritmi koji se koriste su tajni ključ, javni ključ i hash funkcije i pomoću njih se provodi proces dekriptiranja podataka (Kessler, 2015).
- Digitalni potpis - potvrđuje identitet originalnog pošiljatelja i može se koristiti kod svih oblika elektroničkih dokumenata kao što su elektronička pošta ili forma. Digitalni potpis može se potvrditi korištenjem jedinstvenog ključa (NIST, 2004).
- Upravljanje ključem - izrazito važna komponenta kriptografskog procesa. Kako bi kriptografski sustav funkcionirao na željenoj razini, ključevi moraju biti propisano generirani, distribuirani, korišteni te naposljetku uništeni (NIST, 2004).
- Sigurnost kriptografskih modula - komponenta kojom se opisuje dizajn, implementacija i način korištenja kriptografskih modula (NIST, 2004).

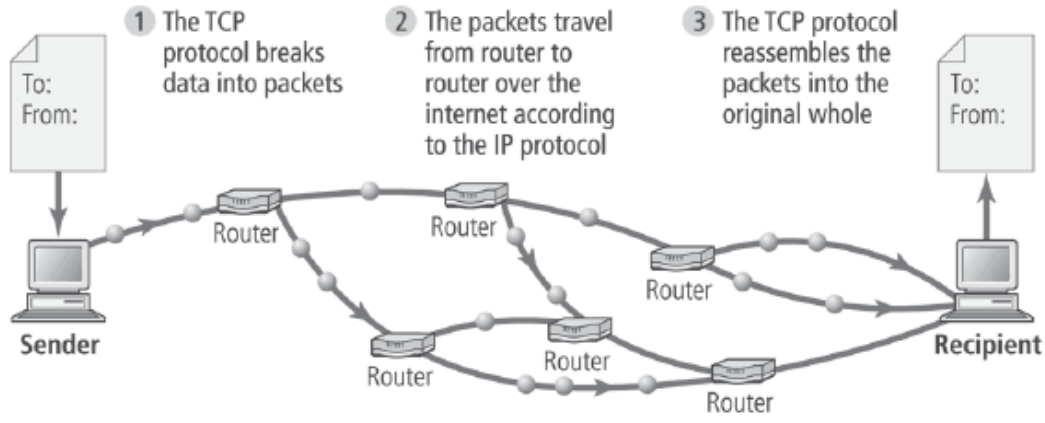
- Kriptografska validacija - posljednja komponenta kriptografije kojom se verificiraju kriptirani podaci (NIST, 2004).

Digitalni potpis temeljna je metoda zaštite u kriptografskom procesu i slanje kriptiranih poruka bez njega nije moguće jer služi kao autorizacija kojom se primatelju potvrđuje da kriptirana poruka dolazi od konkretnog pošiljatelja, a uvjet za korištenje digitalnog potpisa je njegova jedinstvenost za pošiljatelja i metoda verifikacije kojom se može utvrditi njegov identitet (Spremić, 2017). Iako je kriptografija efektivan način očuvanja integriteta i dostupnosti podataka, niti jedan podatak nije moguće u potpunosti zaštiti te kako bi njihova sigurnost bila što kvalitetnija potrebno ju je kombinirati s ostalim metodama zaštite. Kriptografija se kao zaštita koristi u *man-in-the-middle* napadima koji se mogu klasificirati kao vrsta *phishing* napada, gdje se napadač pozicionira u komunikacijski kanal između pošiljatelja i primatelja, međutim proboj kriptografske zaštite je moguć ako napadač posjeduje ključ kojim dekriptira poruke (Mallik, 2018).

Jedan od najvažnijih segmenata poslovanja organizacija je široka upotreba računalnih mreža, kompleksnih sustava koji se sastoje od međusobno povezanih računala i ostalih elektroničkih uređaja koji, uz primjenu komunikacijskih protokola, mogu povezivati poslovanje i distribuirati resurse poslovanja (Spremić, 2017). Život u današnjem vremenu gotovo je nemoguć bez korištenja računalnih mreža. Internet je kao globalna i hibridna mreža u znatnoj mjeri pojednostavio poslovanje organizacijama ali i poboljšao životne standarde korisnicima zbog čega se danas smatra javnim dobrom, a njegovom uporabom korisnici mogu pristupiti velikoj količini podataka i informacija koji bi im inače bili nedostupni, omogućuje pojedinačno slanje podataka i komuniciranje u realnom vremenu medijima poput elektroničke pošte i društvenih mreža, koji s vremenom postaju primarnim medijima *phishing* napada (Spremić, 2017).

Sav sadržaj koji se šalje putem Interneta dijeli se u „pakete“ koji čine mrežni promet i koji se uređuje protokolima, a osnovni protokoli koji se koriste za tu svrhu su TCP/IP protokoli (Spremić, 2017). TCP/IP protokoli poslani sadržaj dijele između više usmjernika i ponovno ga sastavljaju kada dođe kod primatelja, kao što je prikazano na slici 3.

Slika 3 - Postupak razmjene sadržaja u internetskome okruženju primjenom TCP/IP protokola



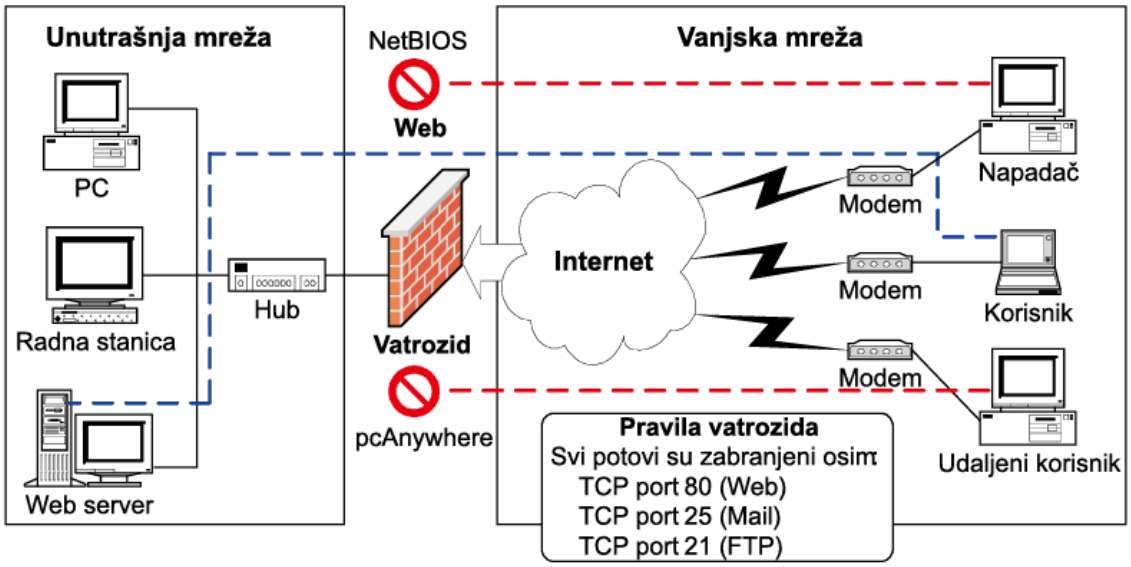
Izvor: Spremić, M. (2017), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.

Vatrozid ili obrambeni zid (eng. *firewall*) je uređaj koji korisnicima osobnih računala omogućuje da zaštite svoju mrežu od vanjskih prijetnji. Vanjske prijetnje dolaze iz javne mreže pa sam vatrozid djeluje na principu da omogući kontrolirani pristup javnoj mreži putem privatne mreže. Osnovne funkcije koje vatrozid koristi kao sigurnost sustava su (Sviličić, Kraš, 2005):

- Paketno filtriranje koje uspoređuje IP i TCP protokole sa pravilima iz baze pravila i time određuje koji će se paketi prosljeđivati (Sviličić, Kraš, 2005). Princip rada paketnog filtriranja prikazan je na slici 4.
- Maskiranje mrežnih adresa kojim se skriva identitet korisnika unutarnje mreže pa tako predstavlja značajnu sigurnosnu mjeru privatnosti, no ne i direktne sigurnosti sustava (Sviličić, Kraš, 2005).
- Posredne usluge (eng. *proxy services*) koje štite identitete korisnika preuzimanjem njihovih zahtjeva, primjerice pretraživanja na Internetu, i prosljeđuje ih dalje servisima na vanjskoj mreži (Sviličić, Kraš, 2005).
- Virtualne privatne mreže koje su metoda kriptografske zaštite podataka koji se prenose iz jedna privatne mreže u drugu putem javne mreže, kombinirajući pritom pozitivne strane obje (manjih troškova i šire dostupnosti javne mreže i sigurnost privatnih mreža (Sviličić, Kraš, 2005).

S obzirom na funkcionalnosti vatrozida može se zaključiti kako se njime ne može zaustaviti *phishing* napade jer ne posjeduje funkcionalnost sprječavanja dolaska elektroničke pošte, međutim ima sposobnost blokiranja zloćudnog sadržaja i stranica koje se nalaze u *phishing* pošti.

Slika 4 - Paketno filtriranje kao funkcija vatrozida



Izvor: Sviličić, B.(2005), Zaštita privatnosti računalnog sustava, Pomorstvo, 19, 275-284.

Određene vrste protokola nisu samo metoda zaštite podataka od krađe već i temeljni zahtjevi funkcionalnosti sustava, kao što je HTTP (eng. *Hyper Text Transfer Protocol),* protokol kojim se realizira razmjena sadržaja između web preglednika i stranice te omogućuje vidljivost

sadržaja na zaslonu, dok HTTPS (eng. *Hyper Text Transfer Protocol Secure*) predstavlja njegovu sigurniju verziju koja šifrira sadržaj prije razmjene i koristi se u područjima kao što su internetsko bankarstvo ili e-trgovina kako bi se zaštitili povjerljivi osobni podaci (Spremić, 2017.). Phishing napadi često u sadržaju elektroničke pošte sadrže HTTP linkove koji korisnike preusmjeravaju na zlođudne stranice (Khonji, Iraqi, Jones, 2013).

Zbog opsežnosti i kompleksnosti računalnih mreža one se često razdvajaju uporabom raznih uređaja poput usmjernika, prespojnika ili mostova procesom koji se naziva segmentacija mreže, a vrši se zbog sigurnosnih i poslovnih razloga kao što su utjecaji lokalnih kvarova i zagušenje rada mreže (Spremić, 2017). Segmentiranjem mreže stvaraju se razine sigurnosti čime se sprječava širenje posljedica napada unutar organizacije (Mhaskar, Alabadd, Khedri, 2021). Primjerice ako se dogodi *phishing* napad na djelatnika organizacije napadačima se onemogućuje pristup važnijim informacija sa višom razinom sigurnosti.

3.3.3. Revizija informacijskog sustava

Gotovo svaka poslovna organizacije današnjice koristi informacijske sustave pri provođenju procesa poslovanja, međutim konstantna orijentiranost na progresiju takvih sustava u njima stvara mnoge slabosti koje se često uoče tek kad je prekasno i kad je sigurnost sustava narušena. Kako bi se odredila razina efektivnosti informacijskog sustava potrebno je nad njim redovito provoditi revizije.

Revizija informacijskih sustava je postupak kojim stručnjaci, koji se nazivaju revizorima, prikupljaju i procjenjuju pokazatelje pomoću kojih donose zaključak o djelotvornosti sigurnosti informacijskog sustava i čiji je temeljni zadatak precizno i sustavno procijeniti rad kontrola svih dijelova informacijskog sustava te trenutno stanje u kojemu se sustav nalazi (Spremić, 2007).

Kako bi se uspješno revidirali informacijski sustavi potrebno je odrediti razinu kvalitete informacijskih sustava, odnosno odrediti u kojoj mjeri njegova realna funkcija odstupa od idealne, pri čemu manje odstupanje rezultira višom kvalitetom sustava (Spremić, 2017). Pri reviziji kvalitete sustava poželjno je primijeniti zakon minimuma kvalitete informacijskih sustava koji nalaže da je kvaliteta istih jednaka umnošku razina kvalitete svake pojedine komponente (Spremić, 2017). Drugim riječima, potrebno je održavati i ulagati u sve komponente istovremeno jer prisustvo jedne koja ne zadovoljava standarde rezultira nezadovoljavajućom kvalitetom cijeloga sustava (Spremić, 2017).

Proces revizije organizacija može se provoditi samostalno ili pomoću nezavisnog revizora, pri čemu je važno naglasiti kako samostalna metoda revizije može biti izrazito neobjektivna ako menadžeri odluče ne prijaviti nedostatke u dizajnu sustava (NIST, 2017).

Proces revizije sustava provodi se alatima i metodama poput (NIST, 2017):

- Automatiziranih alata koje dijelimo na aktivne alate čiji je zadatak lociranje slabosti u sustavu te pasivna testiranja koja analiziraju sustav i deduciraju postojanje problema u istima (NIST, 2017).
- Interne revizije kontrola gdje se donosi zaključak o efektivnosti informatičkih kontrola metodama nadgledanja, ispitivanja i testiranja (NIST, 2017).
- Planovima sigurnosti sustava koji revizorima pruža implementacijske detalje o sustavu nad kojima je moguće provesti reviziju (NIST, 2017).
- Penetracijskim testiranjem kojima se simulira napad na sustav. Napadi na sustav mogu se vršiti putem istih automatiziranih alata kojima se vrši revizija ili metodama socijalnog inženjeringa, kojim se informacije o sustavu prikupljaju od djelatnika organizacije (NIST, 2017).

Penetracijskim testiranjem simulira se *phishing* napad gdje revizori nastoje imitirati napadače i analizirati postotak djelatnika podložan ovakvim prijetnjama (Volkamer, Sasse, Boehm, 2020). Međutim provođenje takvih simulacijskih testiranja može predstavljati etički problem jer se nad djelatnicima vrši prijevara, što može imati negativan utjecaj na njihovo psihološko stanje a samim time i na kvalitetu poslovnog procesa (Resnik, Finn, 2017).

Izvještaj revizora informacijskih sustava predstavlja rezultat svih poduzetih analiza i revizija informacijskog sustava i na temelju njega revizor daje mišljenje o kvaliteti provedenih ključnih poslovnih ili informatičkih procesa (Spremić, 2007). Revizor po završetku izvještaja daje preporuku menadžmentu kao smjernicu kojom se potencijalno može unaprijediti poslovna praksa u određenom području poslovanja., a dužnost menadžmenta je detaljno pročitati izvještaj i sastaviti objašnjenje pogrešaka i nedostataka navedenih u revizorskom izvješću (Spremić, 2007).

Logičan je zaključak kako je revizija veoma bitan proces u funkcioniranju informacijskih sustava i da je od iznimne važnosti uključenost svih djelatnika u njen proces, posebice ako se simuliraju *phishing* napadi koji ciljaju ljudske slabosti. Posebnu pažnju treba obratiti na ažuriranost informacijskog sustava, što je dokazano u slučaju zrakoplovne kompanije ComAir. Zrakoplovnoj kompaniji ComAir su 2014. godine u vrijeme božićnih blagdana otkazali transakcijski rezervacijski sustavi jer nisu bili sposobni registrirati više od 32 000 odgođenih letova. Pad u sustavu uzrokovala je logička pogreška koja prije nije otkrivena jer kompanija nikada nije provodila reviziju nad zastarjelim sustavom. Posljedice ove ranjivosti i katastrofalne nepažnje menadžmenta kompanije iznosile su 40 milijuna dolara i velik broj tužbi ljudi koji su morale blagdane provesti kod kuće (Spremić, 2017).

3.4. Vrste napada na informacijske sustave

U suvremenom svijetu gotovo je nemoguće izbjeći kibernetičke rizike koji su uz konstantnu primjenu tehnologije u osobnom i poslovnom svijetu sveprisutni. Napadi na informacijske sustave se događaju kada pojedinci ili organizacije zanemaruju važnost sigurnosti

informacijskih sustava ne poštujući protokole zaštite podataka. Kada osnovni koraci digitalne predostrožnosti nisu poduzeti, napadi na sustave mogu imati ozbiljne posljedice za pojedince ali i organizacije.

Koncepti određenih vrsta prijetnji nastali su i prije razvoja samih informacijskih sustava. Ljudi se od davnina koriste socijalnim tehnikama manipuliranja ili prijevara kako bi se domogli tuđe imovine. U današnje vrijeme kada su ove tehnike kombinirane s digitalnim tehnologijama njihova se efektivnost značajno amplificira. Plodno tlo kibernetičkog kriminala postala su ilegalna tržišta gdje se mogu nabaviti napredni alati koji zlonamjernim pojedincima omogućuju planiranje i izvršavanje sofisticiranih vrsta kibernetičkih napada.

Neke od najčešćih vrsta informatičkih prijetnji povezanih sa *phishing* napadima su socijalni inženjering, zlćudni kod, *keyloggers*, i *man-in-the-middle* napadi (Whitman, Mattord, 2021).

Pojam socijalni inženjering odnosi se na vrstu prijetnje sigurnosti gdje kriminalci s izrazito razvijenim interpersonalnim vještinama navode pojedinca da otkrije osjetljive podatke o organizaciji u kojoj je zaposlen (Whitman, Mattord, 2021). Pojedinci iza napada prethodno prikupljaju podatke o organizaciji kao što su imena i razine autorizacije zaposlenika kako bi mogli oponašati tu osobu te zatim stupiti u kontakt sa zaposlenicima te iste organizacije. (Whitman, Mattord, 2021). Napadi pomoću socijalnog inženjeringa smatraju se najopasnijim oblicima kibernetičkih napada što potvrđuju i brojke. Procjenjuje se da je samo u SAD-u financijska šteta koja je uzrokovana socijalnim inženjeringom 2016. godine iznosila 121 milijardu dolara (Salahdine, Kaabouch, 2019). Postoji mnogo oblika kibernetičkih prijetnji temeljenih na socijalnom inženjeringu. *Phishing* napadi pripadaju domeni socijalnog inženjeringa jer koriste emocionalno manipuliranje kako bi prevarili korisnike da otkriju vrijedne informacije (Salahdine, Kaabouch, 2019).

Zlćudni kod je posebna vrsta programskog koda koji kriminalci koriste kako bi pristupili korisnikovom računalu ili ga na neki drugi način onesposobili. Oblici zlćudnog koda su (Whitman, Mattord, 2021):

- Virus - dio programskog koda koji se može replicirati i tako priključiti na neku od izvršnih datoteka. Pokretanjem tih izvršnih datoteka pokreće se i sam virus koji često može prouzročiti padove sustava ili onemogućiti korisniku korištenje računala (Gerić, Hutinski, 2007).
- Trojanski konj - vrsta zlćudnog koda koja se samostalno instalira na korisnikovo računalo i pritom izvodi neželjene aktivnosti, kao što su preuzimanje zlćudnih programa ili internetskih preglednika koje je kasnije gotovo nemoguće ukloniti (Gerić, Hutinski, 2007).
- Crv - vrsta zlćudnog koda koja nakon svoje instalacije dramatično usporava rad informacijskog sustava (Gerić, Hutinski, 2007).
- *Spyware* - podvrsta zlćudnog koda koji kriminalci koriste kako bi prikupili informacije o preferencijama pojedinaca koje se kasnije mogu koristiti pri socijalnom inženjeringu, a pojavljuje se kao web *bug* unutar HTML koda stranice ili kao kolačić koji prati aktivnost pojedinca na internetskom pregledniku (Whitman, Mattord, 2021).

- *Ransomware* je virus koji funkcionira po principu ucjene odnosno prilikom instalacije virusa na korisnikov sustav on se zaključava te mu je onemogućen daljnji rad. Tada se sustav može otključati ključem koji napadači razmjenjuju za financijska sredstva (Spremić, 2017).

Pegasus je primjer *spywarea* koji se širi metodom *spear phishing* napada. Sam program razvila je izraelska tvrtka NSO i ima potencijal zaraziti milijune pametnih telefona bez obzira na operacijske sustave koje koriste. Za njegovo preuzimanje nije potrebna ljudska interakcija, već je dovoljno posjedovati aplikaciju za komuniciranje poput WhatsAppa. Zvanjem na WhatsApp program se automatski instalira na sustav pametnog telefona i napadač može preuzeti bilo koju informaciju, fotografiju ili dokument koji je na sustavu skladišten (The Guardian, 2021).

Locky je vrsta *ransomware* napada koja započinje *phishing* poštom koja korisnika navodi na preuzimanje datoteke. Preuzimanje datoteke aktivira instaliranje zlćudnog koda koji korisniku automatski kriptira sve podatke. Na ekranu se zatim prikazuje tekst kojim se od korisnika traže novčana sredstva u zamjenu za ključ koji dekriptira njihove podatke. Pretpostavlja se da je zlćudni kod djelo ruske hakerske grupe Evil Corp. Najpoznatiji napad dogodio se u bolnici u Los Angelesu, kada je grupa uspješno izvela napad te oštetila bolnicu za 17 000 dolara. Napadi na bolnice postali su *modus operandi* ove zločinačke udruge jer su shvatili kako su metode skladištenja podataka i sigurnosne mjere informacijskog sustava u bolnicama zastarjele (NordVPN, 2023).

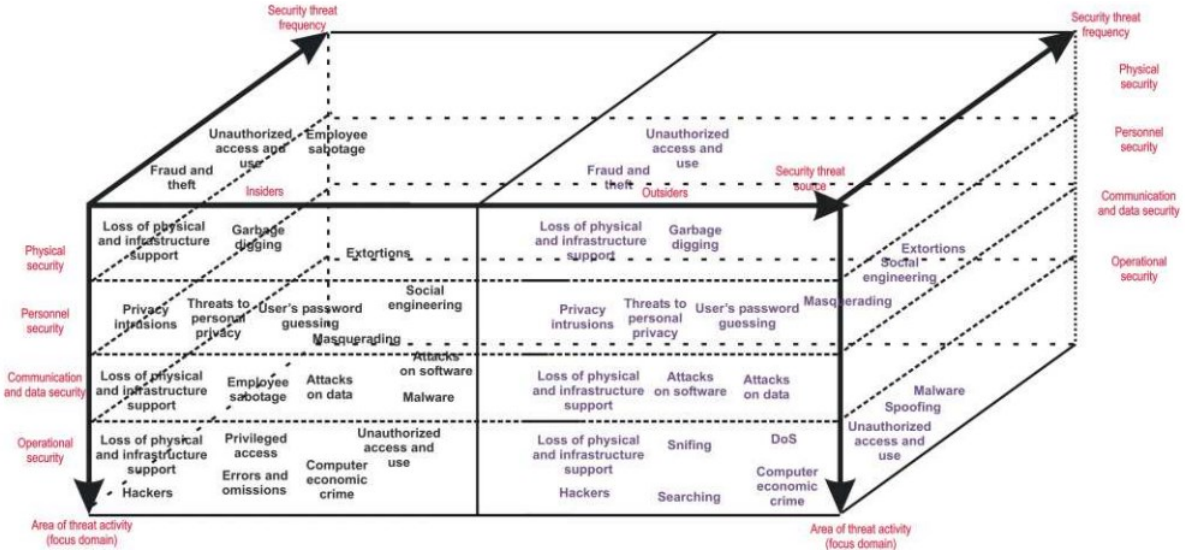
Keyloggers je naziv za programe koji prikupljaju uzorke pritisnutih tipki na tipkovnici i potom se analiziraju kako bi se došlo do lozinki poslovnih korisničkih računa ili PIN-ova za bankovne račune (Spremić, 2017). Prijenos ovakvih vrsta zlćudnih programa moguć je fizičkim putem pomoću uređaja nalik USB priključcima ili pomoću *phishing* pošte (Badra, Sawda, Hajjeh, 2010). Među najozloglašenijim primjerima *keyloggera* koji se šire *phishing* napadima zasigurno je *Snake Keylogger* koji u prilogu pošte najčešće ima PDF dokument. Zlćudni kod unutar dokumenta aktivira preuzimanje navedenog programa koji omogućuje napadačima analiziranje uzoraka pritisnutih tipki, krađu korisničkih podataka pohranjenih na sustavu te neautorizirano snimanje zaslona (Check Point, 2022).

Man-in-the-middle napadi pripadaju domeni *phishing* napada i odvijaju se u komunikacijskom kanalu na način da je napadač smješten između pošiljatelja i primatelja poruke te pritom prati ili „prisluškuje“ razmjenu informacija ili nastoji imitirati jednog od aktera u tom kanalu kako bi ukrao informacije (Mallik, 2018). Jedan od potencijalno najvećih propusta dogodio se kompaniji Lenovo koja je na svojim uređajima imala prethodno instaliran *software* zvan *Superfish. Superfish* je alat proizveden od istoimene kompanije pomoću kojeg je Lenovo stavljalo oglase na rezultate Googleove tražilice presretanjem šifriranog prometa, čime je Lenovo praktički izvelo *man-in-the-middle* napad. Kompanija Lenovo je *Superfish* koristila kao svojevrsni certifikat koji potvrđuje njegovu sigurnost i time je stekla pristup podacima s uređaja korisnika (Forbes, 2015).

Pojavom sve naprednijih i opasnijih kibernetičkih prijetnji organizacije su počele stvarati modele koje im omogućuju lakše praćenje i klasificiranje rizika. Klasifikacija je alat kojim organizacija nastoji utvrditi koje prijetnje štete kojim područjima sigurnosti čime se omogućuje

stvaranje plana obrane od potencijalnog napada (Jouini, Rabai, Aissa, 2014). Autori Gerić i Hutinski 2007. godine predlažu kubni klasifikacijski model čiji je prikaz na slici 6. i kojim se prijetnje klasificiraju prema frekvenciji, području te izvoru prijetnje.

Slika 5 - Prikaz kubnog klasifikacijskog modela



Izvor: Gerić, S., Hutinski Ž. (2007), Information system security threats classifications // Journal of information and organizational sciences, Journal of information and organizational sciences, 31(1), 51-61.

Temeljem ovog modela *phishing* napadi se, kao podvrsta socijalnog inženjeringa, mogu klasificirati kao visokofrekventne vanjske i unutarnje prijetnje kojima je područje aktivnosti sigurnost djelatnika u organizaciji (Gerić, Hutinski, 2007).

3.5. Propusti i ostale prijetnje sigurnosti informacijskih sustava

Propuste u sigurnosti informacijskih sustava najbolje možemo definirati kao situacije u kojima je došlo do nenamjerne ili namjerne ljudske pogreške (Gerić, Hutinski, 2007) ili kao nesuparničke prijetnje (NIST, 2017) kojima se smanjuje efikasnost informacijskog sustava. Propusti se mogu dogoditi u svakom trenutku poslovnog ciklusa sustava i mogu biti uzrokovani pogrešnim unosom podataka čime se narušava njihov integritet ili pogreškama u programiranju koje se popularno nazivaju „*bugovima*“ (NIST, 2017) i koje dovode do teških financijskih posljedica za organizaciju zato što je nužno provesti proces njihovog otklanjanja (Gerić, Hutinski, 2007). Osim financijskih troškova koje ti procesi zahtijevaju ovakva vrsta propusta, ako se često ponavlja, može trajno naštetiti reputaciji organizacije (Gerić, Hutinski, 2007). Do propusta u sigurnosti informacijskih sustava potencijalno može doći i na razini menadžmenta ako je isti uvjeren da organizacija ima neprobojan sigurnosni sustav, pri čemu se izlažu riziku podcjenjivanja propusta u sigurnosti istih (Choobineh, Dhillon, Grimaila, 2007). Zanemarivanjem sigurnosti kao strateškog prioriteta, logičan je zaključak kako organizacija

potencijalno premalo ulaže u obrazovanje zaposlenika i reviziju sustava, što može dovesti do većeg rizika od *phishing* napada i kibernetičkih prijetnji.

4. OBILJEŽJA *PHISHING* NAPADA

4.1. Definicija *phishing* napada

Phishing napad je vrsta kibernetičke prijetnje sigurnosti informacijskih sustava koja se temelji na vještinama socijalnog inženjeringa i krajnji joj je cilj krađa identiteta (Aleroud, Zhou, 2017). Napad se temelji na krivotvorenoj elektroničkoj pošti te kriminalac iza napada najčešće imitira važnu instituciju koja je prisutna u životu pojedinca, kao što je banka ili poslovna organizacija. Ova vrsta napada je veoma raširena u moderno vrijeme i još uvijek predstavlja velik problem sigurnosti informacijskih sustava (Aleroud, Zhou, 2017).

U moderno vrijeme *phishing* napadi su se proširili izvan upotrebe elektroničke pošte kao primarnog medija napada. Današnji *phishing* napadi mogu se vršiti oglasnim pločama, internetskim reklamama ili chat aplikacijama kako bi stupili u kontakt sa svojom ciljanom žrtvom. Najraširenija strategija *phishing* napada je kreiranje stranica koje su kopije originalnih web stranica poslovnih organizacija (IBM, 2004) Kao što je na početku rada naglašeno, *phishing* napadi primarno se izvode pomoću komunikacijskih informacijskih sustava (Bossetta, 2018).

Istraživanjem autora Butavicius et al. iz 2015. godine pokazano je kako vjerojatnost da će pojedinac otvoriti sadržaj pošte raste ako je to prethodno učinio netko od njegovih poznanika, kao što je kolega iz poslovne organizacije. Jedan od faktora uspješnosti *phishing* napada je i princip autoriteta koji nalaže da su ljudi osjetljivi na one *phishing* napade za koje misle da su poslani od strane osobe s višom razinom autorizacije. Provođenjem treninga protiv *phishing* napada ne utječe se značajno na imunost pojedinca na iste već se samo povećava njegova razina sumnjivosti što može rezultirati svrstavanjem legitimne pošte u kategoriju *phishing* napada (Harrison, Svetieva, 2016).

4.2. Proces *phishing* napada

4.2.1. Faze i sudionici procesa *phishing* napada

Phishing napadi, iako su naizgled jednostavni, izuzetno su sofisticirani i potrebno je mnogo planiranja i strategije kako bi bili uspješno izvedeni. Proces ili životni ciklus *phishing* napada može se podijeliti na 5 faza (Shaikh, Shabut, Hossain, 2016):

- Planiranje i priprema napada – početna faza napada u kojoj napadači određuju cilj napada koji može biti pojedinac, organizacija ili država. U ovoj fazi vrši se prikupljanje podataka i razmatraju se mediji kojima će se napad provesti (Shaikh, Shabut, Hossain, 2016).
- *Phishing* – provođenje napada slanjem lažne elektroničke pošte kojom se nastoji prikupiti podatke o žrtvama (Shaikh, Shabut, Hossain, 2016).

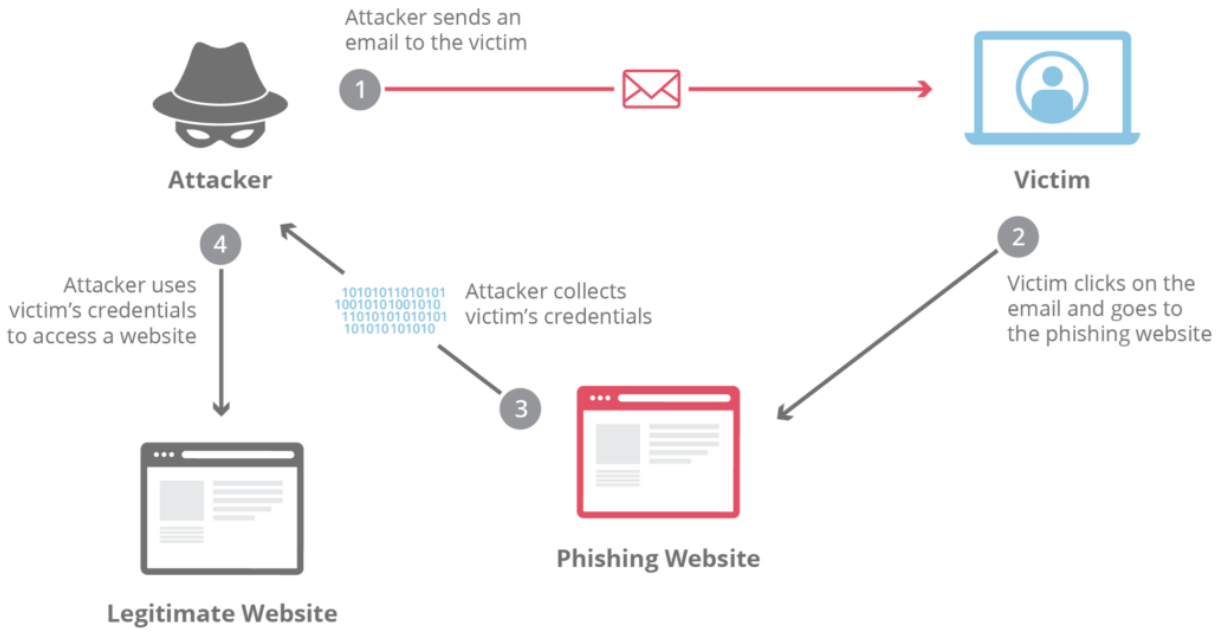
- Prodor u sustav – počinje klikom žrtve na link i preuzimanjem zloćudno sadržaja ili odlaskom na lažnu web stranicu, čime je napadačima osiguran pristup njenom sustavu i podacima (Shaikh, Shabut, Hossain, 2016).
- Prikupljanje podataka – napadač nastoji prikupiti što je više podataka moguće ili, ako se napad temeljio na zloćudnom kodu, nastoji preuzeti kontrolu nad sustavom (Shaikh, Shabut, Hossain, 2016).
- Eksfiltracija – posljednja faza u kojoj napadač briše sve dokaze o napadu i analizira koliko je trenutni napad bio uspješan kako bi se poboljšali modeli budućih napada (Shaikh, Shabut, Hossain, 2016).

Naziv za pojedinca koji vrši *phishing* napad je *phisher* i dijeli se na uloge pošiljatelja, čija je uloga u procesu distribucija elektroničke pošte korisnicima, sakupljača koji prikupljaju podatke kreiranjem lažnih web stranica te blagajnika koji prikupljene informacije koriste kako bi financijski oštetili žrtvu (Banu M., Banu S., 2013).

Proces *phishing* napada započinje slanjem elektroničke pošte od strane *phisher* pošiljatelja sa sadržajem koji emocionalno manipulira pojedinca stvaranjem osjećaja hitnosti ili panike, a kako bi ovo postigli, *phisher* pošiljatelji najčešće imitiraju poslovnu banku čije usluge koristi potencijalna žrtva kako bi otkrili njene korisničke podatke ili poziraju kao dobrotvorna organizacija koja prikuplja pomoć i traže novčanu uplatu (Hong, 2012).

Klikom na link u poruci pošiljatelja, pojedinac je najčešće preusmjeren na web stranicu koja nerijetko uvjerljivo imitira stranicu banke ili neke druge organizacije. Ove zloćudne stranice u prošlosti su bile loše kvalitete i bilo je jednostavnije uočiti da su nelegitimne, međutim danas se stranice stvaraju pomoću posebnih alata koji otežavaju takvu spoznaju. Ipak, određene jednostavne radnje, poput prelaska pokazateljem računalnog miša preko adrese, mogu otkriti radi li se o legitimnoj stranici ili ne. Primjer procesa *phishing* napada prikazan je slikom 6.

Slika 6 - Prikaz phishing napada



Izvor: https://cyberhoot.com/cybrary/phishing/

4.2.2. Komunikacijski mediji i ciljni uređaji *phishing* napada

Primarni komunikacijski mediji kojim se vrše *phishing* napadi su elektronička pošta i spam (IBM, 2004). Elektronička pošta mora izgledati i zvučati legitimno, međutim u današnje vrijeme gotovo je nemoguće utvrditi razliku između stvarnog i službenog e-maila te nije rijetkost da poruke budu egzaktne kopije već viđenog prethodno poslanog službenog dokumenta (IBM, 2004). Detekcija *phishing* elektroničke pošte vrši se različitim strukturalnim svojstvima poput HTML-a, URL-a baziranog na IP adresi, starošću imena domene, brojem domena, brojem poddomena, prisutnošću JavaScripta i brojem linkova (Basnet, Sung, Mukkamala, 2008).

Napadi koji se baziraju na HTML kodu koriste se kako bi se prikrila informacija o URL-u. Podatak o URL kodu je veoma bitan u internetskim preglednicima jer nam pokazuje stvarnu adresu stranice. Pomoću HTML koda je moguće ove informacije zamagliti korištenjem (IBM, 2004):

- iste boje slova URL koda i pozadine stranice (IBM, 2004);
- maskiranjem URL koda kodom zloćudne stranice (pri tome pomakom pokazatelja miša prema linku možemo vidjeti pravu adresu stranice) (IBM, 2004);
- korištenjem grafičkih alata kako bi izgledale kao tekstualna poruka ili URL (IBM, 2004);
- HTML-a koji je konfiguriran da izgleda kao običan e-mail (IBM, 2004).

Drugi najrasprostranjeniji komunikacijski medij je putem web stranica (IBM, 2004). Phishing napadi u poruci često sadrže link na uvjerljivu kopiju druge poznate web stanice i korisnici najčešće ne uoče detalje koji upućuju da se radi o prijevari (Varshney, Misra, Atrey, 2016). Jednostavna metoda kojom se može odrediti autentičnost web stranice je detaljan pregled karakteristika njene adrese kao što je duljina teksta jer se ona, zbog dodavanja ili brisanja slova i znakova, često razlikuje od duljine adrese legitimne stranice, kao što je prikazano na slici 8 (McGrath, Gupta, 2008). Cilj *phishera* je kreirati stranicu koja je uvjerljiva kopija legitimne stranice pa time kopiraju i dio URL koda, međutim nije moguće kreirati dvije stranice koje imaju potpuno identičnu adresu.

Slika 7 - Phishing/spoofing stranica sa lažnom domenom

Izvor: https://www.etechcomputing.com/5-online-scams-to-look-out-for-this-holiday-season/

IM (*instant messaging*) je internetska razmjena poruka između dva ili više korisnika u realnom vremenu putem mobilne aplikacije, društvene mreže ili unutar online video igre (Verheijen, 2013). Ovim komunikacijskim medijem *phishing* napadi se najčešće izvršavaju putem *hyperlinka* ili glasovnim porukama i pozivima tako da kriminalac imitira službenu osobu i ispituje korisnika o povjerljivim podacima (Aleroud, Zhou, 2017). *Instant messaging* je u današnje vrijeme jedan od najraširenijih medija komunikacije koji uključuje popularne aplikacije poput WhatsAppa. Brojke govore sve, WhatsApp je u četvrtom kvartalu 2019. godine zabilježio porast *phishing* napada od nevjerojatnih 13 476.6% (Alwanain, 2020).

Društvene mreže, zbog svoje popularnosti i povjerenja koje pružaju korisnicima, idealna su platforma za izvršavanje *phishing* napada gdje se vrše stvaranjem lažnih profila te kontaktiranjem žrtava ili stvaranjem kopija početnih stranica pri čemu korisnik, ne sluteći da se radi o lažnoj stranici, unosi svoje podatke kako bi se prijavio na račun i time daje pristup svojim informacijama (Aleroud, Zhou, 2017).

Ciljni uređaj napada je tehnološka oprema kojom se komunicira u virtualnom svijetu i dijeli se na osobna računala, pametne uređaje i druge komunikacijske uređaje. Planiranje napada za svaku vrstu uređaja značajno se razlikuje pa se time razlikuje i tehnologija koju napadač mora posjedovati kako bi uspješno izvršio napad (Aleroud, Zhou, 2017).

Razvojem pametnih telefona kao uređaja koji svojom tehnologijom konkuriraju modernim računalima *phisherima* je omogućilo lakše provođenje napada. Putem mobilnog uređaja teže je

prepoznati da se radi o ovakvoj vrsti napada zato što je na ekranu manjih dimenzija teško odrediti je li stranica koju je korisnik otvorio legitimna (Porter Felt, Wagner, 2011). Prema istraživanjima autora Aleroud i Zhou (2017), pokazano je kako najviše *phishing* napada uspijeva na pametnim telefonima jer većina korisnika uređaje drži konstantno upaljenima i u fizičkoj blizini čime se povećava vjerojatnost provođenja napada. Korištenje aplikacija putem pametnih telefona karakterizirano je nedostatkom indikatora identifikacije i samim time korisnik ne može znati nalazi li se na autentičnoj aplikaciji ili njenoj kopiji (Porter Felt, Wagner, 2011). Ovaj problem rješiv je odvajanjem dijela zaslona na pametnom telefonu na koji se može dodati adresna traka koja određuje autentičnost stranice no sama implementacija ovog rješenja ograničena je visokim postotkom ignoriranja indikatora od strane korisnika te prejednostavnim i lako krivotvorenim dizajnom polja za unos podataka (Porter Felt, Wagner, 2011).

Od svih komunikacijskih medija u praksi pokazalo se kako je kod elektroničke pošte najjednostavnije uočiti *phishing* prijetnje, što je i logično jer se u pošti često direktno traži od pojedinaca unos osobnih podataka što ih čini sumnjivima, dok se najmanje sumnjivim smatraju automatske poruke ili poruke u realnom vremenu, pogotovo ako su individualizirane (Jakkobson, 2007). Međutim, sposobnost uočavanja napada temelji se na digitalnoj pismenosti pojedinaca što je prikazano istraživanjem autora Alwanaina 2020. godine koje naglašava da su osobe starije životne dobi posebno ciljana skupina korisnika zbog viška financijskih sredstava i niže razine digitalne pismenosti.

4.3. Vrste *phishing* napada

Provođenje tradicionalnih *phishing* napada pokazalo se sve manje uspješnom metodom krađe podataka zbog njihove općenitosti, nepravilne upotrebe jezika i velikog broja gramatičkih pogrešaka. Sve većom razinom kvalitete edukacija i treninga, pogotovo u okvirima kulture sigurnosti organizacija, povećalo je svijest o njihovoj opasnosti. Posljedično tome, počele su se razvijati kompleksnije, zahtjevnije ali i samim time opasnije vrste *phishing* napada.

Spear phishing je vrsta *phishing* napada u kojem je sadržaj elektroničke pošte individualiziran i prilagođen pojedincu ili organizaciji kako bi se povećale vjerojatnosti ostvarenja napada (Bullée, Montoya, Junger, Hartel, 2017).

Spear phishing napadačima je koristan zbog (Bullée, Montoya, Junger, Hartel, 2017):

- Manjeg broja žrtava što smanjuje vjerojatnost od negativnih posljedica za napadače (Bullée, Montoya, Junger, Hartel, 2017).
- Veće vjerojatnosti uspješnog provođenja napada zbog posjedovanja detaljnih informacija kojima se individualizira poruka (Bullée, Montoya, Junger, Hartel, 2017).

Prema istraživanjima udruge CISCO, korištenje masovnih i generičkih *phishing* napada je u padu dok sve više raste upotreba *spear phishinga*. Iako je provođenje uspješnog *spear phishing* napada vremenski i financijski iscrpnije, dobici napadača su znatno veći (Parmar, 2012).

Uspješnost *spear phishing*a ovisi o kombinaciji više faktora, kao što su ljudska psihologija i široka upotreba pametnih uređaja (Parmar, 2012). Većina će ljudi kada primi poruku čiji je sadržaj prilagođen njima ili naizgled potječe od njihove banke ili poslovne organizacije kliknuti na taj sadržaj. Dodatni psihološki čimbenici koji utječu na prosudbu pojedinca su i užurbani način života zbog kojeg ljudi imaju manje vremena dobro promisliti prije donošenja odluke (Parmar, 2012).

Pametni telefoni dodatno su napadačima olakšali proces zbog činjenice da u moderno vrijeme ljudi imaju lakši pristup elektroničkoj pošti čime su potencijalno više izloženi ovakvoj vrsti napada jer često otvaraju poštu u žurbi i ne pročitaju do kraja poslane poruke pa tako ne mogu uočiti detalje koji pokazuju da se ne radi o legitimnoj poruci (Parmar, 2012).

Društvene mreže također su jedne od faktora sve veće uspješnosti *spear phishing* napada. U današnje vrijeme korisnici društvenih mreža često objavljuju privatne podatke iz života kao što su informacije o radnom mjestu. Iako poslodavci sve češće kontroliraju vrstu sadržaja koju zaposlenici mogu objavljivati na društvenim mrežama pogreške je ipak nemoguće u potpunosti izbjeći (Parmar, 2012).

Jedan od najvećih *spear phishing* napada dogodio se u Googleu. Kriminalci iza napada precizirali su osobu zaposlenu u Googleu koja je imala pristup vrijednim informacijama i počeli su kontinuirano pratiti njene online aktivnosti kroz kraći period. Pojedincu su poslali poruku s Facebook Messengera koja je izgledala kao da je bila poslana od strane njegovog prijatelja. Poruka je sadržavala web link koji je automatski preuzeo novu vrstu zloćudnog koda. Pojedinac je, nesvjestan da se radi o prevari jer je mislio da je poruku dobio od prijatelja, kliknuo na link i tako omogućio napadačima pristup Googleovim serverima (Parmar, 2012).

Drugi primjer napada koji se odvio putem društvenih mreža je slučaj kompanije RSA Security. Napadači su izolirali zaposlenika u odjelu ljudskih resursa nakon što su analizirali njegov LinkedIn profil. Elektronička pošta je filtrirana u spam, međutim zaposlenik ju je ručno otvorio jer je smatrao da je došlo do pogreške i time kriminalcima omogućio kontrolu nad podacima. Posljedice je osjetilo približno 100 milijuna korisnika. Ovaj napad prikazuje kolike posljedice može imati nepažnja pojedinaca u javnom dijeljenju informacija (Parmar, 2012).

Istraživanje autora Kwak et al. (2020) pokazuje kako većina djelatnika koji su žrtve *spear phishing* napada ne prijavljuju napade svojim poslodavcima. Postoji više faktora koji utječu na donošenje odluke o prijavi napada pri čemu autori Kwak et al. (2020) posebno ističu socijalno-kognitivne motivacijske procese i uvjerenja o kibernetičkim rizicima. Socijalno-kognitivno motivacijski procesi su psihološki faktori koji reguliraju ljudski motivacijski mehanizam u donošenju odluka i dijele se na spoznaje o samoučinkovitosti kod prijavljivanja *phishing* napada, utjecaj očekivanja posljedica prijavljivanja napada i utjecaj samoregulacije kod prijavljivanja napada (Kwak et al., 2020). Pokazano je da su pojedinci koji su mislili da će doživjeti ismijavanje od kolega zbog nepotrebnog prijavljivanja napada ili ako na neki drugi način nisu zadovoljavali navedene faktore u manjem broju prijavljivali napade (Kwak et al., 2020).

Big Five je test osobnosti koji karakter osobe opisuje s pet psiholoških osobina: neurotičnost, ekstrovertiranost, otvorenost, ugodnost i savjesnost (Halevi, Memon, Nov, 2015). Neurotičnost

je tendencija doživljavanju negativnih emocija kao što su krivnja, ljutnja ili strah; ekstrovertiranost je osobina koja karakterizira veću sklonost prema socijalnim interakcijama, dok osobina introvertiranosti podrazumijeva težnju samoći i socijaliziranju u manjim, ograničenim vremenskim intervalima; otvorenost podrazumijeva motivaciju za iskušenjem novih, neisprobanih doživljaja; ugodnost karakterizira ljude koji su skloni slaganju s drugima, primjerice na radnom mjestu, dok niska razina ugodnosti karakterizira manje empatične i više sebične te kompetitivne ljude dok visoka razina savjesnosti karakterizira ljude koji vrijede trud i organizaciju (Halevi, Memon, Nov, 2015).

Dodatna istraživanja autora Halevi, Memon i Nov (2015) pokazala su da na stupanj osjetljivosti na *phishing* napade utječe spol žrtve te njene karakterne osobine te je donesen zaključak kako su osobe ženskog spola s visokom razinom neurotičnosti i savjesnosti najviše izložene ovakvoj vrsti napada (Halevi, Memon, Nov, 2015). Odvojena analiza autora Sheng et al. (2010), koja se temeljila isključivo na stupnju edukacije protiv *phishing* napada pokazuje slične rezultate; u kontrolnoj grupi koja nije imala prethodnu edukaciju protiv phishing napada na link u poruci je kliknulo 54.7% od ukupnog broja žena i 49% od ukupnog broja muškaraca. Sukladno provedenim analizama može se reći kako postoje temeljne razlike u karakterima žena i muškaraca koje žene u prosjeku čine podložnijima tehnikama socijalnog inženjeringa a time i *phishing* napadima.

VoiP, voice phishing ili *vishing,* je telefonska prijevara kojoj je primarni medij komunikacije glasovna poruka na telefonskom uređaju i najčešće se sastoji od upozorenja da im je provaljeno u bankovni račun te da hitno moraju dostaviti svoje informacije (Kalaharsha, Mehtre, 2021).

Vishing napadi potencijalno mogu imati veći broj uspješno provedenih prijevara u usporedbi s ostalim vrstama *phishing* napada. Kombinacija faktora koja ovo omogućuje su (IBM, 2004):

- Veća razina povjerenja u telefonske i pametne uređaje nego u medije komunikacije poput Interneta (IBM, 2004).
- Veći postotak populacije koristi telefonske i mobilne pametne uređaje naspram elektroničke pošte (IBM, 2004).
- Starija populacija, koja je statistički osjetljivija na prevare, više koristi ovaj medij komunikacije (IBM, 2004).
- Utjecaj na vrijeme isporuke poruke može povećati šanse uspješnosti napada. Prevara telefonom je trenutačna, dok elektroničku poštu neki korisnici ne čitaju (IBM, 2004).
- Komunikacija telefonom u realnom vremenu omogućuje bolju upotrebu tehnika socijalnog inženjeringa (IBM, 2004).
- Ljudi su skloni vjerovati službenicima pozivnih centara koji lako mogu biti imitirani (IBM, 2004).

Više od 2.4. milijuna ljudi u SAD-u žrtve su kontinuiranih napada u kojima napadači koriste metode *vishinga* i predstavljaju se kao djelatnici IRS-a (američke porezne tvrtke) i pojedince obavještavaju da nisu platili porez. Žrtve napada nisu bile samo starije osobe i migranti, koji se smatraju lakšim metama, već širi dio populacije. Ovakve prijevare aktivne su i danas, te je 2018. godine zabilježeno čak 60% novih napada. Prevencija napada moguća je jednostavnim

informiranjem o načinu komuniciranja tvrtke pošto IRS nikada ne zove korisnike na telefonske uređaje već komunikaciju provodi isključivo poštom (idwatchdog).

Whaling je vrsta *phishing* napada koji koristi iste tehnike napada kao i *spear phishing*, no razlikuje se u odabiru žrtava. Žrtve *whaling* napada su bogati i moćni pojedinci od kojih bi napadači potencijalno mogli izvući najveće količine informacija (Bhavsar, Kadlak, Sharma, 2018). Proces *whaling* napada započinje prikupljanjem informacija o specifičnim osobama unutar organizacije koje su najčešće na višim pozicijama u hijerarhiji, kao što je direktor informatičkog odjela (IBM, 2004). Poznati slučaj *whaling* napada koji zorno prikazuje koliko je informacija i koraka potrebno za uspješan napad dogodio se američkoj tvornici igračaka Mattel. U travnju 2015. direktorica financija zaprimila je e-mail od novog direktora kompanije Cristophera Sinclaira da određenu sumu novaca prebaci u banku u kineskom gradu Wenzhou. Ne sumnjajući da se radi o prijevari jer je kompanija bilježila jak rast u Kini te takva vrsta transakcije ne bi bila neuobičajena u to vrijeme, odobrila je prijenos 3 milijuna dolara u navedenu banku. Sreća u nesreći bila je da je taj dan kada je transfer autoriziran u Kini bio državni praznik što je kriminalcima onemogućilo podizanje novaca i vraćen je u roku dva dana (CSO, 2016).

Smishing je skraćeni naziv za SMS *phishing* i odnosi se na vrstu *phishing* napada gdje je komunikacijski medij SMS poruka (Kalaharsha, Mehtre, 2021). SMS poruke najčešće sadrže obavijesti o osvajanju nagrada na igrama sreće i link stranice gdje bi korisnici trebali tu nagradu preuzeti, a zapravo vodi na lažnu stranicu gdje žrtva napadačima predaje osobne informacije (Kalaharsha, Mehtre, 2021). Početkom 2023. godine u gradu Sydneyju u Australiji uhićen je pojedinac koji je pomoću SMS *phishinga* ukrao 100 000 dolara od 39 ljudi. SMS je sadržavao poveznicu na stranice koje su zahtijevale od korisnika unos osobnih podataka. Pretpostavljeno je kako je napadač bio dio organizacije koja provodi phishing napade od 2018. godine (AFP, 2023).

Pojam *pharming* odnosi se na *phishing* napad bez korištenja faktora koji privlači žrtvu, a izvršavaju se promjenom lokacije datoteke na korisnikovom računalu ili iskorištavanjem slabosti na DNS serverskom softwareu (tehnika poznata kao DNS trovanje) (Kalaharsha, Mehtre, 2021). Poznati *pharming* napad dogodio se početkom 2007. godine i oštetio je najmanje 50 financijskih institucija od SAD-a do južnog Pacifika. Napad je bio izrazito dobro osmišljen i sastojao se od konstruiranja lažne web stranice za svaku pojedinačnu financijsku instituciju. Nakon otvaranja stranice, korisnicima bi se na računala automatski instaliralo 5 zasebnih datoteka sa servera u Rusiji. Ako bi nakon toga pojedinac ponovno išao posjetiti pravu web stranicu bio bi preusmjeren na lažnu stranicu financijske kompanije koja bi prikupljala njihove korisničke podatke i slala ih na server u Rusiji. Nakon unosa podataka korisnici su automatski vraćeni na legitimnu stranicu što je učinilo detektiranje napada gotovo nemogućim (ComputerWorld, 2007).

4.4. Zaštita i metode obrane od *phishing* napada

Pomno isplanirani i izvršeni phishing, *spear phishing* ili *whaling* napadi imaju potencijal značajno financijski oštetiti ili trajno onesposobiti organizaciju. Iako se od njih teško zaštititi jer ne napadaju direktno informacijske sustave već ljude, kombinacijom zaštitnih mehanizama moguće je smanjiti vjerojatnost uspješnog napada. Zaštita od *phishing* napada je proces koji se provodi prevencijom i detekcijom napada te edukacijom korisnika (Vayansky, Kumar, 2018).

Metode obrane od *phishing* napada tehnike su kojima je cilj uočiti i spriječiti *phishing* napade prije ili poslije procesa prikupljanja podataka korisnika (Aleroud, Zhou, 2017). Među najčešće korištenim metodama ističu se penetracijska testiranja u okviru revizije informacijskog sustava, *phishing blacklist,* dvofaktorska autentifikacija, anti-*phishing* alati te protokoli za prijenos zaštitno kodiranih podataka.

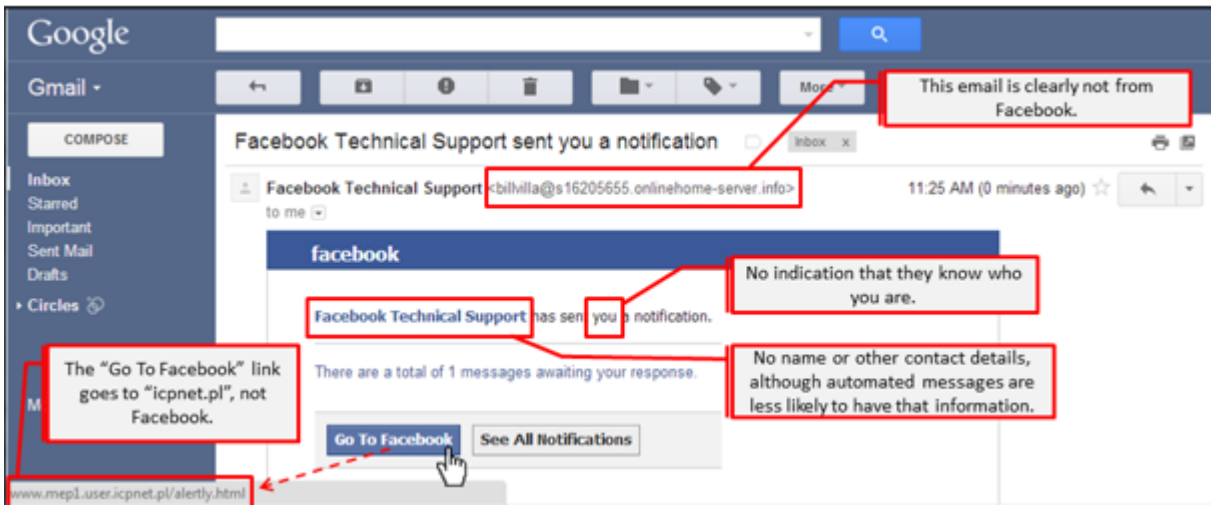
4.4.1. Prevencija, detekcija i edukacija

Prevencijom napada cilj je spriječiti napad prije nego što dođe do njegove realizacije, pri čemu se primarna prevencija napada vrši provjeravanjem autentičnosti adrese stranice i filtriranjem *phishing* poruka (Vayansky, Kumar, 2018). Posebni filtri za *phishing* napade koriste strojno učenje prilikom detekcije i automatski prepoznaju riječi koje se često koriste u *phishing* pošti te ostale karakteristike svojstvene takvim prijetnjama (Vayansky, Kumar, 2018).

SpamAssasin je primjer alata koji koristi naprednije metode filtriranja koje ne uključuju samo skeniranje teksta u sadržaju već i mjerenje omjera piksela teksta i slika s onima poslanima s legitimne pošte (Fette, Sadeh, Tomasic, 2006.).

Detekcija napada vrši se posebnim alatima kojima je cilj informirati korisnika na potencijalno prisustvo *phishing* sadržaja aktivnim ili pasivnim indikatorima, a njena uspješnost ovisi o pravilnoj uporabi takvih alata od strane korisnika (Vayansky, Kumar, 2018). Napad elektroničkom poštom moguće je detektirati temeljitim pregledom njenih karakteristika kao što je prikazano na slici 9. Na slici je prikazana pošta od navodne tehničke podrške Facebooka, a detaljnom analizom faktora kao što je email adresa lako se može zaključiti da ne odgovara legitimnoj adresi tog pošiljatelja.

Slika 8 - Detalji koji otkrivaju da se radi o phishing pošti



Izvor: https://blogs.otago.ac.nz/infosec/examples-of-phishing-emails/

Istraživanje autora Kirlapossa i Sasse (2011) naglašava najčešće pogreške ili uvjerenja korisnika pri korištenju online trgovine te potrebu za edukacijom u tom području. Zabrinjavajuća je informacija da većina korisnika web stranica za kupovinu ne primjećuje detalje koji upućuju da je stranica krivotvorena već se tijekom detekcije vode vlastitom intuicijom i logikom koja je često pogrešna. Istraživanje je tako pokazalo kako većina ispitanika vjeruje u autentičnost stranice ako ona posjeduje certifikate, reklame ili informacije o kompaniji koje je nažalost lako krivotvoriti. Autori ističu važnost provođenja edukacije u kontekstu potraživane usluge pri čemu je odličan primjer eBay koji je stvorio online zajednice koje pružaju kratke edukacije u detektiranju krivotvorenih proizvoda ili prijevara (Kirlapossa, Sasse, 2011).

Cilj edukacije korisnika je osvijestiti pojedinca o karakteristikama *phishing* napada., međutim one mogu biti nedovoljne ako obuhvaćaju samo opće informacije o takvim napadima i ako nisu konstantno ažurirane (Vayansky, Kumar, 2018).

Jedna od metoda edukacije korisnika o rizicima *phishinga* je gamifikacija, proces kojim se korisnika educira kroz interaktivnu igru, ili simulacijom napada u organizaciji. Anti-*Phishing* Phil je primjer interaktivne web igre kojoj je cilj educirati korisnike o *phishingu*. Istraživanja autora Alsharnouby, Alaca i Chiasson (2015) su pokazala da su korisnici koji su redovito igrali igru bolje detektirali znakove koji su ukazivali na *phishing* poštu od onih koji igru nisu igrali.

4.4.2. Penetracijska testiranja u okviru revizije informacijskog sustava

Penetracijska testiranja u okviru *phishing* napada provode se simuliranjem istih kako bi se otkrile i dokumentirale slabosti informacijskih sustava (Shavran, Neha, Pawan, 2014). Iako je primarni cilj većine penetracijskih testiranja otkriti ranjivosti tehničkih dijelova sustava poput vatrozida ili usmjernika, cilj *phishing* napada su djelatnici organizacije i revizori sustava tijekom testiranja moraju primijeniti metode socijalnog inženjeringa kako bi se procijenila razina sigurnosne osviještenosti u organizaciji (Shavran, Neha, Pawan, 2014).

Provođenje penetracijskih testiranja na pravilan način može pružiti organizaciji podlogu kojom će stvoriti sigurnosni okvir i tako pružiti što bolju edukaciju djelatnicima, međutim ovakvi testovi nisu savršeni. Vremenski okvir u kojem se provode penetracijska testiranja često nije adekvatan kako bi se obuhvatila sigurnost svih aspekata poslovanja što nije slučaj sa stvarnim napadima gdje *phisheri* imaju više vremena detaljno procijeniti slabosti u sustavu (Shavran, Neha, Pawan, 2014).

Kao što je u ranijim poglavljima naglašeno, problem provođenja penetracijskih testiranja može predstavljati etički problem kada se tijekom testiranja revizori koriste metodama socijalnog inženjeringa jer se djelatnici mogu osjećati prevareno što znatno utječe na njihov rad. Komuniciranje s djelatnicima i objašnjavanje ciljeva može pozitivno utjecati na stav zaposlenika o testiranjima no sama spoznaja da se u organizaciji provode takva testiranja može značajno smanjiti njihovu efektivnost jer će zaposlenici biti više pripravni i neće biti elementa iznenađenja, čime se stvara kontradiktorna situacija (Shavran. Neha, Pawan, 2014).

4.4.3. *Blacklist*

Jedan od načina na koji se može provjeriti autentičnost stranice, ako pojedinac sam ne može prepoznati radi li se o legitimnoj adresi, je putem *blacklista*.

Blacklist najbolje može biti definiran kao kontrolna lista koja se sastoji od svih elemenata prepoznatih kao prijevarama, kao što su *phishing* stranice ili email adrese sa kojih dolazi spam pošta (Bell, Komisarczuk, 2020). Primjena *blacklista* efektivna je pri blokiranju phishing pošte, međutim pruža ograničenu zaštitu od phishing stranica zbog nemogućnosti blokiranja cijelih domena (Sheng et al. 2009). Efektivnost funkcije *blacklista* ovisi o njenoj sveobuhvatnosti, količini grešaka i brzini slanja obavijesti (Whittaker, Ryner, Nazif, 2010). Ako funkcija nije sveobuhvatna ne može zaštiti sve svoje korisnike dok prisutnost grešaka potencijalno može dovesti do situacije da korisnicima šalje preveliki broj nepotrebnih upozorenja koja će korisnici vjerojatno ignorirati. Brzina slanja obavijesti možda je najbitniji faktor efektivnosti funkcije jer od iznimne je važnosti da korisnik primi poruku o nelegitimnosti stranice prije nego ju posjeti (Whittaker, Ryner, Nazif, 2010).

Blacklist je moguće onesposobiti raznim tehnikama kao što je maskiranje zloćudnog sadržaja stranice legitimnim kako bi se izbjegla detekcija te linkovima za preusmjeravanje koji mijenjaju

originalne linkove svrstane u *blackliste* ali usmjeravaju na iste zloćudne stranice (Oest, Safaei, Zhang, 2020).

4.4.4. Dvofaktorska autentifikacija

Dvofaktorska autentifikacija je metoda obrane od kibernetičkih napada koja se temelji na identifikaciji korisnika pomoću dva podatka. Faktori dvofaktorske autentifikacije su (Ramzan, 2010):

- Nešto što posjedujemo, kao što je osobna iskaznica ili ključ (Ballad, Banks, 2011).
- Biometrijska identifikacija koja se vrši biološkim karakteristikama (Ballad, Banks, 2011).
- Nešto što znamo, kao što je lozinka ili neka druga informacija koja nas može identificirati (Ballad, Banks, 2011).

Autentifikacija informacijom poput lozinke dominantan je faktor dvofaktorske autentifikacije dok je drugi najčešće korišteni faktor nešto što posjedujemo (Ramzan, 2010). Token je primjer uređaja koji korisniku generira nasumičan kod koji se sastoji od četiri broja. Medij slanja koda ne mora biti zaseban token uređaj već server može kodove slati i na mobilne uređaje SMS porukom, a tim kodom korisnik dokazuje da je početna lozinka njegova i da posjeduje telefon koji je primatelj poslanog koda (Ramzan, 2010).

Biometrijska identifikacija dijeli se na dva podtipa: fiziološki i bihevioralni (Lian, Kanellopoulos, Ruffo, 2008). Fiziološka biometrijska identifikacija vrši se fizičkim obilježjima poput otiska prsta, skeniranja lica ili šarenice oka, dok se bihevioralna identifikacija vrši potpisom ili glasovnim prepoznavanjem (Lian, Kanellopoulos, Ruffo, 2008). Biometrijska identifikacija podložna je pogreškama koje se kategoriziraju kao postoci pogrešnih odbijanja (eng. *false rejection rate)* i postoci pogrešnih odobravanja (eng. *false acceptance rate*). Zbog toga biometrijska identifikacija jednim faktorom često nije dovoljna za potpunu zaštitu informacija već je potrebno kombinirati više metoda biometrije ili koristiti više faktora autentifikacije (Lian, Kanellopoulos, Ruffo, 2008).

Nedostatak dvofaktorske autentifikacije je da ne može spriječiti krađu podataka uživo ako unutar djelovanja privremenog koda korisnik nekome svjesno ili nesvjesno otkrije povjerljivu informaciju čime se kriminalcu otvara vremenski okvir unutar kojeg može uspješno napasti sustav, međutim dvofaktorska autentifikacija je i tada efektivna u osiguravanja sustava ako je za napad potrebno više vremena od predviđenog (Ramzan, 2010).

4.4.5. Anti-*phishing* alati

Anti-*phishing* alati su ekstenzije internetskih preglednika koje pružaju korisniku informacije o legitimnosti stranice (Ramzan, 2010). Metode kojima se ekstenzije koriste su provjeravanje je li URL stranice na crnoj listi i provjeravanje vremena nastanka domene uz pretpostavku da domene s novijim datumom nastanka imaju veću vjerojatnost da su nelegitimne (Ramzan, 2010).

Anti-*phishing* alate dijelimo na tri podtipa (Ramzan, 2010).

- Alate koji koriste neutralne informacije i prikazuju ime domene, ime domaćina i datum registracije (Ramzan, 2010).
- SSL verifikacijske alate koji prikazuju SSL potvrdne informacije za sigurne stranice (Ramzan, 2010).
- Alate koji se koriste sistemskim odlukama i prikazuju koliko je stranica legitimna (Ramzan, 2010).

Prema istraživanju autora Ramzana (2010), najvišu razinu zaštite pružaju alati koji se koriste sistemskim odlukama gdje je postotak korisnika koju su prevareni internetskom stranicom 33% dok su se najlošijom opcijom pokazali alati koji koriste neutralne informacije, gdje je postotak prevarenih korisnika 45%. Temeljni problem ovakvih alata je što korisnici u većini slučajeva nisu u stanju adekvatno interpretirati informacije koje im alati prenose (Ramzan, 2010).

Anti-*phishing* alati paralelno su u kontinuiranom razvoju s alatima koje koriste kriminalci što ih ponekad čini neefektivnima u zaštiti informacijskog sustava, posebice kod korisnika koji nisu svjesni *phishing* prijetnji i nemaju instalirane takve alate (Downs, Holbrook, Cranor, 2006).

Inkrementalna poboljšanja alata daju prednost kriminalcima zato što je jednostavnije analizirati nedostatke u sigurnosti nego konstantno nadograđivati alate (Parno, Kuo, Perrig, 2005). Može se zaključiti da je za razvijanje boljih alata za zaštitu od *phishinga* potrebno naći fundamentalno rješenje problema.

Programeri koji se bave razvojem takvi alata trebaju obratiti pozornost na ponašanje pojedinaca tijekom primljenih obavijesti od strane korištenih alata jer loš dizajn ili situacija da korisnik ne razumije rizik dovodi do situacije da poruka upozorenja najčešće bude ignorirana (Downs, Holbrook, Cranor, 2007).

Anti-*phishing* alati nisu savršeni jer nelegitimne stranice mogu klasificirati kao prijetnje a zloćudne stranice kao sigurne i potrebno je korisnike educirati o prepoznavanju ostalih znakova koji ukazuju da se radi o prijetnji kako bi sami mogli odrediti u kojim je situacijama potrebno uključiti ili isključiti zaštitu koju isti pružaju (Downs, Holbrook, Cranor, 2007).

4.4.6. Protokoli za prijenos zaštitno kodiranih podataka

Primjena protokola za prijenos zaštitno kodiranih podataka, ili skraćeno SSL protokola, u velikoj mjeri ovisi o korištenju javnog ključa (Ramzan, 2010). Javni ključ je tehnika korištena u kriptografiji koja omogućuje transakcije između stranaka koje se nisu susrele u stvarnom svijetu i njegovo se funkcioniranje temelji na mehanizmu kojim se javni ključ veže uz identitet korisnika (Ramzan, 2010). Digitalni certifikati najčešće su korišteni takvi mehanizmi, a sastoje se od dokumenta digitalno potpisanog od strane tijela za izdavanje certifikata i sadrže javni ključ te informacije koje se uz javni ključ žele vezati, kao što su ime osobe ili naziv domene (Ramzan, 2010).

Primarna svrha SSL protokola je zaštita podataka dok su u procesu slanja, pa samim time pružaju i zaštitu od *phishing* napada. Većina *phishing* stranica ne koristi SSL protokole i korisnikova je dužnost uočiti koriste li određene stranice SSL protokole ili ne (Ramzan, 2010).

Zaštita podataka SSL protokolima u praksi se smatra slabom zaštitom sigurnosti podataka, a razlozi tomu su da većina korisnika nije svjesna koriste li se na stranici ti protokoli ili ne (Dhamija, Tygar, Hearst, 2006). Prisutnost SSL protokola prikazuje se simbolom lokota na desnoj strani adresne trake i korisnik ju teško uočava ako detaljno ne pregleda stranicu (Dhamija, Tygar, Hearst, 2006). Neke *phishing* stranice nastoje prevariti korisnike korištenjem lažne ikone lokota u adresnoj traci, međutim lako je uočiti kada se koristi lažna ikona lokota jer se autentična ikona uvijek nalazi desno od adrese na adresnoj traci dok pozicija lokota na drugoj lokaciji u adresnoj traci (najčešće lijevo od adrese) signalizira da se radi o *phishing* stranici (Ramzan, 2010).

Međutim, ništa ne sprječava *phishera* da kupi certifikat za domenu svoje stranice, zbog čega su neke organizacije za izdavanje certifikata počela primjenjivati dodatne sigurnosne protokole prilikom izdavanja digitalnih certifikata (Ramzan, 2010). Kupovina certifikata najčešće se odvija lažiranjem identiteta kompanije te preuzimanja certifikata od organizacija zaduženih za njihovo izdavanje (Nagunwa, 2014).

Dodatnim sigurnosnim protokolima detaljnije se utvrđuje autentičnost stranice, pri čemu se izdaju odvojeni, posebni certifikati koji jamče višu razinu autentičnosti ali i sami pate od istih nedostataka kao i njihove manje sigurne varijante (Ramzan, 2010). Implementacija SSL protokola predstavlja problem i legitimnim financijskim institucijama i većina *phishera* može zaobići zaštite koje ti protokoli pružaju (Ramzan, 2010).

Istraživanja autora Alsharnouby et al. iz 2015. godine pokazuju kako je od svih internetskih preglednika SSL indikatore najlakše identificirati na Google Chromeu zbog korištenja većeg fonta na adresnoj traci i širom uporabom boja prilikom njihova lociranja.

5. ANALIZA STUDIJA SLUČAJEVA

5.1. Analiza prve studije slučaja: *Phishing* napad u Amsterdamu

Prva analiza slučaja odnosi se na *phishing* napad u Amsterdamu 2013. godine koji je organizirala kriminalna organizacija i nad kojim je provedena policijska istraga. Provedena istraga daje uvid u kompleksnost mreže i detaljnost plana te proces njegove provedbe (Leukfeldt, 2014).

Kriminalna mreža odgovorna za napade prethodno je bila odgovorna za niz zločina u domeni krađe osobnih ili bankovnih podataka, pa čak i provala u poslovne zgrade. Napad se sastojao od tri faze: faze pripreme, faze krađe i faze prijenosa sredstava na račun. Cilj, odnosno žrtve napada, bili su korisnici dvije banke, od kojih je svaka imala zaseban sustav autentifikacije (Leukfeldt, 2014).

Proces *phishing* napada započinjao je slanjem elektroničke pošte koja je uvjerljivo kopirala službenu poštu iz banaka. U privitku poruke nalazila se forma i tražila je od korisnika da u nju unese svoje osobne informacije. Tim putem kriminalci su se domogli lozinki korisnika kao i brojeva njihovih kartica. Jedinu informaciju koju nisu mogli prikupiti je jedinstveni transakcijski broj koji su, kako korisnici ne bi posumnjali da se radi o prevari, prikupljeni telefonskim razgovorima. Bez jedinstvenog transakcijskog broja nije bilo moguće realizirati prijenos novčanih sredstava (Leukfeldt, 2014).

Kako bi kriminalci osigurali da pozivi budu što uvjerljiviji, unajmili su osobe koje su prethodno bile djelatnici pozivnih centara ili banaka. Kako je većina tih pojedinaca bila nezadovoljna otkazom i načinom kojim su tretirani na bivšem radnom mjestu, kriminalcima je bilo lakše izmanipulirati ih te potom regrutirati. U većini slučajeva, žrtve su izjavile kako su osobe s kojima su pričale zvučale vrlo uvjerljivo, te su čak davale identifikacijske brojeve koji su potvrđivali da je osoba s kojom pričaju stvarno djelatnik njihove banke (Leukfeldt, 2014).

Jedan od regrutiranih članova bio je djelatnik poštanske službe koji je tijekom radnog vremena krao kartice korisnika koje su im se slale putem pošte. Kako bi to napravio, djelatnici organizacije primijenili su poštanski broj pošiljke na područje koje je pokrivao navedeni radnik što mu je omogućilo pristup tim paketima (Leukfeldt, 2014).

Kako se novčani transferi ne bi mogli lako pratiti, kriminalci su za prijenos novčanih sredstava koristili financijske mule. Financijske mule su sudionici napada koji djeluju kao vanjski suradnici kriminalne organizacije te je njihova uloga u procesu napada prekinuti digitalni trag novca otvaranjem računa na koji će ukradena sredstva biti prebačena. Sredstva prebačena na te račune zatim bivaju podignuta s istih već unutar nekoliko trenutaka od realizacije prijenosa (Leukfeldt, 2014).

Nakon provedene istrage nije bilo moguće utvrditi kako su se prvotno upoznali organizatori međutim utvrđeno je kako se radilo o osobama iste etničke pozadine. Svih osam članova imalo je pozadinu u organiziranim kriminalnim aktivnostima (Leukfeldt, 2014).

Regrutirani članovi organizacije bavili su se prikupljanjem informacija. Jedna je osoba pozirala kao službenik banke i svojim je interpersonalnim vještinama navodila korisnike da otkriju svoj jedinstveni transakcijski broj. Pozivatelj je u većini slučajeva navodio da postoje kvarovi na internetskim računima pojedinaca i da korisnik mora poslati svoje informacije kako bi se uklonio. Istrage su pretpostavljale kako je osoba koja je provodila ove pozive, koji su nerijetko trajali i 30 minuta, bila bivša zaposlenica pozivnog centra (Leukfeldt, 2014).

U napad je bilo uključeno osam zaposlenika banaka, od kojih je sedam uhićeno i ispitano. Njihov zadatak bio je pružanje informacija organizatorima o informacijskim sustavima i povjerljivim informacijama banaka u kojima su bili zaposleni, kao što su adrese korisnika i podaci o prijenosima novaca s računa, te su također mogli promijeniti iznose limita na korisničkim računima što je omogućilo podizanje veće količine novčanih sredstava i korištenje manjeg broja financijskih mula. Zajednička karakteristika svih zaposlenika koji su radili za organizaciju je bila da nisu dugo bili zaposlenici banaka i nisu svojim poslodavcima bili veoma odani. Proces njihove regrutacije proveden je na ulici te im je kao za nagradu bila obećana financijska isplata (Leukfeldt, 2014).

Za otvaranje privremenih računa na koje su sredstva prebačena regrutirane su financijske mule koje su organizatorima dale svoje kartice. Putem tih kartica, organizatori su otvarali nove, privremene račune na koje bi se prebacivala ukradena novčana sredstva. Tijekom istrage većina regrutiranih mula je izjavila da su kartice izgubili kako ih se ne bi povezalo sa napadom, no utvrđeno je da je nekolicina pojedinaca bilo aktivno uključena u procesu regrutacije novih mula. Bili su svjesni da je njihova uloga u napadu ilegalna i da im je za njihove usluge obećan dio ukradenih novčanih sredstava kao kompenzacija, no i sami su bili žrtve prevare jer im organizacija nije pružila obećanu zaštitu niti isplatila sredstva (Leukfeldt, 2014).

Jedan od faktora koji analizirani *phishing* napad čini efikasnim je korištenje tehnika socijalnog inženjeringa koje se ne mogu prevenirati korištenjem tehnologije. Bitnom fazom napada, izuzev samih lažnih elektroničkih pošiljki, smatraju se telefonski razgovori između korisnika i pozivatelja. Kako bi se prevenirale prevare ovakve prirode, potrebno je ulagati u kampanje sigurnosti kojima se podiže svijest građana o opasnostima davanja povjerljivih informacija nepoznatim pozivateljima, čak i ako se predstavljaju kao zaposlenici banke i imaju uvjerljive priče (Leukfeldt, 2014).

Kod provođenja istrage kod ovakvih vrsta napada važno analizirati prethodne aktivnosti organizacije, pogotovo u slučaju *phishing* napada ako se prethodno znalo da su organizacije vršile takvu vrstu napada. Provjerom znakova koje bi mogli istražiteljima dati do znanja da se radi *phishing* napadačima moguće je poduzeti preventivne mjere koje bi u korijenu spriječile takve napade prije nego što dođe do financijske ili druge vrste štete (Leukfeldt, 2014).

Banke ili druge financijske institucije same mogu provesti mjere prevencije *phishing* ili drugih vrsti kibernetičkih napada, posebice u slučajevima kada zaposlenici tih banaka budu uključeni u organizaciju koja je napad provela. Prvi korak je otežati proces pristupa povjerljivim informacijama unutar organizacije dodjelom različitih razina autorizacije. Implementiranjem automatskog sustava pretraživanja mogu se provjeriti nelogične promjene na računima

korisnika i samim time mogu se otkriti zaposlenici koji vrše takve promjene u sustavu (Leukfeldt, 2014).

Iako su napadi bili uspješno izvršeni, činjenica da su organizatori otprije poznati istražiteljima kao grupa koja se bavila ilegalnim aktivnostima potaknulo ih je na poduzimanje koraka kako bi ih se uhvatilo u prijevari. Istražitelji su prisluškivanjem njihovih mobilnih uređaja i ostalim metodama uspjeli dokazati kriminalne aktivnosti organizacije te su kriminalci privedeni i protiv njih je podignuta optužnica (Leukfeldt, 2014).

5.2. Analiza druge studije slučaja: Simulacija *phishing* napada u bolnici

Druga studija slučaja analizira simulirane *phishing* napade u talijanskoj bolnici sa 6000 zaposlenika u vrijeme pandemije COVID-a 19. Ukupno su izvedene tri kampanje simulacijskih napada i svaka se razlikovala po količini poslane elektroničke pošte i njenom sadržaju. Osoblje koje je sudjelovalo u simulaciji napada bilo je prethodno zaposleno u bolnici dulji period dok su novi zaposlenici isključeni iz procesa simulacije. Sve poslane lažne elektroničke pošte poslane su od istog pošiljatelja čija se domena razlikovala od uobičajene domene adrese bolnice (Rizzoni et al., 2022).

Prva simulacija sastojala se od dvije vrste napada: generičkog *phishing* napada i prilagođenog *phishing* napada. Općeniti *phishing* napad sadržavao je obavijest da je Microsoftova pošiljka prebačena u karantenu i da je potrebno kliknuti na link u prilogu kako bi se dobila lozinka pomoću koje će se dokument izvaditi iz karantene. Prilikom napada umjesto teksta se koristila tekstualna grafička slika koja je sadržavala velik broj gramatičkih grešaka. Prilagođena *phishing* poruka sastojala se od upozorenja da je u roku od dva dana potrebno odraditi obavezan online tečaj iz područja sigurnosti informacijskih sustava te je u prilogu bio priložen link na koji je trebalo kliknuti kako bi tečaj započeo. Prilagođena verzija napada iskoristila je situaciju u bolnici u vrijeme kada je većina zaposlenika prolazila online tečajeve informacijske sigurnosti i pomoću nje je bilo moguće zaključiti uočavaju li zaposlenici detaljnije greške koje upućuju na napad ako im je prezentirana poruka koja naglašava hitnost i obavezu (Rizzoni et al., 2022).

Druga simulacija sastojala se od jednog prilagođenog *phishing* napada, a poruka je određenm postotku zaposlenika objavila da će se prije božićnih blagdana isplaćivati novčani bonus. Poruka je ovoga puta bila gramatički ispravno napisana (Rizzoni et al., 2022).

Treća simulacija sastojala se od kombiniranog napada, a u poruci se zaposlenicima nudila dropbox nadogradnja kao zahvala za posao obavljen tijekom COVID krize. I u ovom slučaju tekst je zamijenjen grafičkom slikom (Rizzoni et al., 2022).

Proces provođenja napada izvršavala je konzultantska kompanija koja je svojim prethodnim iskustvom utvrdila da je izolirane napade najbolje izvoditi u intervalima od četiri mjeseca. Konzultantska je kompanija, u suradnji s internim sigurnosnim timom, donijela odluku da je za simulaciju napada najbolja kombinacija standardnih, općih poruka i prilagođenih poruka. Sve poruke sadržavala su linkove čija je lokacija imala isti HTML, a stranica je sadržavala obavijest kako se radi o *phishing* napadu te je zaposlenicima pružala informacije kako se zaštititi od

daljnjih napada, kao što je izbjegavanje klika na nepoznate linkove ili provjeravanje stvarne adrese putem pokazatelja na mišu. U procesu analize rezultata simulacije izbjegavalo se imenovanje zaposlenika koji su otvorili link kako bi se zaštitila njihova privatnost i mogući utjecaj na radni performans, koji je već bio na nižoj razini od idealne zbog duljeg stresnog perioda epidemije (Rizzoni et al., 2022).

Temeljem provedenih simulacijskih napada organizatori su došlo do zaključka kako su najveće prijetnje sigurnosti sustava upravo prilagođeni *phishing* napadi. Broj klikova na linkove standardne *phishing* poruke iznosio je 7% od ukupnog broja poslanih poruka dok je postotak klikova kod prilagođenih *phishing* poruka iznosio 55% od ukupnog broja poslanih poruka, što dovodi do zaključka kako davanje konteksta poruci značajno utječe na vjerojatnost otvaranja sadržaja poruke. Kroz cijelu kampanju sukcesivno je smanjen broj klikova na sadržaj poruka, što se može pripisati većoj razini opreza temeljem prethodnih simulacija. Zanimljiva je činjenica da iako je značajno smanjen broj klikova na sadržaj standardnih poruka zbog povećane svijesti o provođenju simulacija napada tijekom tri kampanje, postotak broja klikova na linkove kod prilagođenih simulacijskih napada nije se značajno smanjio. Uobičajeni mehanizmi zaštite poput filtriranja poruka u otpad ili spam nisu pružali značajnu zaštitu jer je i dalje velik broj pošte ručno izvađen iz otpada (Rizzoni et al., 2022).

Vremenski period u kojem su se provodile simulacije značajno je utjecao na rezultate istih. Tijekom simulacija zaposlenici bolnice su bili pod povećanim razinama stresa zbog epidemije COVID-a 19 što je u velikoj mjeri utjecalo na njihovu sposobnost rasuđivanja ali i retencije informacija, pošto su uz trening sigurnosti svi zaposlenici bili dužni prolaziti dodatne tečajeve o suzbijanju širenja bolesti (Rizzoni et al., 2022).

Provođenje simulacijskih napada u bolnicama pokazalo se kao težak zadatak za administraciju iz više sociooloških i psiholoških faktora. Određene provedene simulacije, kao što je lažna obavijest da će zaposlenici dobiti božićni bonus, mogu imati značajan negativan utjecaj na zadovoljstvo na radnom mjestu djelatnika i moraju biti odrađene u sukladnosti sa zakonom o radu, što može biti problem kada broj djelatnika koji je svjestan provođenja simulacija radi efektivnosti mora biti minimalan. U provedenim simulacijama nije bila uključena administracija bolnice što se smatra lošim potezom jer je velikom broju *phishing* metoda, kao što je *whaling,* upravo cilj menadžment institucije iz kojeg se može izvući najviše povjerljivih informacija (Rizzoni et al., 2022).

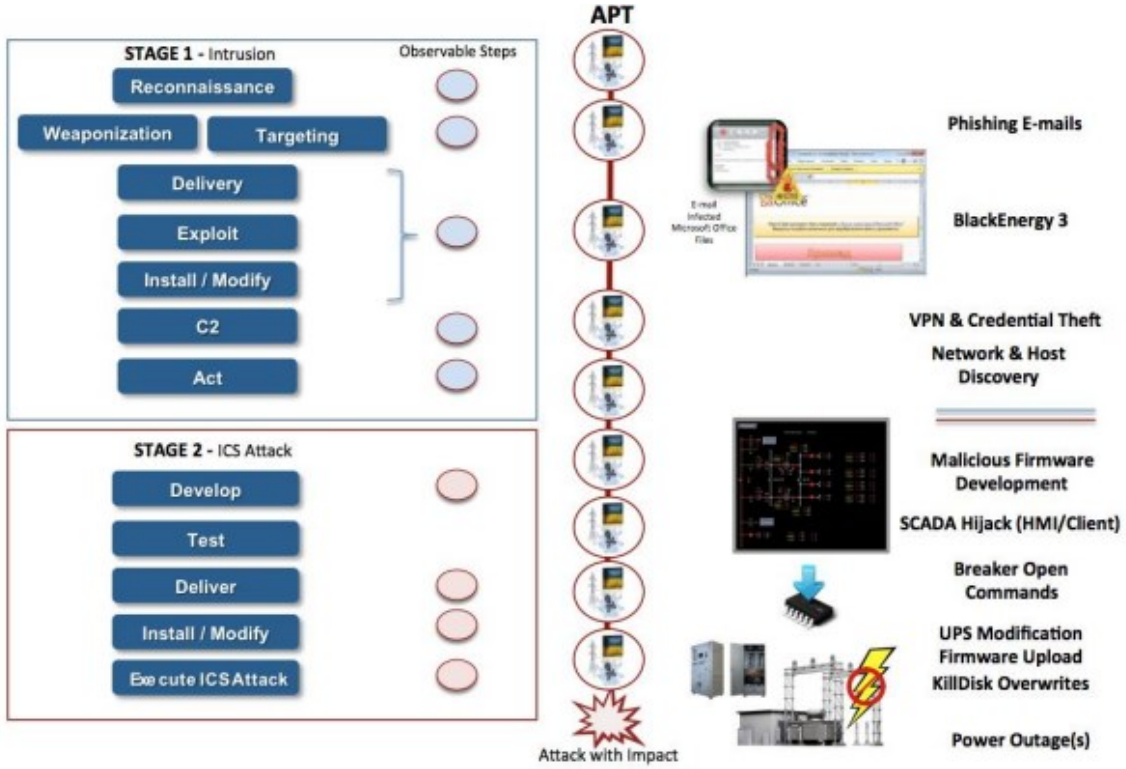
5.3. Analiza treće studije slučaja: Napad na ukrajinsku električnu mrežu

Treća studija slučaja bavi se analizom napada na tri distribucijske jedinice električne kompanije Kyivoblenergo u prosincu 2015. godine. Cilj napada bio je sustav upravljanja SCADA koji je izvršenim napadom uspješno kompromitiran, a posljedica je bila nestanak električne energije kod 225 000 korisnika u Ukrajini. Kriminalci iza napada na ukrajinsku električnu mrežu pokazali su se izuzetno organiziranima i pripremljenima te su tijekom napada koristili više metoda kao što su *spear phishing*, *BlackEnergy* zloćudni kod i manipulacija Microsoft Office dokumenata. Kriminalci su napadima ciljali uređaje u manjim distribucijskim jedinicama kako

bi onesposobili njihov rad i pomoću telefonskih sustava su organizirano i strateški generirali velik broj poziva na broj tehničke podrške kompanije kako bi onemogućili korisnicima prijavu nestanka energije (Lee, Assante, Conway, 2016).

Prilikom planiranja i izvršenja napada kriminalci su koristili *ICS h Killer Chain*, plan napada detaljno prikazanog na slici 10. koji opisuje korake izvođenja visoko sofisticiranih kibernetičkih napada. Napad je bio podijeljen na dvije razine (Lee, Assante, Conway, 2016).

Slika 9 - ICS Cyber Killer Chain



Izvor: Lee. R. M., Assante, M. J., Conway, T. (2016),_Analysis of the Cyber Attack on the Ukrainian Power Grid.

Prva razina napada bila je podijeljena na dvije faze, gdje se prva faza naziva fazom izviđanja a druga fazom ciljanja.

Faza izviđanja odnosi se na period prije samoga napada kada je kriminalna organizacija prikupljala sve potrebe podatke potrebne za njegovo izvršavanje. Iako nema dokaza o prikupljanju podataka prije samog napada na mrežu, sofisticiranost i organiziranost napada na distributivne jedinice implicira da je ova faza morala biti izvršena u određenom vremenu prije napada (Lee, Assante, Conway, 2016).

Drugi korak je faza ciljanja, prilikom koje se određuju sustavi nad kojima će se vršiti napad. Tijekom ovoga napada nije se moglo doći do zaključka koja je specifična infrastruktura bila primarni cilj jer se napad vršio umetanjem zlćudni koda u Microsoft dokumente. Prilikom otvaranja programa Microsoft Office paketa zaposlenicima se prikazao upit o korištenju određenih postavki tijekom korištenja paketa. Odobravanjem određenih postavki aktiviralo se

preuzimanje zloćudnog programa koji je kriminalcima omogućio pristup podacima i komunikaciju sa sustavom (Lee, Assante, Conway, 2016).

Šest mjeseci prije glavnog napada na mrežu, kriminalci su pomoću *spear phishinga* prikupljali podatke o djelatnicima i elektroničkom poštom slali poruke pojedincima. Kako bi se prevenirala ovakva vrsta napada u postrojenjima potrebno je zaposlenike slati na tečajeve sigurnosti i provoditi kontinuirano testiranje podložnosti na *phishing* napade. Postavljanjem zaštita sustava kriminalci modificiraju napade kako bi im se prilagodili i nužno je obrazovati djelatnike u anticipiranju napada i uočavanju tehnika korištenih kod socijalnog inženjeringa (Lee, Assante, Conway, 2016).

BlackEnergy 3 zloćudni kod korišten u napadu u pozadini je djelovao kao *keylogger* i analizirao uzorke pri unošenju podataka za registraciju. Instalacija zloćudnih programa mogla je biti spriječena strateškom uporabom forenzičkih alata koje, nažalost, kompanija nije posjedovala. Djelatnike postrojenja trebalo je poticati na češće mijenjanje lozinki i nadzirati njihove aktivnosti tijekom korištenja sustava kako bi se utvrdile bilo kakve sumnjivosti (Lee, Assante, Conway, 2016).

Preuzimanjem podataka kriminalci su mogli identificirati slabosti sustava te osmisliti koncept napada kojim je postignut prekid energije. Kako bi se ovo spriječilo, potrebno je identificirati osjetljive informacije i ograničiti njihovu dostupnost. Djelatnici koji su zaduženi za obranu sustava moraju preispitati svoje sposobnosti uočavanja i reakcije na prijetnje dok uprava mora upravljati planovima za obnovu ukradenih informacija. Jedna od metoda aktivne obrane od krađe informacija je metoda nadgledanja sigurnosti mreža (eng. *Network Security Monitoring*) kojom se može utvrditi je li došlo do neautoriziranih preuzimanja podataka i prekinuti taj proces prije no što je nastala šteta na industrijskom kontrolnom sustavu (Lee, Assante, Conway, 2016).

Nedostatak nadgledanja mreže u napadu, kao i nedostatak dvofaktorske autentifikacije kod pristupanja, omogućio je kriminalcima kontinuirani pristup sustavu (Shehod, 2016).

Analizom napada utvrđeno je daljinsko upravljanje sustavom u svrhu provođenja druge faze napada. Kako bi se sustav zaštitio od ovakvog napada potrebno je uspostaviti sigurnu okolinu koja privremeno onemogućuje uspostavu kontrolnog signala od nepoznatih uređaja. Prevencija napada može se vršiti uspostavljanjem razina autorizacije, koja ograničava operaterima sustava da utječu na sve njegove komponente i čime se otežava kriminalcima da imaju pristup svim radnim stanicama istovremeno. Prepoznavanjem ovih ograničenja napadači će moći prilagoditi napad i ukloniti takva ograničenja, međutim operateri mogu uočiti promjene nadgledanjem komunikacijskih sesija (Lee, Assante, Conway, 2016).

5.4. Analiza rezultata istraživanja i diskusija

Uloga phishinga u slučaju napada u Amsterdamu

Phishing napad pokazao se kao primarna prijetnja u slučaju u Amsterdamu gdje su se kriminalci koristili svojim organizacijskim vještinama i tehnikama socijalnog inženjeringa kako bi nanijeli financijsku štetu pojedincima. Strateškim kombiniranjem socijalnog inženjeringa i tehnologije kriminalci su uspjeli izvršiti napade na dvije banke s različitim sustavima autentifikacije te preuzeti značajne količine financijskih sredstava s računa pojedinaca.

Primarna metoda kriminalaca bila je regrutirati vanjske suradnike u fazama napada kada je korištenje tehnologije bilo neophodno. Kritični faktor uspješnosti napada bilo je prethodno međusobno poznavanje organizatora te ostali čimbenici poput njihove etničke pripadnosti, što je u sociološkom i psihološkom smislu pridonijelo funkcioniranju organizacije.

Proces prikupljanja podataka od regrutiranih zaposlenika banaka uvelike je olakšan nedostacima primjerenih kontrola zaštite njihovim informacijskih sustava. Primjerice, iako su većina regrutiranih bili novi zaposlenici banaka imali su pristup povjerljivim dokumentima o prošlim transakcijama korisnika što upućuje na nedostatak adekvatne autorizacije, a samim time i na zanemarivanje sigurnosti sustava. Implementiranjem sustava autorizacije, fizičkom zaštitom dokumenata i redovitim revizijama ne samo tehničkih već i socijalnih dijelova sustava značajno se mogla smanjiti vjerojatnost uspješnog napada.

Jedan od najvažnijih čimbenika uspjeha organizacije bilo je korištenje tehnika socijalnog inženjeringa kao napada na korisnike, ali i kao metode regrutiranja novih članova u organizaciju. Navedenom metodom cilj je bio prevariti što je veći broj pojedinaca u otkrivanje povjerljivih podataka kao i regrutirati nove članove u organizaciju, pošto sami organizatori nisu posjedovali vještine potrebne kako bi se napad proveo.

Slučaj prikazuje koliko opasne mogu biti metode socijalnog inženjeringa i koliko lako se može izmanipulirati ljude u otkrivanje osobnih podataka. Zbog toga je potrebno naglasiti važnost informiranosti o politikama institucija čije se usluge koriste. Primjerice, da su korisnici imali informaciju da banke ne traže povjerljive podatke od korisnika telefonom već dolaskom u poslovnicu banke mogli su prepoznati da se radi o prijevari i slučaj odmah prijaviti policiji.

Primjeri napada poput ovoga ističu koliko je važno biti svjestan rizika direktnog ili indirektnog otkrivanja osobnih informacija ali i sudjelovanja u ilegalnim aktivnostima zbog financijske dobiti.

Uloga phishinga u simulaciji napada na bolnicu

Tijekom simulacijskog napada korištene su razne *phishing* metode kako bi se testirala pozornost i reaktivnost zaposlenika bolnice u slučaju da dođe do stvarnog napada na bolnicu, što je u vrijeme epidemije koja je tada bila prisutna u svijetu moglo za pacijente biti pitanje života i smrti ako bi potencijalni napadi onemogućili pristup informacijskom sustavu bolnice gdje se skladište njihovi podaci.

Korištenje prilagođenih poruka prilikom napada pokazalo se kao najopasnijom metodom *phishing* napada na djelatnike bolnice, što je logično zato što je većina ljudi psihološki podložna sadržaju koji je njima namijenjen, a činjenica kako se radi o velikoj bolnici koja se suočavala s teškom epidemijom povećava vjerojatnost da ovakva vrsta *phishing* napada ostavi kobne posljedice za bolnicu i njene pacijente. Primjerice ako bi se izvršio *ransomware* napad kakav se dogodio u bolnici u Los Angelesu koji bi potencijalno onemogućio pristup zdravstvenim kartonima pacijenata i tako direktno ugrozio njihovo zdravlje.

Iako je poželjno što češće provoditi simulacije napada kako bi se smanjila vjerojatnost uspjeha stvarnog napada, pojedine faktore tijekom simulacije je trebalo prilagoditi kako bi se bolje analizirala spremnost djelatnika na obranu od phishing napada. Autorovo je mišljenje kako su simulacije trebale biti provedene nad svim djelatnicima bolnice, uključujući novim zaposlenicima i menadžmentom jer se uz manji postotak uključenog osoblja ne mogu u potpunosti prikazati eventualne posljedice stvarnog napada. Ipak je važno naglasiti da dodavanjem novih obaveza zaposlenicima može stvoriti i dodatan umor koji ih može kompromitirati tijekom donošenja odluka, pri čemu se može zaključiti kako pretjerano provođenje edukacija i simulacija može imati negativan efekt na djelatnike i kvalitetu istraživanja.

Nedostatak simulacije očituje se u isključenju menadžmenta iz procesa te njegovo provođenje isključivo elektroničkom poštom. Isključenje menadžmenta izrazito je loša odluka jer, kako je ranije navedeno, većina *phishera* zapravo cilja ovaj sloj organizacije jer iz njega mogu izvući najviše informacija. Provođenje simulacije isključivo putem elektroničke pošte ograničava prikaz potencijalne štete koja bi nastala eventualnim kombiniranjem više medija u stvarnom napadu. Primjerice u simulaciju se moglo uključiti *vishing*, *smishing* ili *instant messaging* napade koji bi možda prikazali bolju sliku sigurnosti informacijskog sustava bolnice. Može se reći kako je provedena simulacija nepotpuna jer nije obuhvatila sve aspekte sigurnosti informacijskih sustava. Nakon analize rezultata provedenih simulacija lako je uočiti nedostatke istih, posebice kod izvanrednih situacija kao što je epidemija. Zbog nehomogenosti djelatnika i njihovih sposobnosti teško je utvrditi razinu izloženosti ovakvim vrstama napada, dok su se skrivanjem identiteta pojedinaca koji su otvorili sadržaje poruka zbog njihove privatnosti ograničile analize kojima bi se utvrdilo koja je skupina njima najviše izložena (Rizzoni et al., 2022).

Uloga phishinga u napadu na ukrajinsku mrežu

Napad na ukrajinsku mrežu jedan je od najboljih primjera kojim se prikazuju razmjeri štete koja može biti prouzročena kombiniranje *phishing* napada sa drugim kibernetičkim napadima. Iako se tijekom istrage napada kriminalci nisu uspjeli identificirati, politička situacija u kojoj se Ukrajina tada nalazila i još danas nalazi upućuje da je motiv napada političke prirode. Kombinacija *phishinga* kao tehnike prodiranja u industrijski informacijski sustav, kombinirana s ostalim tehnikama kibernetičkog ratovanja i zavidnom razinom organizacije i strategije pokazala se izuzetno učinkovitom u izvršenju napada.

Uspješno provođenje napada i posljedice koje su uslijedile pokazatelj su koliko je ljudski faktor bitan u upravljanju i zaštiti informacijskih sustava te koje mogu biti posljedice ako ti faktori nisu na prihvatljivoj razini. Analizom napada uočen je niz grešaka u ponašanju djelatnika koje su se mogle izbjeći implementiranjem osnovnih koraka provođenja sigurnosti sustava i jačim naglaskom na opreznost prilikom njihove uporabe. Korišteni SCADA sustav nije posjedovao kriptografski šifrirane komunikacijske protokole, što je napadačima olakšalo presretanje poruka razmijenjenih unutar komunikacijskog sustava kompanije, a samim time i prikupljanje informacija potrebnih u izradi plana napada (Gaoqi et al., 2016).

Istragom nisu utvrđene specifičnosti u napadu koje bi upućivale na nedostatke u infrastrukturi ovih sustava te je prilikom upravljanja sustava bilo potrebno poduzeti opće korake u zaštiti kojima bi se spriječila ovakva vrsta napada. Korištenje *ICS Cyber Kill Chain* metode provođenja napada na mrežu pružalo je djelatnicima više prilika da uoče i obrane sustav od ovakvih vrsta napada. Za uspješno provođenje ove metode potrebno je više mjeseci, što djelatnicima dalo dovoljno velik vremenski okvir za uočavanje sumnjivih aktivnosti i implementiranje zaštite. Sam koncept izvođenja procesa napada bilo je potrebno poopćiti na cijeli sustav. Pretpostavka je da su napadači stvorili razarajući *firmware* nakon prodora u sustave i analize slabih točaka sustava (Lee, Assante, Conway, 2016).

Ozbiljnost napada u Ukrajini, koji se mogao klasificirati kao kibernetičko ratovanje, promptno je alarmirala djelatnike i upravitelje mreža diljem svijeta, posebice u Sjedinjenim Američkim Državama. Prilikom simulacije *spear phishing* napada na informacijske sustave postrojenja u blizini Seattlea ustanovljeno je kako je značajan broj djelatnika kliknuo na sadržaje poslane *spear phishing* pošte, slično kao u ukrajinskom napadu. Ekspertima iz područja digitalnih znanosti trebalo je točno 22 minute kako bi probili sigurnosni sustav postrojenja. Prednost ukrajinske mreže je u starijoj opremi koja koristi kombinaciju automatskih i ručnih kontrola, dok se američka postrojenja u potpunosti oslanjaju na informacijske sustave, što dovodi do zaključka kako bi potencijalni napadi na postrojenja u američkim gradovima mogla imati ozbiljnije posljedice (Shehod, 2016).

Usporedba slučajeva i diskusija

Provedenim analizama na tri odvojena slučaja dolazi se do zaključka o zajedničkim faktorima i efektivnostima metoda obrane kod ovakvih vrsta kibernetičkih prijetnji. Iako *phishing* napadi nisu u svim slučajevima bili jedina metoda kibernetičkih napada može se ustanoviti da pripadaju u najopasnije metode kibernetičkih prijetnji današnjice jer im je cilj napasti najslabiju kariku u procesu zaštite informacijskih sustava; ljude.

Ono što čini ovakve vrste napada toliko opasnima jest činjenica da se ne temelje na tehnologiji a samim time od njih se ne može zaštititi upotrebom iste, već je potrebno kontinuirano prakticiranje sigurnosnog ponašanja. Slučaj simulacije napada izvedenog u bolnici u Italiji odličan je pokazatelj kako su vježbe u organizacijama opravdane i potrebne kako bi se sukcesivno i u značajnijoj mjeri smanjila vjerojatnost uspješnog *phishing* napada. Negativne strane provođenja simulacija su što ne mogu točno odrediti posljedice stvarnog napada, kao što

su bili napadi na banke u Amsterdamu ili napad na ukrajinsku električnu mrežu, kao i etičnost njenog provođenja.

Paralelno analizirajući ova tri slučaja može se zaključiti kako sigurnost informacijskog sustava mora biti imperativ u poslovanju organizacije. Prepreke u implementiranju kulture sigurnosti kao zaštite od *phishing* napada nerijetko može predstavljati ljudska psihologija. Pojedinci često imaju misli kako se ovakve prijevare njima ne mogu dogoditi i samim time postaju prijetnja vlastitoj sigurnosti i sigurnosti organizacija u kojima su zaposleni ili čije usluge koriste. Najvišu razinu odgovornosti za informacijsku sigurnost ipak snosi menadžment organizacije, što je posebno vidljivo u ukrajinskom napadu u kojem postrojenja energetske mreže nisu imala niti osnovnu zaštitu i njeni djelatnici nisu posjedovali osnovne vještine prepoznavanja prijetnji, što je i dovelo do tako ozbiljnih posljedica.

Slučajevi dokazuju da su *phishing* napadi jedni od najopasnijih kibernetičkih prijetnji današnjice te da neimplementiranjem kontrola i zaštita protiv njihova djelovanja može dovesti pojedinca, organizaciju ali i državu u kritičnu situaciju. Idealna kombinacija zaštita protiv phishing napada, ali i ostalih napada temeljenih na socijalnom inženjeringu, je kontinuirana edukacija, snažan naglasak na kulturu sigurnosti u organizaciji i redovito provođenje temeljitih revizija informacijskih sustava.

6. ZAKLJUČAK

Sigurnost informacijskih sustava postala je jedan od temeljnih ciljeva pojedinaca i organizacija današnjice. Paralelnim razvojem informacijskih sustava kao primarnog faktora uspješnosti u poslovanju razvijale su se i sve kompleksnije prijetnje njihovoj sigurnosti. Prodor u informacijske sustave kriminalcima omogućuje krađu podataka pomoću kojih mogu onemogućiti organizacijama daljnje poslovanje ili ukrasti financijska sredstva. Idealna razina sigurnosti informacijskih sustava postiže se strateškom primjenom kombinacija kontrola rada, zaštitnih mjera te redovitih provođenja revizije, pri čemu je važno naglasiti da navedenu razinu sigurnosti nikada nije moguće postići već je cilj njoj stalno težiti.

Phishing napadi vrsta su kibernetičkih prijetnji u kojima kriminalci koriste kombinaciju metoda socijalnog inženjeringa i tehnologije u svrhu otkrivanja povjerljivih podataka o pojedincima i organiziranja visoko individualiziranih napada kojima je najčešći medij prijenosa elektronička pošta. Smatraju se jednom od najopasnijih vrsta kibernetičkih prijetnji unatoč svojoj jednostavnosti i kontinuirano predstavljaju prijetnju sigurnosti pojedinaca, organizacija i država. Posebno štetnima smatraju se *spear phishing* i *whaling* napadi koji se detaljnim informacijama prilagođavaju pojedincima u organizacijama i čine najveći postotak uspješno provedenih kibernetičkih napada iz domene socijalnog inženjeringa.

Zaštita od *phishing* napada provodi se kontinuiranim obrazovanjem i uspostavljanjem kulture sigurnosti u organizacijama. Implementiranjem kulture sigurnosti u organizaciju djelatnici su neprekidno izloženi informacijama o posljedicama uspješno provedenih napada. Dužnost organizacija današnjice je provoditi redovite simulacije *phishing* napada u okviru revizije informacijskih sustava kojima se pruža uvid u spremnost djelatnika na obranu od takvih vrsta prijetnji.

Cilj ovog rada bio je analizirati obilježja i faktore uspješnosti *phishing* napada prikazom tri odvojene studije slučajeva. Pri tome, u svakoj analizi su *phishing* napadi imali drugačije funkcije i nastojalo se dokazati koje posljedice mogu nastati njihovim uspješnim provođenjem te navesti metode kojima se njihovo izvršavanje moglo prevenirati ili ublažiti.

Analiziranjem studija slučajeva dolazi se do zaključka kako su phishing napadi izuzetno opasne vrste kibernetičkih prijetnji i da je potrebna kontinuirana edukacija i provođenje simulacija u organizacijama kako bi se spriječio njihov potencijalni devastirajući učinak na sigurnost informacijskih sustava.

7. POPIS LITERATURE

1. AFP, NSW man jailed for SMS phishing scam targeting 450 victims, Dostupno na: https://www.afp.gov.au/news-media/media-releases/nsw-man-jailed-sms-phishing-scam-targeting-450-victims
2. Aleroud, A., Zhou, L. (2017), Phishing Environments, Techniques, and Countermeasures: A Survey. Dostupno na: https://www.sciencedirect.com/science/article/am/pii/S0167404817300810
3. Al-Mamary, Y. H., Shamsuddin, A., Aziati, N. (2014), The Role of Different Types of Information Systems In Business Organizations: A Review, *International Journal of Research,* 1(7), 1279-1286. Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/55341839/Aalmamray-2014-libre.pdf?1513793682=&response-content-disposition=inline%3B+filename%3DThe_Role_of_Different_Types_of_Informati.pdf&Expires=1693830870&Signature=R-u~q4tN1WED48zsd~9xiGPahAc8hRXykOHwzCK9ds8glDm~XAegM7EKwUAsPpe7qBcITCnlPhZ-xRsEe5M~6TGlcyI87RrPDiZRH9orLKArhHEjCAtT9dpdp7TmKIKMA0erxgKiWmKFAVOWXUlU5b~AIBZJ4ysZrksVqD6SxGCaXUojoDrMPMkQcRbc0e0TIiolgQ5j7jvt-h-bk78DzyB9ERP3rcgt1X9rx3eEXYWIT8PxfZCyynfQCUf6WoVVZ7sGdirkrppaFsb3nLpQObAfnJzMtrY4AHMYZtQJcB7IhPo3V4A5dSANbMWztPCv80DLbgRdytQpc2BOrAHGcw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
4. Alsharnouby, M., Alaca, F., Chiasson, S. (2015), *Why phishing still works: user strategies for combating phishing attacks*. Dostupno na: https://chorus.scs.carleton.ca/wp-content/papercite-data/pdf/alsharnouby2015phishing-ijhcs.pdf
5. Alwanain, M. (2020), Phishing Awareness and Elderly Users in Social Media, *International Journal of Computer Science and Network Security,* 20(9) 114-119. Dostupno na: https://www.researchgate.net/profile/Mohammed-Alwanain/publication/344134421_Phishing_Awareness_and_Elderly_Users_in_Social_Media/links/5fc562ffa6fdcce95268ebef/Phishing-Awareness-and-Elderly-Users-in-Social-Media.pdf
6. Arbanas, K., Spremić, M., Žajdela Hrustek, N. (2021), Holistic framework for evaluating and improving information security culture, *Aslib Journal of Information Management,* 73(5), 699-719.
7. Badra, M., El-Sawda, H., Hajjeh, I. (2010), Phishing Attacks and Solutions, *3rd International ICST Conference on Mobile Multimedia Communications.* Dostupno na: https://eudl.eu/pdf/10.4108/ICST.MOBIMEDIA2007.1899
8. Ballad, B., Ballad, T., Banks, E. K. (2011), Acess Control, Authentication, and Public Key Infrastructure, London: Jones & Bartlett Learning
9. Banu, M. N., Banu, S. M. (2013), A Comprehensive Study of Phishing Attacks, *International Journal of Computer Science and Information Technologies,* 4(6), 783-786. Dostupno na:

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2bf12ff75150903efee426f23035c94d599597ae
10. Basnet, R., Mukkamala, S. & Sung, A. H. (2008), Detection of Phishing Attacks: A Machine learning approach, *Studies in Fuziness and Soft Computing.* Dostupno na: https://www.researchgate.net/profile/Andrew-Sung-4/publication/226420039_Detection_of_Phishing_Attacks_A_Machine_Learning_Approach/links/09e4150857ea2c526b000000/Detection-of-Phishing-Attacks-A-Machine-Learning-Approach.pdf
11. Bell, S., Komisarczuk, P. (2020), An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank. Dostupno na: https://phishalytics.com/publications/Bell-Komisarczuk-An-Analysis-of-Phishing-Blacklists-Google-Safe-Browsing-OpenPhish-and-PhishTank-aisc.pdf
12. Bhavsar, V., Kadlak, A., Sharma, S. (2018), Study on phishing attacks, *International Journal of Computer Applications.* Dostupno na: https://www.researchgate.net/profile/Shabnam-Sharma-2/publication/329716781_Study_on_Phishing_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf
13. Bossetta, M. (2018), The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy, *Journal of International Affairs Editorial Bord,* 71(1.5.), 97-106. Dostupno na: https://www.jstor.org/stable/pdf/26508123.pdf?casa_token=i56M-k5ysN8AAAAA:nbVPfxvJ-dN3frCqo2lYCyAbl3biMjtT9CqAvnb-zrVyXeO-_3dlL-amZnPk3_SloJ5DZHyJ-kwTeYNngmui_vsZsFXesiQuhpUscm5LaHpvbu2aUzZ7
14. Bullée, J. W. H, Montoya, L., Junger, M., Hartel, P. (2017), Spear phishing in organisations explained, *Information and Computer Security.* Dostupno na: https://www.researchgate.net/profile/Marianne-Junger/publication/320207541_Spear_phishing_in_organisations_explained/links/5e1dfa3d299bf136303ab301/Spear-phishing-in-organisations-explained.pdf
15. Butavicius, M., Parsons, K., Pattinson, M., McCormac, A. (2015), *Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails*. Dostupno na: https://arxiv.org/ftp/arxiv/papers/1606/1606.00887.pdf
16. Choobineh, J., Dhillon, G. Grimaila, M. R., Rees, J. (2007): Management of Information Security: Challenges and Research Directions, *Communications of the Association for Information Systems,* 20(57) 958 – 967.
17. ComputerWorld, (2007), Elaborate „pharming“ attack targeted 50 banks. Dostupno na: https://www.computerworld.com/article/2543237/elaborate--pharming--attack-targeted-50-banks.html
18. Council on Foreign Relations. Dostupno na: https://www.cfr.org/cyber-operations/operation-aurora
19. CSO, Chinese scammers take Mattel to the bank, Phishing them for $3 million, Dostupno na: https://www.csoonline.com/article/555513/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html
20. CyberHoot, Phishing. Dostupno na: https://cyberhoot.com/cybrary/phishing/
21. Dhamija, R., Tygar, J. D., Hearst, M. (2006), Why Phishing Works. Dostupno na: https://escholarship.org/content/qt9dd9v9vd/qt9dd9v9vd.pdf
22. Downs, J. S, Holbrook M. B. &, Cranor, L. F. (2006), *Decision Strategies and Susceptibility to Phishing.* Dostupno na:

https://kilthub.cmu.edu/articles/journal_contribution/Decision_Strategies_and_Susceptibility_to_Phishing/6621860/files/12118340.pdf
23. Downs, J. S., Holbrook, M., Cranor L. F. (2007), *Behavioral Response to Phishing Risk.* Dostupno na: file:///C:/Users/38591/Downloads/file%20(7).pdf
24. Felt, A. P., Wagner, D. (2011), *Phishing on Mobile Devices*. Dostupno na: http://people.eecs.berkeley.edu/~daw/papers/mobphish-w2sp11.pdf
25. Fette, I., Sadeh, N., Tomasic, A. (2006), *Learning to Detect Phishing Emails, Pittsburgh.* Dostupno na https://apps.dtic.mil/sti/pdfs/ADA456046.pdf
26. Flores, D. A., Qazi, F., Jhumka, A. (2016), Bring Your Own Disclosure: Analysing Threats to Corporate Information. Dostupno na: https://wrap.warwick.ac.uk/88165/1/WRAP-Bring-disclosure-corporate-Flores-2017.pdf
27. Forbes, How Lenovo's Superfish „Malware“ Works And What You Can Do To Kill It, Dostupno na: https://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-need-to-know/
28. Gaoqi, L., Weller, S. R., Junhua, Z., Fengji, L., Zhao, Y. D. (2016), The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. Dostupno na: https://nova.newcastle.edu.au/vital/access/services/Download/uon:30883/ATTACHMENT02
29. Gerić, S., Hutinski Ž. (2007), Information system security threats classifications, *Journal of information and organizational sciences,* 31(1), 51-61. Dostupno na: https://hrcak.srce.hr/file/33758
30. Hajdarevic, K., Allen, P., Spremić, M. (2016) Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments, *Tellecommunications Forum (TELFOR),* 2016 24th, IEEEExplore, 2016, pp. 41-44. https://www.researchgate.net/profile/Mario-Spremic/publication/312571255_Proactive_security_metrics_for_Bring_Your_Own_Device_BYOD_in_ISO_27001_supported_environments/links/5d99af3b92851c2f70eeea1e/Proactive-security-metrics-for-Bring-Your-Own-Device-BYOD-in-ISO-27001-supported-environments.pdf
31. Halevi T., Memon N., Nov O. (2015), Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks, *SSRN Electronic Journal*. Dostupno na: https://www.researchgate.net/profile/Tzipora-Halevi/publication/317904745_Spear-Phishing_in_the_Wild_A_Real-World_Study_of_Personality_Phishing_Self-Efficacy_and_Vulnerability_to_Spear-Phishing_Attacks/links/5da079eea6fdcc8fc3474953/Spear-Phishing-in-the-Wild-A-Real-World-Study-of-Personality-Phishing-Self-Efficacy-and-Vulnerability-to-Spear-Phishing-Attacks.pdf
32. Harrison, B., Svetieva, E., Vishwanath, A. (2016), Individual processing of phishing emails: How attention and elaboration protect against phishing, *Online Information Review.* Dostupno na: https://www.researchgate.net/profile/Brynne-Harrison/publication/299552211_Individual_processing_of_phishing_emails/links/59c65440aca272c71bc2aca2/Individual-processing-of-phishing-emails.pdf
33. Hirrscheim, R, Klein, H. K. (2012), A Glorious and Not-So-Short History of the Information Systems Field, *Journal of The Association for Information Systems*, 13(4), 188-235. Dostupno na:

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2a5d28982c56e887fc23654f3f201c7d3de4d6e1
34. Hong, J. (2012), *The Current State of Phishing Attacks.* Dostupno na: file:///C:/Users/38591/Downloads/file%20(5).pdf
35. IBM (2004), *The Phishing Guide: Understanding & Preventing Phishing Attacks*, IBM Internet Security Systems
36. IBM. What is BYOD (bring your own device)? Dostupno na: https://www.ibm.com/topics/byod
37. Idwatchdog, Beware of IRS Phishing and Impersonation Scams – During Tax Season and Year-Round, Dostupno na: https://www.idwatchdog.com/irs-phishing-and-impersonation-scams
38. IT Assurance and Cyber Security, Examples of Phishing Emails Covid-19 Specific Examples. Dostupno na: https://blogs.otago.ac.nz/infosec/examples-of-phishing-emails/
39. Jakkobsson, M. (2007), The Human Factor in Phishing. Dostupno na: http://markus-jakobsson.com/papers/jakobsson-psci07.pdf
40. Jouini, M., Rabai L. B, A. & Aissa A. B. (2014), Classification of security threats in information systems, u: Jouni M. (ur.), *5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014*), (str. 489-496), Elsevier
41. Kalaharsha P. & Mehtre, B. M. (2021), *Detecting Phishing Sites – An Overview.* Dostupno na: https://arxiv.org/pdf/2103.12739.pdf
42. Kessler, G. C., (2015), An Overview of Crypthography. Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/38411944/An_Overview_of_Cryptography.pdf?1438962673=&response-content-disposition=inline%3B+filename%3DAn_Overview_of_Cryptography.pdf&Expires=1693251856&Signature=F5SrvJPadcu3JDF1uOV8VpdeTFQ9P8ib-X8C~cyJVBhhiRr6T3KxLSQtdcGcpt2X35~1iWLeaR77Vb8RbdWExHxxuuJwolJdHJumLUeDl-Vhcdp7ttR-NkTXdwbMUXiUKP9-daj3DP1Af~7pZReji34q7kIzwN-iR2XmuEIGYp3b7iDwQApQfdCwBuNxMA3YjnLWuwUq6PgKcG6s4wCu1aLlkCa68X1H6Jt52ZbNM7LHsBk9WyzPeQR1OtBomwJbzCCKzb0NYJ4FGO1j1cvzt7itbhF2XreeIUtBDyjjppgNtKoCRc5LMCtnrjSVCh~fsJ0M3F-R~Ox6-bz8z88OTQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
43. Khonji M., Iraqi, Y., Jones, A. (2013), Phishing Detection: A Literature Survey, *IEEE Communications Surveys & Tutorials,* 15(4), 2091-2121. Dostupno na: http://romisatriawahono.net/lecture/rm/survey/network%20security/Khonji%20-%20Phishing%20Detection%20-%202013.pdf
44. Kirlapappos, I., Sasse, M. A. (2011), Security education against phishing: A modest proposal for a major re-think. Dostupno na: https://discovery.ucl.ac.uk/id/eprint/1353958/1/Kirlappos_Security_2012.pdf
45. Kwak, Y., Lee, S., Damiano, A., Vishwanath, A. (2020), Telematic and Informatics: Why do users not report spear phishing emails? *Elsevier.* Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/87780494/why-do-users-not-report-phishing--libre.pdf?1655728589=&response-content-disposition=inline%3B+filename%3DWhy_do_users_not_report_spear_phishing_e.pdf&Expires=1693940243&Signature=XvFv3Vc-TUFES5D5s0eUr0GRHZC9xUF8tTqAq7IBXBULTb-6nAtA7hm~~wtdDG8HoFK-~-dr0wk4dJsVTazuTFBS9hAlwl6-

qL8r9OtSSsZ9xajIWWifZ5jt51yxh2Gf8Vbj2ToiiDQTyQhpRWWAm35xec2qtGrRFRTNI5JtGPkqU~xRY5ho6tGcmWbrHoxjz1J04LTs80d3PO3ql8Tq4fgtfLgeiEUbBSj-noDULrno~h9w~0F-XoZkkhX~wTP1yUVP6cctLpbNWdNFPlN5GoKXJORxI0HZiXz-poE94hA8riEqSOkEiyBEh2N8u45b-AwzRdsbVqvKZPgsVf8UWQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

46. Laycock, A., Petrić, G., Roer., K. (2019), The seven dimensions of security culture. Dostupno na: https://www.knowbe4.com/hubfs/CLTRe-The7DimensionsSecurityCulture-ResearchPaper.pdf
47. Lee, R. M., Assante, M. J., Conway, T. (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid. Dostupno na: https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf
48. Leukfeldt, E. R. (2014), Phishing in Amsterdam, *Trends Organ Crim,* 17, 231-249, Springer. Dostupno na: https://www.researchgate.net/profile/Eric-Leukfeldt/publication/280014116_Leukfeldt_ER_2014_Cybercrime_and_social_ties_Phishing_in_Amsterdam_In_Trends_in_Organized_Crime_174_231-249/links/575ec6d508aed884621b798d/Leukfeldt-ER-2014-Cybercrime-and-social-ties-Phishing-in-Amsterdam-In-Trends-in-Organized-Crime-174-231-249.pdf
49. Lian, S., Kanellopoulos, D., Ruffo, G. (2009), Recent Advances in Multimedia Information System Security, *Informatica.* Dostupno na: https://www.informatica.si/index.php/informatica/article/viewFile/220/217
50. Mallik, A. (2018), Man-in-the-middle: Understanding in Simple Words, *Jurnal Pendidikan Tehnologi Informasi,* 2(2), 109-134. Dostupno na: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/viewFile/3453/2707
51. McGrath, D. K, Gupta, M. (2008), *Behind Phishing: An Examination of Phisher Modi.* Dostupno na: https://www.usenix.org/legacy/event/leet08/tech/full_papers/mcgrath/mcgrath_html/
52. Mhaskar, N., Alabbad, M., Khedri, R. (2021), A Formal Approach to Network Segmentation. Dostupno na: https://www.researchgate.net/profile/Neerja-Mhaskar/publication/348333249_A_Formal_Approach_to_Network_Segmentation/links/6047898a299bf1e07867b8b3/A-Formal-Approach-to-Network-Segmentation.pdf
53. Nagunwa, T. (2014), Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors, *International Journal of Cyber- Security and Digital Forensics,* 3(1), 72-83. Dostupno na: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4c49e591bf6679f9430e1b8d038c18f9a871ae03
54. NIST (2004), *Security Considerations in the Information System Development Life Cycle,* Gaithersburg: National Institute of Standards and Technology
55. NIST (2017), *An Introduction to Information Security,* National Institute of Standards and Technology
56. NordVPN (2023), What is Locky ransomware, and how do you prevent it? Dostupno na: https://nordvpn.com/blog/locky-ransomware/
57. Oest, A., Safaei, Y., Zhang, P. (2020), PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists, *29th USENIX Security Symposium,* 379-386. Dostupno na: https://www.usenix.org/system/files/sec20-oest-phishtime.pdf

58. Parmar, B. (2012), Protecting against spear-phishing, *Faronics*. Dostupno na: https://www.faronics.com/assets/CFS_2012-01_Jan.pdf
59. Parno, B., Kuo, C., Perrig, A (2006), *Phoolproof Phishing Prevention*. Dostupno na: https://kilthub.cmu.edu/ndownloader/files/11896526
60. Pejić-Bach, M., Spremić, M., Bosilj Vukšić, V., Ćurko, K., Jaković, B., Milanović Glavan , Lj. … Zoroja, J. (2020), *Osnove Poslovne Informatike*, Zagreb: Sveučilišna tiskara d.o.o.
61. Porter Felt, A., Wagner, D. (2011), Phishing on Mobile Devices. Dostupno na: http://people.eecs.berkeley.edu/~daw/papers/mobphish-w2sp11.pdf
62. Ramzan, Z. (2010), Phishing Attacks and Countermeasures, Handbook of Information and Communication Security, 433-448. Springer. Dostupno na: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9bcdb69f5dc2bac151c811a137501f25bec77e80
63. Rekouche, K. (2011), Early Phishing. Dostupno na: https://arxiv.org/ftp/arxiv/papers/1106/1106.4692.pdf
64. Resnik, D.B., Finn, P. R. (2017), Ethics and Phishing Experiments. Dostupno na: https://finn.lab.indiana.edu/PDFs/Resnik%20Finn%202017.pdf
65. Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., Coventry, L. (2022), Phishing simulation exercise in a large hospital: A case study. Dostupno na: https://journals.sagepub.com/doi/pdf/10.1177/20552076221081716
66. Salahdine, F., Kaabouch, N. (2019), Social Engineering Attacks: A Survey, *Future Internet,* 11(89). Dostupno na: https://www.mdpi.com/1999-5903/11/4/89/pdf
67. Shaikh, A. N., Shabut, A.M., Hossain, M. A. (2016), A Literature Review on Phishing Crime, Prevention Review and Investigation of Gaps, *International Conference on Software Knowledge, Information Management & Applications (SKIMA),* 9-15.
68. Shavran, K., Neha, B., Pawan, B. (2014), Penetration Testing: A Review, *Compusoft, An internationa journal of advanced computer technology,* 3(4), 752-757. Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/42046583/COMPUSOFT__34__752-757-libre.pdf?1454595834=&response-content-disposition=inline%3B+filename%3DCOMPUSOFT_3_4_752_757.pdf&Expires=1693508032&Signature=PbzBe6AzJFQzoBw1oR~n0uy1Fp2Gsk2U1~jRrb~Gbl-Wg117kDXmqez3EmNXrkQRPw4YmWxbAUQbhpfK2ojSxPFTGgBtNQGEu-HZMVNFdHiFUOoFDrOVDcRU-nV2Jcai~wgHAAPGxE-aROpmCJ0kqq3h6GFVB0Ch--mqh1Yi59-fawywi94nMJancwynJr60MjKrBrT19e5vnw6zLtF3r1~W3aCqZzl4YgKShccguZj7PH2B0F~V-WgzsNztRiUzZLhowuZf1~pzN4QyNT7kh7fO2jtvHhYusadB11EZwyx4Z9wJZ1Pz0ebY2N0S539Yt4-l2L1ZfzKp4vXVKeSE2Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
69. Shehod, A. (2016), Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US, *MIT.* Dostupno na: https://web.mit.edu/smadnick/www/wp/2016-22.pdf
70. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J. (2010), Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Dostupno na: https://www.researchgate.net/profile/Steve-Sheng/publication/221514257_Who_falls_for_phish_A_demographic_analysis_of_phishing_susceptibility_and_effectiveness_of_interventions/links/00463531e0f41f06510

00000/Who-falls-for-phish-A-demographic-analysis-of-phishing-susceptibility-and-effectiveness-of-interventions.pdf
71. Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., Zhang. (2009), An Empirical Analysis of Phishing Blacklists. Dostupno na: https://kilthub.cmu.edu/articles/An_Empirical_Analysis_of_Phishing_Blacklists/6469805/files/11898359.pdf
72. Sousa, K.J., Oz, E. (2014), *Management Information Systems,* sedmo izdanje, Cengage Learning
73. Spremić, M. (2007), Metode provedbe revizije informacijskih sustava, *Zbornik Ekonomskog fakulteta u Zagrebu*, (str. 295-312). Dostupno na: https://hrcak.srce.hr/file/41339
74. Spremić, M. (2012), Corporate IT risk management model: a holistic view at managing information system security risks, u: Spremić M., *International Conference on Information Technology*, (str. 299-304), London.
75. Spremić, M. (2017), *Digitalna transformacija poslovanja,* Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
76. Spremić, M. (2017), *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije,* Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
77. Spremić, M. (2018), *Enterprise Information Systems in Digital Economy,* Zagreb: University of Zagreb, Faculty of Economics & Business.
78. Stair, R., Reynolds, G. (2015), *Fundamentals of Information Systems,* osmo izdanje, Boston: Cengage Learning.
79. Sviličić, B., Kraš, A. (2005), Zaštita privatnosti računalnog sustava, *Pomorstvo,* 19, 275-284. Dostupno na: https://hrcak.srce.hr/file/6510
80. The Guardian (2021), What is Pegasus spyware and how does it hack phones? Dostupno na: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones
81. Varshney, G., Misra, M., Atrey P. (2016), A survey and classification of web phishing detection schemes. Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/53941667/SCNOnline-libre.pdf?1500702253=&response-content-disposition=inline%3B+filename%3DSCNOnline.pdf&Expires=1693392819&Signature=W~Dfyfw2OQT8JEEP2~0kMKGyUhsIdzotPCLppFFJWHys-FRFPs-3yLIGqWWuzV5SaPD5Lob1lO3lavgZjmD~2socs4GBfH4PRNxdb3o~ouH9TrzlL-JE6qh74eeeZd4jPRjE5T0HRCiLXo4JDTsgbIW8~diJDaw1VLLOAyWtG4YMZhF6pHklqyexYzeX6jXCrB23EAOMUd0pKM2C~ueTTF-km~KaKhIQBIzJ0LCvzSPsw0QosjEg8-17sZpZOR6GjKA~DOKN6~5Z9lTRbk9OJ-cWOaGMy2RaWLXr8CABqC5gmAZ-OXaZfIjeUJVmtweTaFtlddptI2FvdgHJtA86OA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
82. Vayansky, I., Kumar, S. (2018), Phishing – challenges and solutions, Computer Fraud & Security.
83. Verheijen, L. (2013), The Effects of Text Messaging and Instant Messaging on Literacy, *English Studies,* 94(5), 582-602, Routledge. Dostupno na: https://www.researchgate.net/profile/Lieke-Verheijen/publication/256507070_The_Effects_of_Text_Messaging_and_Instant_Mes

saging_on_Literacy/links/5ccc03a392851c3c2f81b2a2/The-Effects-of-Text-Messaging-and-Instant-Messaging-on-Literacy.pdf
84. Volkamer, M., Sasse, M. A., Boehm, F. (2020), Analysing Simulated Phishing Campaings for Staff. Dostupno na: https://d1wqtxts1xzle7.cloudfront.net/81922402/102846833-libre.pdf?1646816244=&response-content-disposition=inline%3B+filename%3DAnalysing_Simulated_Phishing_Campaigns_f.pdf&Expires=1693313248&Signature=SmRzsdav5HJhX1GEZEtdYY9OCyPjm-t1J1-N0u5D5r1NV6bet7uTspNmhCyb2nYTl3sqYxBX-GCGMUWuuqkWCGGE~qbj0KxCVAkGiPxQHHi-Rk~yt5kgUJkk2XOdmImK0gXffe1pcXB-e~O019t1x04DAjW3In0Qo6LnFMpLk-9e2lPkRYeLwcAFw6X~RvA9LxpVihnXTl6uI8W0bsG4DPDe5LskWqXwn2HE16rDPY~quTn9sPEoTFmVvue4TESiDmuexFbByLn3YiABn76MUI7FkjIxS8XGbDcMnBxsS25fBUKaP71Jeu~8lgui9d8OWwWKy7X462BumjQSw0-08Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
85. Whitman M. E., Mattord, H. J. (2021), Principles of Information Security, sedmo izdanje, Cengage
86. Whittaker, C., Ryner, B., Nazif, M. (2010), Large-Scale Automatic Classification of Phishing Pages. Dostupno na: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/35580.pdf

8. POPIS SLIKA

9. ŽIVOTOPIS

Dominik Starček rođen je 27. srpnja 1994. godine u gradu Zagrebu gdje završava svoje osnovnoškolsko i srednjoškolsko obrazovanje. Godine 2016./2017. upisuje Integrirani studij poslovne ekonomije na Ekonomskom fakultetu u Zagrebu, gdje na višim godinama odlučuje upisati smjer Menadžerska informatika. 2019. godine zapošljava se u Photomathu kao anotator i verifikator matematičkih podataka i s vremenom postaje mentor novim studentima u timu. Aktivno se služi hrvatskim i engleskim, a pasivno talijanskim jezikom.