Korisnik kao najslabija karika sigurnosti računalne mreže

Barišić, Jakov

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET TURIZMA I RURALNOG RAZVOJA U POŽEGI

STUDENT: Jakov Barišić, JMBAG: 0253054510

KORISNIK KAO NAJSLABIJA KARIKA SIGURNOSTI RAČUNALNE MREŽE

ZAVRŠNI RAD

Požega, 2024. godine.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET TURIZMA I RURALNOG RAZVOJA U POŽEGI

PRIJEDIPLOMSKI STUDIJ ELEKTRONIČKO POSLOVANJE I PROGRAMSKO INŽENJERSTVO

KORISNIK KAO NAJSLABIJA KARIKA SIGURNOSTI RAČUNALNE MREŽE

ZAVRŠNI RAD

MENTOR: izv. prof. dr. sc. Krešimir Šolić

STUDENT: Jakov Barišić

JMBAG studenta: 0253054510

Požega, 2024. godine

SAŽETAK

Ovaj rad analizira korisnika kao ključni element internetske sigurnosti, a zapravo vrlo često kao i najslabiju kariku u obrani od prijetnji kibernetičkih napada. Pruža definicije internetske i kibernetičke sigurnosti i popise prijetnji kao što su: virusi, zlonamjerni softver, krađa identiteta, ransomware. Bavi se ljudskim faktorima, kao što su naivnost, nemar i nesvjesnost, koji mogu rezultirati sigurnosnim incidentima te raspravlja njihov stvarni utjecaj na tvrtke. Istražuje ponašanja korisnika koja povećavaju rizik, poput neispravnih lozinki i otkrivanja osobnih podataka, te preporučuje formalne obrazovne programe za smanjenje tih rizika. Opširno se raspravlja o tehničkim rješenjima koja se tiču antivirusnih programa, vatrozida i višefaktorske provjere autentičnosti, ali naglašava važnost i potrebu za informiranim korisničkim praksama. Konačno, daje praktične savjete o sigurnijem digitalnom ponašanju u zaštiti osobnih i poslovnih podataka.

Ključne riječi: Antivirusi, Internetska sigurnost, Kibernetička sigurnost, Obrazovni programi, Zaštita podataka

SUMMARY

This paper analyzes the user as a key element of internet security, and quite often as the weakest link in defending against the threats of cyberattacks. It provides definitions of internet and cyber security, along with a list of threats such as viruses, malware, identity theft, and ransomware. It addresses human factors such as naivety, negligence, and unawareness, which can result in security incidents, and analyzes their real impact on companies. It explores user behaviors that increase risk, such as weak passwords and the disclosure of personal data, and recommends formal educational programs to reduce these risks. The paper extensively discusses technical solutions related to antivirus programs, firewalls, and multi-factor authentication, but emphasizes the importance and necessity of informed user practices. Finally, it offers practical advice on safer digital behavior in protecting personal and business data.

Keywords: Antivirus, Internet security,Cybersecurity. Educational programs, Data protection

SADRŽAJ

1. UVOD

U današnje vrijeme gotovo sve u našim životima vezano je uz internet. Ljudi koriste Internet za razmjenu informacija, komunikaciju, kupnju, zabavu, rad i tako dalje. S obzirom da se digitalne tehnologije brzo i široko razvijaju, pitanja zaštite osobnih podataka i kibernetičke sigurnosti vrlo su aktualna. Koje god sigurnosne komponente mrežne infrastrukture organizacije bile implementirane (pa čak i napredniji alati!) ne postoji potpuna zaštita. Računalna mreža spojena na internet, bez obzira na to koliko su sofisticirane sigurnosne mjere korištene, može biti napadnuta. U radu se govori o važnosti korisnika u održavanju sigurnosti računalne mreže spojene na internet, te o tome kako informirati i educirati korisnike o sigurnosnim prijetnjama. Također naglašava opće sigurnosne prijetnje koje proizlaze iz ljudskih faktora i daje pragmatične preporuke koje bi pomogle u smanjenju povezanih rizika. U sklopu ovog završnog rada provedeno je ispitivanje korisnika kroz anketu ,a rezultati analize dali su uvid u razinu svijesti o sigurnosnim prijetnjama, što ukazuje na potrebu daljnje edukacije za bolje razumijevanje sigurnosnih mjera.

2. OSNOVE INTERNETSKE SIGURNOSTI

Internetska sigurnost nije samo stari skup mjera i postupaka koji se koriste za zaštitu računala, mreža, programa ili podataka od neovlaštenog pristupa; također uključuje zaštitu, krađu ili oštećenje kao i napade na informacije putem interneta. Takva vrsta sigurnosti je skup svih metoda koje se brinu da korisnički podaci budu sigurni tijekom prijenosa mrežama, uključujući identitete korisnika i druge važne informacije. Internetska sigurnost vrlo je ključna u sprečavanju gubitka podataka i gubitaka povezanih s narušavanjem privatnosti i financijskih gubitaka: ovo se jednako odnosi na korporativne infrastrukture ili mala poduzeća koja koriste (ili se oslanjaju na) internet za osobnu upotrebu. Mogu postojati antivirusni programi koji se koriste kao jedan od načina osiguravanja sigurnosti sustava ili mreže protiv potencijalnih ranjivosti - ali to također mogu biti vatrozidi plus enkripcija podataka zajedno s autentifikacijom. Osim tehničkih rješenja, u pojam 'internetska sigurnost' ulazi i svijest korisnika o prijetnjama, kao i edukacija o problemima te razvoj vještina za rješavanje sigurnosnih problema (Dangubić, I. 2019).

2.1. Razlika između internetske sigurnosti i kibernetičke sigurnosti

Iako se internetska sigurnost i kibernetička sigurnost koriste naizmjenično, razlikuju se. Internetska sigurnost koncentrira se na zaštitu podataka i aktivnosti koje se odvijaju putem Interneta; odnosno zaštita korisničkih računa te transakcija i bilo kakvih komunikacija putem interneta. S druge strane, kibernetička sigurnost ima širi opseg. Odnosi se na zaštitu svih digitalnih podataka i infrastruktura bez obzira jesu li povezani na internet ili ne. Kibernetička sigurnost odnosi se na zaštitu računalnih sustava mreža, programa kao i podataka od digitalnih napada bez obzira na to prenose li se ti napadi putem interneta ili čak unutar lokalne mreže. Stoga tamo gdje se internetska sigurnost usredotočuje na prijetnje koje dolaze sa samog interneta, kibernetička sigurnost pokriva sve oblike digitalne sigurnosti uključujući fizičke aspekte poput sigurnosti podatkovnog centra (Rudeš, I. i Pavelić, I. 2023).

Internet je postao mjesto brojnih sigurnosnih prijetnji koje mogu utjecati na privatnost i sigurnost korisnika. Neke od najčešćih prijetnji uključuju: viruse, *malware, ransomware*

Virusi su zlonamjerni programi koji se lako mogu širiti s jednog računala na drugo, obično putem zaraženih datoteka ili privitaka e-pošte. Nakon što virus uđe u računalo, može

rezultirati različitim oblicima oštećenja, od usporavanja sustava do uništavanja podataka. Virusima je često potreban neki oblik ljudske radnje kako bi se pomoglo njihovom širenju, poput otvaranja zaraženih privitaka ili preuzimanja sumnjivih datoteka s interneta

Malware skraćeno od "*malicious software*" je zlonamjerni software koji uključuje viruse, trojance, spyware i adware. Zlonamjerni programi imaju za cilj oštećivanje ili preuzimanje kontrole nad računalnim uređajima, krađu podataka ili promatranje aktivnosti korisnika. Obično se vrlo suptilno instalira bez znanja korisnika kada se otvore zaražene web stranice, e-pošta ili preuzete aplikacije (Dangubić, I. 2019).

Metoda prijevare u kojoj se korisnike suptilno pokušava natjerati da otkriju privatne podatke uključujući šifre i brojeve kreditnih kartica. Obično se to postiže slanjem lažnih e-poruka ili stvaranjem lažnih web stranica koje izgledaju kao stvarne. Napadi krađe identiteta temelje se na psihologiji, a namjera im je prevariti korisnika da pomisli da razgovara s organizacijom ili pojedincem od povjerenja.

Ransomware je vrsta zlonamjernog softvera koji vam ne dopušta korištenje računalnog sustava. Kada *ransomware* inficira računalo, može kriptirati datoteke ili zaustaviti upotrebu prikazivanjem početnog zaslona na kojem se neka poruka trajno prikazuje i ne može se ukloniti. Napadi ransomwarea obično su žrtve tvrtki i organizacija; korisnicima daju poruku s uputama za plaćanje otkupnine (u većini slučajeva u kriptovalutama) kako bi nakon uplate korisnici dobili svoje podatke natrag. *(Ransomware and phishing cyberattacks*. 2022)

Slika 1 - Primjer ransomware napada

Prilagođeno prema: https://www.varonis.com/blog/cryptolocker

Osnove internetske sigurnosti dotiču se različitih aspekata zaštite korisnika i podataka od golemog prostora kakav je internet. To znači da je jasno razumijevanje temeljnih prijetnji kao što su virusi, malware, phishing i ransomware vrlo važno kada se osmišljavaju odgovarajuće sigurnosne mjere. Dok tehnička rješenja obavljaju stvarni posao, svijest o prijetnjama i educiranost o sigurnosnim praksama uvelike pomažu pojedincima da se zaštite.

3. KORISNIK KAO NAJSLABIJA KARIKA

U kontekstu internetske sigurnosti, korisnik je svaka osoba koja koristi računalni sustav, mrežu ili aplikaciju. Korisnici mogu biti pojedinci - koji koriste osobna računala za obavljanje svojih dnevnih aktivnosti (npr. pregledavanje interneta, slanje e-pošte, online kupnja) ili zaposlenici unutar organizacija - koji koriste poslovne mreže i sustave za obavljanje svojih radnih zadataka. Unatoč ulozi, svi korisnici imaju pristup određenim informacijama i resursima te su stoga i potencijalne mete sigurnosnih prijetnji, uključujući one da su korisnici odgovorni za sigurnost svojih aktivnosti na internetu i time mogu pridonijeti ili narušiti sigurnosno ponašanje. Njihova svijest o sigurnosnim prijetnjama, poznavanje ispravnih postupaka, način na koji reagiraju na sumnjive situacije kritični su u smislu održavanja ne samo osobne već i zajedničke mrežne sigurnosti.(Conry-Murray A i Weafer V).

3.1. Zašto su korisnici najslabija karika?

Iako su sigurnosne mjere i tehnologije bolje nego ikad, korisnici će uvijek biti najslabija karika sigurnosti iz nekoliko razloga: Ljudska greška, nedostatak svijesti, psihološka manipulacija, preopterećenost informacijama, otpor prema promjenama i novim tehnologijama, lažan osjećaj sigurnosti.

Ljudska greška:bilo da se radi o nemaru, bilo o neznanju, bilo o neiskustvu što može dovesti do ljudske pogreške nesvjesnim otvaranjem zlonamjernih privitaka, klikanjem na zlonamjerne poveznice ili dijeljenjem osjetljivih informacija s nepouzdanim izvorima. Takve ranjivosti napadači mogu iskoristiti za pristup računalnim sustavima ili podacima.

Nedostatak svijesti o sigurnosnim prijetnjama: Mnogi korisnici nisu upoznati s rizicima koji su tipični za moderna vremena ili koliko bi ti rizici mogli biti. To može dovesti do toga da korisnici ne prepoznaju potencijalne indikatore povezane sa shemama krađe identiteta, lažnim web stranicama ili drugim vrstama prijevare.

Psihološka manipulacija: Napadači koriste društveni inženjering često iskorištavajući povjerenje ili emocije u reakcijama svojih žrtava. Na primjer, slanje phishing e-pošte postiže se lažnim predstavljanjem legitimnih organizacija i upotrebom hitnih poruka kako bi se korisnici natjerali na radnje koje inače ne bi bile poduzete.

Preopterećenost informacijama: U današnje vrijeme korisnici su zatrpani informacijama i zadacima na štetu svoje pažnje, što posljedično stvara umor. U takvim okolnostima postoji

veća vjerojatnost da će korisnik zanemariti sigurnosna upozorenja ili poduzeti radnje bez kritičke analize ishoda.

Otpor prema promjenama i novim tehnologijama: Neki od korisnika ne žele mijenjati svoje navike ili ne žele koristiti nove tehnologije, čak i ako su te tehnologije sigurnije. Na primjer, korisnici bi mogli izbjegavati korištenje multifaktorske provjere autentičnosti jer smatraju da je pretjerana(nemaju volje) to bi smanjilo razinu sigurnosti njihovih računa.

Lažan osjećaj sigurnosti: Korisnici često imaju antivirusni program ili druge zaštitne mjere koje im daju lažan osjećaj sigurnosti. Iako su važni sami po sebi, nisu dovoljni ako korisnici pažljivo ne slijede sigurne prakse i ne budu oprezni.

Korisnici su ključni faktor u održavanju sigurnosti internetske mreže, ali su ujedno i najslabija karika zbog sklonosti ljudskim pogreškama, nedostatka svijesti i psihološke manipulacije. Edukacija korisnika i njihova suradnja s tehničkim sigurnosnim mjerama od vitalnog su značaja za stvaranje sigurnijeg internetskog okruženja. Razumijevanje ovih izazova može pomoći u razvoju učinkovitijih strategija za zaštitu podataka i smanjenje rizika od sigurnosnih incidenata. (IT sigurnost - zašto smo sami svoj najveći neprijatelj? (2022.))

4. LJUDSKI FAKTOR U SIGURNOSNIM PRIJETNJAMA

Ljudski faktor je ključni akter u mnogim sigurnosnim incidentima. Varijable stavova ,naivnosti, nemara i nesvjesnosti sigurnosnih prijetnji čine korisnika podložnijim napadima i često aktiviraju situaciju u kojoj korisnik nenamjerno postaje meta zlonamjernosti.

1. Naivnost: mnogi korisnici koji ne znaju vjeruju da na internetu postoje rizici. Imaju vrlo nevino uvjerenje da se "sigurnosni problemi događaju drugima" ili "dovoljno sam zaštićen" stav i to ih navodi na otvaranje e-pošte od nepoznatih pošiljatelja, preuzimanje datoteka iz nesigurnih izvora ili upisivanje osobnih podataka na lažne web stranice .
2. Nepažnja: Pažnja korisnika sve je manja zbog tempa modernog života i stalne internetske povezanosti. Većina korisnika neće stati i razmišljati o riziku kada intenzivno koriste internet u svakodnevnom životu. Nedostatak pažnje se, između ostalog, pokazuje klikanjem na sumnjive linkove ili korištenjem jedne lozinke za više računa ili ignoriranjem sigurnosnih upozorenja.
3. Nedostatak svijesti: Mnogi korisnici nemaju odgovarajuće obrazovanje o trenutnim sigurnosnim prijetnjama i najboljim praksama za zaštitu na internetu. Nedostatak svijesti ih čini lakim metama cyber kriminalaca u njihovim djelima kao što su phishing napadi, širenje zlonamjernog softvera i slično. U većini slučajeva, kada korisnici nemaju dovoljno znanja, teško razumiju znakove koje trebaju tražiti ili kako reagirati u slučaju sigurnosnih incidenata. Iz tih je razloga edukacija korisnika od najveće važnosti kako bi se njegovala kultura znanja o sigurnosti. (Sigurnost na Internetu: Najnovije prijetnje i kako se zaštititi?) (Sigurnost na internetu: Neosvještenost korisnika najveći rizik)

4.1. Primjeri stvarnih incidenata uzrokovanih ljudskim greškama

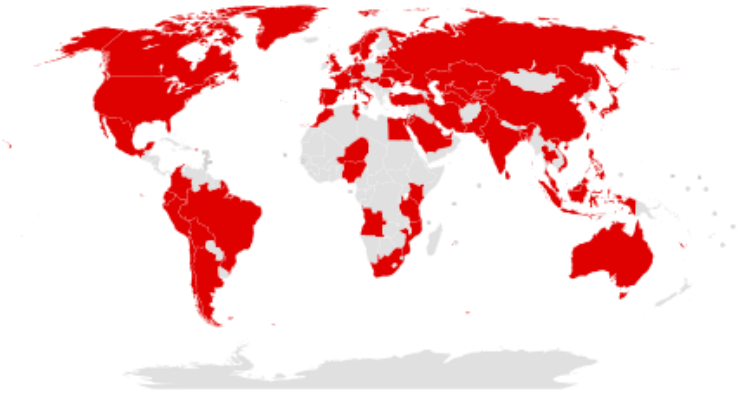
Stvarni incidenti uzrokovani ljudskim greškama ilustriraju koliko lako ljudski faktor može ugroziti sigurnost. Neki od najpoznatijih primjera uključuju:

1. Phishing napad na Sony Pictures (2014.): Jedan veliki slučaj bio je cyber napad na Sony Pictures 2014., pri čemu su napadači ukrali veliku količinu podataka, uključujući e-poruke, od kojih su neke bile osjetljive, i skripte, kao i osobne podatke o zaposlenicima. U ovom slučaju, napadači su koristili phishing e-poštu kako bi namamili zaposlenike da otvore privitke koji su bili zaraženi zlonamjernim softverom i omogućili napadačima

pristup internim sustavima tvrtke. Klikom na zlonamjerne veze od strane ljudskih bića napadači su mogli prouzročiti ogromnu štetu. *(From Breach to Fallout: The Story of the 2014 Sony Hack)*

2. WannaCry ransomware napad (2017.): U 2017. napad ransomwareom WannaCry proširio se na stotine tisuća računala diljem svijeta, uz mnoga izvješća o pogođenim bolnicama, tvrtkama i vladinim organizacijama. Iako je ovaj napad iskorištavao puku ranjivost u softveru, ipak je mnogo toga ovisilo o ljudskom elementu. Puno korisnika nije ažuriralo svoje sustave u vrijeme kada su bile dostupne zakrpe zbog čega se ovaj ransomware proširio poput epidemije. Druga točka su oni korisnici koji su pomogli u širenju napada klikom na zlonamjerne poveznice ili privitke. *(Ransomware and phishing cyberattacks* 2022)

Slika 2 - Karta zemalja koje su prvotno pogođene



Prilagođeno prema: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

3. Incident s lažnim e-mailom u tvrtki Ubiquiti (2015.): U 2015. tehnološka tvrtka Ubiquiti bila je žrtva phishing napada e-poštom u iznosu od preko 46 milijuna dolara u slučaju poznatom kao "prijevara izvršnog direktora". Napadači su slali e-poruke koje su izgledale kao da su od višeg vodstva unutar tvrtke tražeći trenutni prijenos novca. Nedostatak potvrde i svijesti zaposlenika o tim prijevarama doveo je do njihovih premještaja i, zauzvrat, velikih financijskih gubitaka. (*Tech Firm Ubiquiti Suffers $46M Cyberheist*)

4.2. Utjecaj ljudskih grešaka na tvrtke i organizacije

Ljudske greške mogu imati ozbiljan utjecaj na tvrtke i organizacije, uključujući financijske gubitke, štetu reputaciji i povredu povjerenja kupaca. Neke od glavnih posljedica uključuju: financijske gubitke, štetu reputaciji, pravni i regulatorni problemi, gubitak intelektualnog vlasništva.

1. Financijski gubici: Kao što su pokazali primjeri incidenata, ljudske greške mogu dovesti do značajnih financijskih gubitaka. Bilo da se radi o krađi podataka, plaćanju otkupnine zbog ransomwarea ili gubitku novca putem lažnih transakcija, troškovi mogu biti ogromni. Osim direktnih financijskih gubitaka, tvrtke mogu pretrpjeti i dodatne troškove za obnavljanje sigurnosnih sustava, pravne troškove i troškove oporavka. Jedan takav primjer događao se od početka 2014. korisnici internetskog bankarstva u Hrvatskoj bili su meta cyber kriminalaca koji su uspjeli ukrasti oko 1,8 milijuna kuna. Napadi su prijavljeni Hrvatskoj narodnoj banci (HNB), kojoj su sve banke u Hrvatskoj obvezne prijaviti značajnije sigurnosne incidente. Dejana Rebernik iz HNB-a navodi da je intenzitet napada sada značajno smanjen, a žarište napada preusmjereno na druge zemlje Europske unije. Ministarstvo unutarnjih poslova radi na otkrivanju identiteta kriminalaca i povratu novca. Hrvatska, poznata po vrhunskim stručnjacima za digitalnu forenziku, aktivno radi na jačanju sigurnosti IT sustava banaka kako bi spriječila buduće napade (Ivezić, B. 2014).

2. Šteta reputaciji: Kada tvrtka postane žrtva sigurnosnog incidenta, njezina reputacija može biti ozbiljno narušena. Kupci i poslovni partneri gube povjerenje u tvrtku, što može rezultirati gubitkom klijenata i poslovnih prilika. Oporavak reputacije može biti dugotrajan proces, a neki se klijenti možda nikada neće vratiti.

3. Pravni i regulatorni problemi: Ovisno o vrsti podataka koji su ugroženi, tvrtke mogu biti suočene s pravnim posljedicama i kaznama zbog kršenja zakona o zaštiti podataka. Mnoge zemlje imaju stroge zakone koji zahtijevaju zaštitu osobnih podataka, a nepoštivanje tih zakona može rezultirati visokim kaznama i pravnim sankcijama.

4. Gubitak intelektualnog vlasništva: U slučajevima kada su napadači ciljali poslovne tajne ili intelektualno vlasništvo, tvrtke mogu pretrpjeti gubitke koji imaju dugoročne posljedice. Krađa osjetljivih podataka može dovesti do gubitka konkurentske prednosti, smanjenja prihoda i narušavanja inovacijskog kapaciteta tvrtke.

Ljudski faktor igra ključnu ulogu u sigurnosnim prijetnjama i često je izvor ranjivosti u internetskoj sigurnosti. Naivnost, nepažnja i nedostatak svijesti čine korisnike podložnima napadima, što može dovesti do ozbiljnih incidenata s dalekosežnim posljedicama. Tvrtke i organizacije moraju ulagati u edukaciju korisnika, podizanje svijesti i usvajanje sigurnosnih praksi kako bi smanjile rizik od ljudskih grešaka i osigurale sigurnost svojih podataka i resursa. (*Factors Affecting Reputational Damage to Organisations Due to Cyberattacks*)

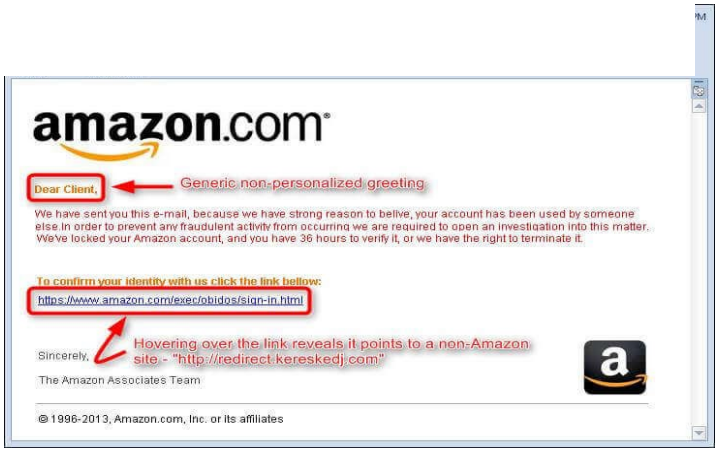
5. NAJČEŠĆE SIGURNOSNE PRIJETNJE UZROKOVANE KORISNIČKIM PONAŠANJEM

Radnje korisnika često su glavni čimbenici sigurnosnih prijetnji na mreži. Bez obzira na to koliko su sofisticirane zaštitne tehnologije, ljudi sami mogu otvoriti vrata lošim akterima da ih koriste. Tri najčešće prijetnje koje proizlaze iz ponašanja korisnika su društvene: phishing i socijalni inženjering, usvajanje slabih lozinki i izazovi autentifikacije te otkrivanje osobnih podataka na mreži.

5.1. Phishing i socijalni inženjering

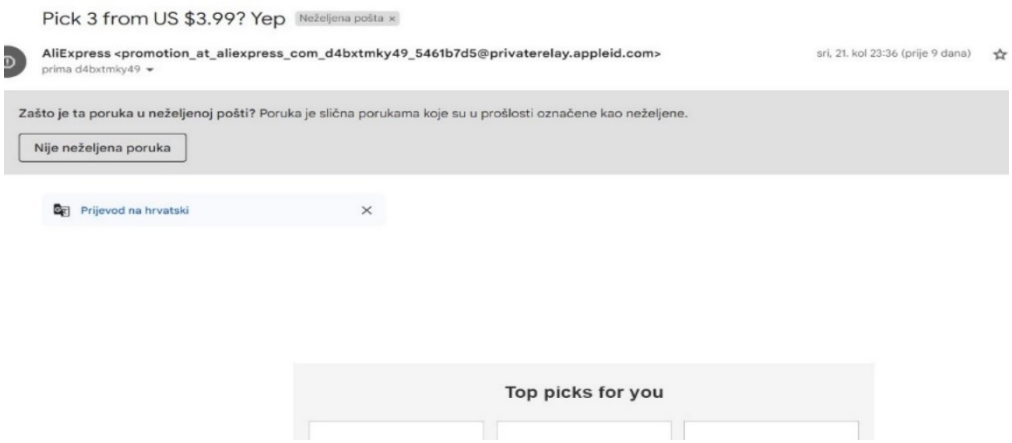
To je lažna e-pošta, poruka ili lažna web stranica koja se koristi za dobivanje osobnih podataka, lozinki i financijskih informacija od korisnika na prijevaran način. Društveni inženjering često ide na ruku hakerima jer zavaravaju korisnike da misle da su u interakciji s legitimnim tvrtkama; kao što su banke, internetske usluge ili čak vlastiti poslodavci.
Tehnike krađe identiteta: Obično se napadi krađe identiteta kreiraju da izgledaju autentično; odnosno koriste se logotipi i dizajni poznatih tvrtki. Tekst poruke obično stvara osjećaj hitnosti prijeteći korisniku obustavom računa ili gubitkom pristupa u porukama u kojima se tvrdi da korisnici moraju poduzeti hitnu radnju. Nakon toga se zapravo usmjeravaju na lažne stranice putem ugrađenih hiperveza ili se od njih traži da preuzmu zlonamjerne privitke. (Vukelić, B., Zvonarić, A.D. i Protrka, N. 2023)

Slika 3. Amazon phishing



Prilagođeno prema: https://www.kxan.com/news/amazon-shoppers-targeted-in-order-cannot-be-shipped-scam/

Slika 4. AliExpress Phishing



(Izvor:Autor)

Socijalni inženjering**:** Ova manipulacija ljudskom psihologijom potiče dijeljenje tajnih informacija od strane korisnika. Na primjer, napadači se mogu pretvarati da su kolege ili nadređeni i tražiti osjetljive podatke. Također mogu koristiti druge psihološke taktike kao što su komplimenti, prijetnje ili emocionalne igre kako bi dobili ono što žele.

Primjeri napada: Phishing napadi toliko su napredovali da ih čak ni iskusni korisnici ne mogu razlikovati. Primjer takvog napada je kada korisnik primi e-poštu od svoje banke i od njega se traži da ažurira podatke klikom na poveznicu. Naravno, to onda vodi do lažne web stranice koja prikuplja korisničke podatke.

Prevencija: Edukacija korisnika je ključna u prevenciji phisinga. Korisnici bi trebali biti dobro informirani o tome kako otkriti e-poštu koja je vjerojatno sumnjiva, izbjeći klikanje na poveznice u neželjenoj e-pošti i uvijek potvrditi da zahtjevi za osobnim podacima dolaze službenim kanalima.

5.2. Slaba lozinka i problemi s autentifikacijom

Korištenje slabih lozinki i nepravilna autentifikacija je, prema ponašanju korisnika, jedna od najčešćih sigurnosnih prijetnji. U početku lozinke djeluju kao početna linija obrane za zaštitu neovlaštenog pristupa. Slabe lozinke: Mnogi korisnici još uvijek koriste osnovne lozinke kao što su datum rođenja, ime ili informacije koje su ljudima lako dostupne i koje često dijele (ime njihovog ljubimca). Takve se lozinke lako pogađaju ili provaljuju, primjerice, *brute force* napadom (napad u kojem napadač koristi programe koji isprobavaju tisuće mogućih kombinacija — postoji nekoliko vrsta *brute force* napada). Jedan od razloga za korištenje slabih zaporki

je koliko su jednostavne i budući da ih je lako zapamtiti, ova praksa uvelike smanjuje sigurnost korisničkih računa. Ponovno korištenje lozinke: Još jedna uobičajena praksa je ponovno korištenje iste lozinke na različitim računima. Drugim riječima, ako haker uspije probiti zaporku za jedan račun, onda može uletjeti ravno u nekoliko drugih korisničkih računa. Ovo dramatično povećava sigurnosne rizike incidenata, posebno u slučaju kada krajnji korisnik primjenjuje identičnu lozinku za svoj poslovni i osobni račun. (*Specops Software* 2023)

Nedostatak višefaktorske autentifikacije (MFA): Iako mnoge usluge nude višefaktorsku provjeru autentičnosti kao opciju za poboljšanje sigurnosti, mnogi je korisnici ne omogućuju. Višefaktorska provjera autentičnosti zahtijevat će dodatni korak potvrde putem koda poslanog na mobitel, čime će sigurnost biti visoka čak i ako je lozinka kompromitirana.

Primjeri napada: Probijanje lozinki jedan je od najčešćih načina napada na korisničke račune.
Primjer koji je postao poznat je napad na LinkedIn 2012. godine kada su hakeri, zbog slabe enkripcije lozinki i loše sigurnosne prakse za korisnike, ukrali lozinke preko 6,5 milijuna korisnika. Prevencija: Korištenje snažne šifre i kombinacije slova, brojeva i posebnih znakova. Također, gdje je to moguće, korisnici bi trebali aktivirati multifaktore kako bi zaštitili svoje račune. Upravitelj zaporki može pomoći u generiranju i pohranjivanju jakih zaporki. (2012 Linkedin)

5.3. Otkrivanje privatnih podataka na internetu

Otkrivanje privatnih podataka na internetu, bilo svjesno ili nesvjesno, može dovesti do ozbiljnih sigurnosnih prijetnji. Korisnici često ne shvaćaju kako se informacije koje dijele na društvenim mrežama i drugim online platformama mogu iskoristiti protiv njih.

1. Dijeljenje osobnih informacija: 1. Dijeljenje osobnih podataka: Mnogi korisnici dijele svoj datum rođenja, adresu, broj telefona ili čak financijske podatke na društvenim mrežama. Iako takvo dijeljenje izgleda bezopasno, napadači mogu iskoristiti ove informacije za krađu identiteta ili kao dio društvenog inženjeringa za daljnje napade.

2. Korištenje javnih Wi-Fi mreža: Pristupanje osjetljivim podacima ili unos lozinki putem nezaštićenih javnih Wi-Fi mreža može omogućiti napadačima da presretnu komunikaciju i pristupe osjetljivim informacijama. Mnogi korisnici nisu svjesni rizika povezivanja na javne mreže bez upotrebe VPN-a (virtualne privatne mreže).
3. Otkrivanje informacija u poslovnim okruženjima: Ono što se događa većinu vremena je da zaposlenici nenamjerno otkrivaju ono što bi trebale biti povjerljive informacije o tvrtki na internetu, na društvenim mrežama, profesionalnim forumima ili nešifriranoj korporativnoj e-pošti. Takve radnje mogu rezultirati curenjem tajnih podataka napada ili omogućiti napadačima ulazak u organizacijske mreže.
4. Primjeri prijetnji: Čest primjer je curenje informacija putem društvenih mreža, gdje su napadači prikupljali informacije o zaposlenicima tvrtke kako bi ih koristili za ciljanje phishing napada. Također, u mnogim slučajevima korisnici su žrtve krađe identiteta jer napadači koriste informacije koje su pronašli na društvenim mrežama za stvaranje lažnih profila ili računa.
5. Prevencija: Korisnici trebaju razumjeti što dijele i čine dostupnim putem interneta u vezi sa svojim osobnim podacima na društvenim mrežama. To se može učiniti tako da se ono što bi trebalo biti privatno ne objavi javno i smanji količina informacija koje se dijele s takvim stranicama. Stoga se treba suzdržati od dijeljenja osobnih podataka preko javnih Wi-Fi mreža ili ako koristimo javni Wi-Fi treba koristiti i VPN. (*Public Wi-Fi: An ultimate guide on the risks + how to stay safe*) (*Ways to protect your personal information online*)

6. EDUKACIJA I PODIZANJE SVIJESTI

Ljudski faktor igra ključnu ulogu u održavanju internetske sigurnosti. Ovo naglašava važnost uključivanja obrazovanja i svijesti korisnika kao jednog od najvažnijih koraka prema smanjenju sigurnosnih rizika. Nakon edukacije korisnici će moći prepoznati prijetnje, razumjeti kako odgovoriti na moguće napade i implementirati najbolju zaštitu svojih podataka. Edukacija je, međutim, osnovni alat u smanjenju rizika od sigurnosnih prijetnji jer omogućuje korisnicima da upoznaju rizik na internetu i kako se mogu zaštititi.

6.1. Uloga edukacije u smanjenju rizika

Edukacija je osnovni alat za smanjenje rizika od sigurnosnih prijetnji prijetnji jer omogućuje korisnicima da upoznaju rizik na internetu i kako se mogu zaštititi. Neke od ključnih uloga uključuju:

1. Povećanje svijesti o prijetnjama: obrazovanje pomaže u prepoznavanju raznih prijetnji uključujući phishing, malware, ransomware i druge oblike kibernetičkog kriminala. Programi o obrazovanju tjeraju korisnike da budu oprezni u pogledu mogućih opasnosti i načina na koji te opasnosti nastaju.

2. Osposobljavanje za prepoznavanje sumnjivih aktivnosti: ovo će povećati vjerojatnost da će korisnici uočiti sumnjivu e-poštu, poveznice ili privitke. Na primjer, provjerite adresu pošiljatelja, pregledajte URL tako da prijeđete pokazivačem iznad vrha veze prije klika i prepoznajte indikatore napada društvenog inženjeringa.

3. Razvijanje sigurnosnih navika: To uključuje obrazovanje i usvajanje sigurnosnih navika od strane korisnika kao što su; korištenje jakih lozinki, redovito ažuriranje softvera i korištenje višestruke provjere autentičnosti kao i učenje o važnosti sigurnosnih kopija i zaštite osjetljivih podataka.

4. Smanjenje ljudskih grešaka: Jedan veliki dio sigurnosnih incidenata rezultat je ljudske pogreške. Obrazovanje može ograničiti takva djela nepažnje minimizirajući ih, osiguravajući izraženo razumijevanje sigurnosnih procedura i uvažavajući implikacije neodgovornog ponašanja na internetu.

5. Jačanje otpornosti organizacija: Kada su zaposlenici educirani i svjesni sigurnosnih prijetnji, cijela je organizacija otpornija na napade. Smanjuje se rizik od sigurnosnih incidenata i, prema tome, potencijalne financijske gubitke, narušavanje ugleda kao i pravne probleme. (*The Importance of Cybersecurity Awareness, Training, and Education*)

6.2 . Programi edukacije i treninzi za korisnike

Obrazovanje o sigurnosti na internetu može se provoditi na različite načine. Programi se također mogu prilagoditi prema specifičnim potrebama korisnika ili organizacije. Neki od najčešćih oblika obrazovanja su:

1. Online tečajevi i webinari: Opisujući jedan od najpristupačnijih oblika obrazovanja, online tečajevi i webinari pokrivaju teme vezane uz internetsku sigurnost. Oni mogu biti dostupni široj javnosti ili određenim skupinama korisnika. Primjeri tema: prepoznavanje phishing napada, sigurno korištenje društvenih mreža, upravljanje lozinkama i zaštita privatnosti na internetu.

2. Praktični treninzi i simulacije: Ovo je mjesto gdje guma pogađa cestu u aktualiziranju onoga što je naučeno iz teoretskog sadržaja. Na primjer, simulirani phishing napadi omogućuju testiranje reakcija korisnika na različite veze i daju im povratne informacije o tome kako prepoznati ili izbjeći sumnjive e-poruke. Ovo pomaže korisnicima da se osjećaju sigurnije u svoju sposobnost prepoznavanja prijetnji i odgovora na njih.

3. Radionice i seminari: Sigurnosne radionice i seminari ustupaju mjesto učenju na zahtjev. To polazniku omogućuje da izrazi svoje brige, uključi se u razgovor i izvuče pouke iz iskustava drugih na primjerima iz stvarnog svijeta. Tvrtke, škole ili društvene organizacije mogu ugostiti ove događaje koji su vrlo relevantni za potrebe sudionika..

4. Sigurnosne kampanje: Organizacije mogu provoditi sigurnosne kampanje koje uključuju informativne materijale, plakate, e-mail obavijesti i druge oblike komunikacije kako bi podigli svijest o sigurnosnim prijetnjama. Kampanje mogu biti usmjerene na specifične prijetnje ili općenito promovirati dobre sigurnosne prakse.

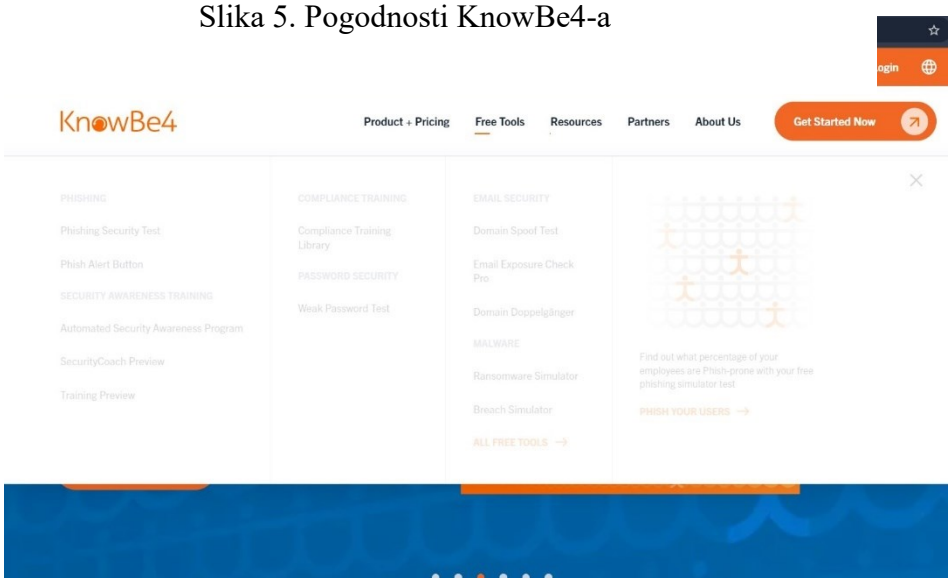
5. Sigurnosne politike i procedure: Edukacija o internetskoj sigurnosti trebala bi adekvatno podržati obrazovanje o sigurnosti na internetu s jasnim sigurnosnim politikama i procedurama unutar organizacija. Korisnici će biti obaviješteni o pravilima u sferi korištenja

internetskih resursa, pravilima o lozinkama, te o proceduri prijave sumnjivih radnji i postupku u slučaju sigurnosnih incidenata. *(Zero Trust Security*)

Mnoge tvrtke i organizacije prepoznale su važnost edukacije i podizanja svijesti te su implementirale inovativne programe sigurnosne edukacije. Neki od primjera dobre prakse uključuju:

1. Google's Phishing Quiz: online i sposoban kviz za borbu protiv različitih vrsta phishing napada koje je razvio Google. Uključuje stvarnu simulaciju phishing e-pošte i na kraju korisnicima daje povratnu informaciju o njihovim odgovorima, govoreći im na što trebaju pripaziti kako ne bi postali žrtve prevaranata. Takvi su kvizovi vrlo zgodni u njegovanju vaše svijesti i jačanju vas u prepoznavanju prijevare kada ju vidite. (*Can you spot when you're being phished?*)
2. Microsoft Cybersecurity Awareness Program**:** Microsoftova globalna obrazovna inicijativa o kibernetičkoj sigurnosti za svoje zaposlenike i klijente. To uključuje e-tečajeve, sigurnosne kampanje, resurse o prijetnjama i njihovoj identifikaciji te alate za procjenu znanja o sigurnosti. Microsoft također nudi obrazovne materijale za škole i zajednice kako bi pomogao podići svijest o sigurnosti na globalnoj razini. (*Awareness-training*)
3. KnowBe4 Security Awareness Training**:** KnowBe4 tvrtka za obuku o svijesti o sigurnosti koja nudi razne alate za edukaciju korisnika. Program uključuje simulacije phishing napada, interaktivne tečajeve i obrazovne materijale o online sigurnosti. Analizira napredak polaznika s alatima i daje povratne informacije o njihovim vještinama u sigurnosti (M. Vuković , 2019).

Slika 5. Pogodnosti KnowBe4-a



Prilagođeno prema: https://www.knowbe4.com/

4. IBM Security Learning Academy: IBM nudi besplatnu edukaciju o internetskoj sigurnosti putem IBM Security Learning Academy s besplatnim online tečajevima i resursima. Teme pokrivaju otkrivanje sigurnosnih prijetnji, zaštitu podataka i provođenje sigurnosnih strategija. IBM Academy dizajnirana je za IT profesionalce, ali je otvorena za javnost koja želi poboljšati svoje sigurnosne vještine. (*IBM Security Learning Academy*)

Obrazovanje i svijest najvažnije su komponente smanjenja sigurnosnog rizika. Korisnicima pomaže da kroz različite oblike edukacije prepoznaju te prijetnje, kreiraju sigurnosna ponašanja i pravilno odgovore na moguće napade. Dokazani industrijski primjeri učinkovite prakse pokazuju da ulaganje u obrazovanje donosi odlične rezultate u poboljšanju sigurnosti. Stoga i organizacije i pojedinci moraju kontinuirano ulagati u obrazovanje kako bi bili korak ispred prijetnji za pravilnu zaštitu svojih podataka i sustava.

7. TEHNIČKA RJEŠENJA ZA SMANJENJE RIZIKA KORISNIČKE GREŠKE

Sigurnosni incidenti na internetu često su uzrokovani korisničkim pogreškama. Iako smanjenje takvih pogrešaka može donijeti dobro obrazovanje i svijest, tehnička rješenja također mogu ponuditi značajnu zaštitu. U tehnička rješenja spadaju antivirusni programi i vatrozidi zajedno s višefaktorskom autentifikacijom (MFA) jer su vrlo učinkovit način za smanjenje rizika od napada i zaštitu korisnika i organizacije od potencijalnih prijetnji.

7.1. Sigurnosne politike i procedure

Skup formalnih pravila i smjernica koje opisuju kako treba upravljati informacijama unutar organizacije. Bez kojih sigurnost ne bi imala temelj za održavanje, politike daju okvir i smjernice za ponašanje korisnika.

1. Definicija sigurnosnih politika Sigurnosne politike definirane su kao dokumenti koji određuju zaštitu koja se mora dodijeliti informacijama unutar organizacije. Govori o upravljanju lozinkama, pristupu osjetljivim podacima, korištenju mobilnih uređaja, mrežnoj sigurnosti i zaštiti podataka i mnogim drugim temama. Sigurnosne politike trebaju biti jasne, razumljive i ažurirane kako se pojavljuju novi rizici i tehnologije. Dizajn napredne sigurnosne politike težak je proces jer lako može biti prerestriktivan ili preopćenit u rješavanju ogromne količine sitnih detalja.
2. Provođenje sigurnosnih procedura Sigurnosne politike su temelj, ali osim navođenja onoga što treba učiniti, ključno je specificirati kako će se sigurnosne mjere provoditi. To uključuje određivanje postupaka koje korisnici trebaju slijediti kako bi se informacije mogle zaštititi na odgovarajući način: na primjer, mijenjanjem lozinki s vremena na vrijeme, prijavljivanjem sumnjivih aktivnosti i korištenjem metoda šifriranja za zaštitu osjetljivih podataka. Takvi sigurnosni postupci moraju se integrirati u svakodnevni rad i rutinu za sve korisnike u organizaciji.
3. Obuka o sigurnosnim politikama: Uvođenje sigurnosnih politika i procedura treba biti praćeno obukom zaposlenika. Svi korisnici trebaju biti upoznati s pravilima i procedurama, razumjeti njihovu važnost i znati kako ih primijeniti. Redovita obuka može pomoći u održavanju svijesti o sigurnosnim pitanjima i osigurati da korisnici slijede najbolje prakse.
4. Primjeri sigurnosnih politika: Tipičan primjer sigurnosnih pravila je pravilo upravljanja lozinkama može sadržavati specifičnosti za sastav jakih zaporki, odredbe o njihovom

redovitom ažuriranju i zabrani njihove ponovne upotrebe. Druga je politika korištenja mobilnih uređaja koja bi definirala kako zaposlenici mogu pristupati mreži tvrtke putem svojih mobilnih uređaja i koje mjere zaštite moraju poduzeti. (*Security and Privacy Controls for Information Systems and Organizations*)

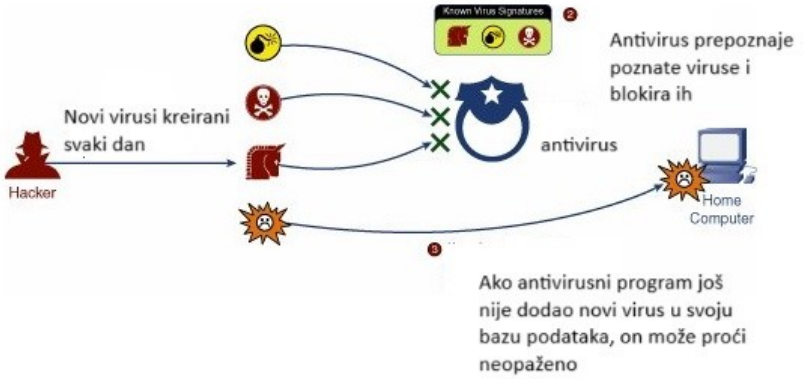
7.2. Upotreba antivirusnih programa i firewall-a

Antivirusni programi i vatrozidi: ovo je mjesto gdje bi svaki korisnik i organizacija trebali započeti u zaštiti od zlonamjernih napada. Djeluju kao prva linija obrane od virusa, malwarea, ransomwarea i drugih oblika cyber prijetnji. (Šimunović, D. 2002).

Antivirusni programi mogu se opisati kao softver koji identificira, blokira i uklanja zlonamjerni softver na ciljanom računalu ili mreži. Oni koriste definicije virusa koje se kasnije ažuriraju kako bi pomogle u identifikaciji i blokiranju novih prijetnji. Antivirusni programi također mogu sadržavati dodatnu sigurnost poput zaštite e-pošte, zaštite preglednika i zaštite u stvarnom vremenu. (Šimunović, D. 2002).

Značajke antivirusnih programa mogu učiniti više nego samo otkriti i izbrisati zlonamjerni softver; mnogi štite od phishing napada, nadziru sumnjive aktivnosti i sprječavaju otvaranje zlonamjernih web stranica. Neki korisnicima daju savjete o sigurnosti kako bi i oni mogli otkriti i izbjeći prijetnje. (Šimunović, D. 2002).

Slika 6. Kako funkcionira antivirus



Prilagođeno prema: https://flylib.com/books/en/2.282.1.27/1/

Vatrozidi (od engl. Firewall) su sigurnosni sustavi. Oni prate i kontroliraju mrežni promet prema unaprijed utvrđenim sigurnosnim pravilima. Drugim riječima, djeluju kao barijera između interne tajne mreže i vanjskog svijeta (Internet), štiteći tako sustave od neovlaštenog pristupa i napada na protok prometa. Postoji nekoliko vrsta vatrozida. To može biti hardver i softver. Hardverski vatrozidi su specifični fizički uređaji postavljeni između mreže i Interneta, dok su softverski vatrozidi programi. I hardverski i softverski vatrozidi mogu filtrirati promet kao i blokirati neovlašteni pristup. Nude i zaštitu tako da organizacije mogu zaštititi svoje mreže od vanjskih napada, spriječiti curenje podataka, osigurati siguran pristup resursima i dodatno postaviti filtriranje internetskog prometa implementacijom vatrozida. Ovo također smanjuje rizik od zlonamjernih aktivnosti. (Šimunović, D. 2002).

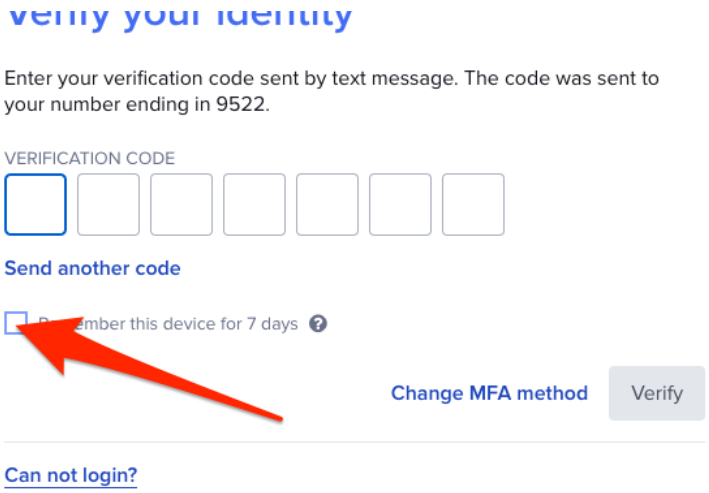
Antivirusne programe i vatrozide treba redovito ažurirati kako bi mogli učinkovito odgovoriti na najnovije prijetnje. To uključuje nove definicije virusa, zakrpe za sigurnosne rajivosti i ažuriranja performansi kako bi se osiguralo da alati ostanu učinkoviti u zaštiti od napada (Šimunović, D. 2002).

7.3. Višefaktorska autentifikacija (MFA)

MFA je još jedan način da provjerite tko ste kada se prijavljujete na račune i vidite osjetljive informacije. MFA smanjuje šanse da neovlašteni korisnici uđu čak i ako je lozinka izložena. MFA je proces u kojem se od korisnika traži da predoče više od jednog identifikacijskog dokumenta prije nego što se odobri pristup. Tipično, MFA uključuje kombinaciju nečega što korisnik zna (lozinka), nečega što korisnik ima (mobilni uređaj ili token) i nečega što korisnik jest (biometrijski podaci poput otiska prsta ili skeniranja lica). MFA metode uključuju: SMS kodovi: Ovo je jedna od najčešće korištenih metoda za MFA gdje se jednokratna šifra šalje SMS-om na mobilni telefon korisnika. Korisnik mora unijeti ovaj kod zajedno sa svojom lozinkom tijekom prijave. Aplikacije za autentifikaciju: Google Authenticator ili Microsoft Authenticator primjer je toga. Generira i osvježava jednokratne kodove za prijavu. Oni su manje rizični od SMS-a jer ne ovise o ugroženim mobilnim mrežama. Biometrijska autentifikacija: Korisnici će morati birati između prepoznavanja lica, otiska prsta ili autentifikacije šarenice. Vrlo je siguran jer sustav reagira samo kada se podudaraju jedinstvene fizičke karakteristike korisnika.

Prednosti MFA: Korištenje MFA smanjuje rizik od krađe identiteta i neovlaštenog pristupa čak i kada je lozinka ugrožena. To osigurava dodatni sloj sigurnosnih poteškoća za hakere koji pokušavaju provaliti u račune i osjetljive podatke. Implementacija MFA u organizacijama: Brojne su organizacije implementirale MFA rješenja za zaključavanje pristupa svojim sustavima i podacima. Višefaktorska provjera autentičnosti može se uvesti kao dio sigurnosne politike i postupno proširivati na sve korisnike. Organizacije također mogu prilagoditi zahtjeve za MFA na temelju razina osjetljivosti informacija i povezanih rizika. (Multi-Factor-Authentication)

Slika 7. Primjer MFA



Prilagođeno prema: https://support.clever.com/hc/s/articles/202062333?language=en_US

8. SIGURNOSNE PREPORUKE ZA KRAJNJE KORISNIKE

Internetska sigurnost nije samo za organizacije i IT stručnjake već i za svakog pojedinog korisnika digitalnih tehnologija. Krajnji korisnici igraju ključnu ulogu u čuvanju svojih osobnih podataka i smanjenju opasnosti od cyber prijetnji. Ovaj dio rada daje neke preporuke koje mogu pomoći u promjeni i praktične, zajedničke ideje o tome kako se sigurnije ponašati na internetu, načine razlikovanja sigurnosnih prijetnji, pravila za korištenje zaštitnih alata.

8.1. Savjeti za sigurnije ponašanje na internetu

Temelj internetske sigurnosti je u svakodnevnom ponašanju i navikama korisnika. Evo nekoliko praktičnih savjeta koji vam mogu pomoći u zaštiti vaše internetske privatnosti i sigurnosti: jake lozinke, ažuriranje lozinki, MFA.

Jake lozinke: One bi trebali biti komplicirane i različite za svaki račun kombinacijom slova, brojeva i posebnih znakova. Osim toga, izbjegavajte očite lozinke poput imena, prezimena ili nekih znamenki poput datuma rođenja. Također, korisnici trebaju imati lozinku dužu od 8 znakova.

Slika 8. Snaga iste lozinke na različitim platformama

(https://www.sentinelone.com/blog/7-signs-weak-password/)

Ažuriranja lozinki: Preporučuje se češće ažuriranje lozinki, barem svakih nekoliko mjeseci. U slučaju da sumnjate da je vaša lozinka procurila, odmah je promijenite.

Multi-Factor Authentication (MFA): gdje je primjenjivo, treba omogućiti MFA u svojim računima na mreži. Ovo osigurava da će dodatni sloj sigurnosti biti dodan identificiranjem s drugim faktorom uz lozinku.

Pazite na *phishing* napade: pripazite na sve e-poruke ili poruke koje traže osobne podatke ili one koje dolaze s poveznicama i privicima sumnjive prirode. Nemojte slijediti veze nepoznatih izvora u svojim e-porukama i nemojte dijeliti osjetljive informacije putem e-pošte.
Redovito ažuriranje softvera: često donose nove sigurnosne zakrpe za pomoć u zaštiti od novih prijetnji. Čim budu objavljeni, ažurirajte operativni sustav, aplikacije i preglednike.

Korištenje sigurnosnog softvera: Ovo uključuje instalaciju antivirusnih programa i vatrozida kako bi se osigurala zaštita od zlonamjernog softvera i napada na vaše računalo. Pobrinite se da se takvi alati redovito ažuriraju.

Sigurno korištenje Wi-Fi mreža: uzdržite se od korištenja javnih Wi-Fi mreža za aktivnosti koje uključuju osjetljive podatke kao što je internetsko bankarstvo. U slučajevima kada je potrebno koristiti javni Wi-Fi, koristite VPN kako bi vaši podaci bili šifrirani.

Obrada i pohrana osobnih podataka: Treba biti vrlo oprezan pri dijeljenju osobnih podataka na društvenim mrežama i drugim web stranicama. Provjerite te postavke privatnosti kako bi informacije bile dostupne samo određenim osobama. Poznavanje sigurnosnih prijetnji ključno je za obranu od kibernetičkih napada. (https://staysafeonline.org/online-safety-privacy-basics/public-computers-and-wi-fi/)
Slijedi nekoliko ideja za prepoznavanje mogućih prijetnji:
Loša e-pošta: pripazite na poruke koje dostavljaju nepoznati pošiljatelji ili one koje imaju dojam hitnosti. Znakovi phishing napada uključuju e-poruke koje dolaze s previše dobrih prilika, traže informacije ili su loše napisane.
Čudna aktivnost: U slučaju da postoje neke čudne prijave ili transakcije na vašim računima na mreži, bolje je da odmah stupite u kontakt s pružateljem usluga i promijenite te lozinke.
Sumnjiva web-mjesta: Što se tiče posjeta bilo kojem naizgled sumnjivom web-mjestu ili onom koje nudi besplatne proizvode, besplatne usluge bez jasnog cilja - pripazite. Takve stranice obično distribuiraju zlonamjerni softver za prikupljanje osobnih podataka.
Softverske zakrpe i ažuriranja: Primit ćete e-poštu ili skočnu obavijest o softverskim zakrpama ili ažuriranjima. Ako je tako, potvrdite da je izvor autentičan prije preuzimanja bilo čega.

Ažuriranja bi trebala dolaziti samo iz izravnih izvora. (https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf)

Loše ponašanje sustava: Siguran znak da je vaše računalo zaraženo nekim zlonamjernim softverom uključuje slučajeve u kojima počinje biti sporo, neočekivano se ponovno pokreće ili prikazuje neobične poruke o pogrešci. Korištenje sigurnosnih alata može značajno poboljšati vašu zaštitu na internetu.

Evo nekoliko preporuka za najbolje alate i kako ih koristiti:

Antivirusni programi: Važan je odabir odgovarajućeg antivirusnog programa koji pruža zaštitu u stvarnom vremenu, redovito ažuriranje definicija i mogućnost skeniranja vašeg računala u potrazi za prijetnjama. Preporučeni uključuju *Bitdefender*, *Norton* ili *Kaspersky*. Firewall-ovi: Koristite firewall-ove za zaštitu vaše mreže od vanjskih napada.

Mnogi operativni sustavi dolaze s već prethodno ugrađenim firewall-ovima, ali možete također razmotriti dodatne softverske ili hardverske firewall-ove za dodatnu zaštitu.

VPN (Virtualna privatna mreža): VPN-ovi kriptiraju vašu internetsku vezu i skrivaju vašu IP adresu, pružajući ovaj dodatni sloj zaštite prilikom pregledavanja weba — osobito na javnoj Wi-Fi mreži. Preporuča se odlučiti se za ugledne VPN usluge kao što su *ExpressVPN*, *NordVPN* ili *CyberGhost.* (https://www.antivirussoftwareguide.com/best-free-antivirus)

Alati za upravljanje lozinkama možete slobodno kreirati složene, jedinstvene šifre i pohraniti ih u alat za upravljanje lozinkama kao što su LastPass, 1Password ili Dashlane. Neki od ovih alata također automatski ispunjavaju obrasce i daju drugu razinu sigurnosti.

Alati za zaštitu privatnosti: Razmislite o korištenju alata za zaštitu privatnosti koji mogu blokirati praćenje web stranica, upravljati kolačićima i zaštititi vaše osobne podatke. Primjeri uključuju Privacy Badger i uBlock Origin (APNIC 2016).

Sigurnost na internetu zahtijeva aktivno sudjelovanje korisnika i primjenu najboljih praksi za zaštitu osobnih podataka. Praktični savjeti za sigurnije ponašanje, sposobnost prepoznavanja sigurnosnih prijetnji i korištenje odgovarajućih sigurnosnih alata ključni su za smanjenje rizika od kibernetičkih prijetnji. Primjenom ovih preporuka, korisnici mogu značajno poboljšati svoju sigurnost na internetu i zaštititi svoje digitalne resurse.

9. ISPITIVANJE SVIJESTI I NAVIKA KORISNIKA U PODRUČJU INTERNETSKE I KIBERNETIČKE SIGURNOSTI

9.1.Cilj istraživanja

Cilj istraživanja je ispitati razinu svijesti i navika prosječnog korisnika računalnih mreža o internetskoj i kibernetičkoj sigurnosti, identificirati koje sigurnosne prijetnje korisnici smatraju najopasnijima te istražiti u kojoj mjeri korisnici primjenjuju neke od najčešćih sigurnosnih mjera.

Istraživanje je trajalo 8 dana, u razdoblju od 25. kolovoza 2024. do 1.rujna 2024. godine. U tom vremenskom razdoblju prikupljeni su podaci od 104 ispitanika. Od ukupno 104 ispitanika 54 osobe bile su muškog spola, 47 osoba ženskog spola, dok se 3 osobe nisu dale informaciju o svom rodu.

Većina ispitanika 48(46,2%) bila je u dobnoj skupini, unutar intervala dobi 18-24, 24 ispitanika nalazi se u dobnoj skupini 25-34, 10 ispitanika ima manje od 18 godina, 8 ispitanika nalazi se u skupini 45-54, a skupine 35-44 i 55+ dijele isti broj ispitanika(7). Svi ispitanici su iz Republike Hrvatske. Primarna metodologija bila je kvantitativna analiza putem online ankete na Google Obrasci platformi. Ispitanici su odabrani na temelju volje i dostupnosti za sudjelovanje.

9.2. Rezultati istraživanja

Ovi podaci pokazuju na visoku razinu svakodnevne upotrebe interneta, što može imati posljedice na njihovu izloženost internetskim prijetnjama, jer istraživanja pokazuju povezanost među različitim vrstama rizičnih ponašanja na internetu (Tablica 1). Korisnici koji puno osobnih podataka i informacija postavljaju na društvenim mrežama ili prekomjerno upotrebljavaju internet rizičnije se ponašaju i u drugim situacijama (Karl, Peluchette i Schlaegel, 2010).

Tablica 1- Koliko često koristite Internet

ODGOVOR	Broj (postotak) ispitanika
Svakodnevno	88 (84,6)
Nekoliko puta tjedno	11 (10,5)
Nekoliko puta mjesečno	2 (1,9)
Rijetko	3 (2,9)

Izvor: Autor

Tablica 2-Jeste li upoznati s pojmovima internetske sigurnosti i kibernetičke sigurnosti?

ODGOVOR	Broj (postotak) ispitanika
Da, potpuno sam upoznat/a	40 (38,5)
Djelomično sam upoznat/a	54 (51,9)
Nisam upoznat/a	10 (9,6)

Izvor: Autor

Ovi rezultati pokazuju da je većina ispitanika barem u osnovama upoznata s pojmovima,a dobar dio ispitanika govori da je u potpunosti upoznat s istim . No, postoji i manji dio ispitanika kojima su svi ovi pojmovi nepoznati, što govori da postoji potreba za daljnom edukacijom i podizanjem razine svijesti o internetskoj i kibernetičkoj sigurnosti. Kako bi se unaprijedila sigurnosna pismenost, korisno bi bilo uvesti cjeloživotne programe obrazovanja koji bi obrađivale „teme internetska i kibernetička sigurnost“ jer savjete o smanjenju rizika i povećanju sigurnosti korisnici najčešće pretražuju na internetu gdje često krše uobičajena pravila zaštite kao što su odavanje adrese ili lozinke. (Šolić, Velki i Galba, 2015; Velki i Sur., 2017).

Tablica 3 - Koje sigurnosne prijetnje na internetu smatrate najopasnijima? (možete odabrati više odgovora)

ODGOVOR	Broj (postotak) ispitanika
Virusi	69 (65,7)
Malware	42 (40)
Phishing	35 (33,3)
Ransomware	25 (23,8)
Zaštita podataka (dodani odgovor)	1 (1)
Ostalo (dodani odgovor)	3 (2,9)

Izvor: Autor

Ovi rezultati pokazuju da su virusi najopasnija prijetnja, prema mišljenju ispitanika, dok *phishing i malware* također imaju težinu. S druge strane zaštita podataka nije prepoznata kao velika prijetnja, što može ukazivati na potrebu podizanja svijesti o istoj.

Tablica 4 - Smatrate li da korisnici igraju ključnu ulogu u sigurnosti internetske mreže?

ODGOVOR	Broj (postotak) ispitanika
Da	71 (67,7)
Ne	12 (12,4)
Nisam siguran/na	21 (20)

Izvor: Autor

Ovi rezultati pokazuju da većina ispitanika smatra da korisnici imaju ključnu ulogu u održavanju sigurnosti internetske mreže, dok manji postotak sumnja ili se ne slaže s tim mišljenjem. Ova percepcija naglašava obrazovanje koje je potrebno za informiranje korisnika o njihovoj ulozi u zaštiti njihovih resursa, osobnih i mrežnih.

Tablica 5 - Smatrate li da je naivnost ili nepažnja korisnika čest uzrok internetskih sigurnosnih prijetnji?

ODGOVOR	Broj (postotak) ispitanika
Da	89 (84,8)
Ne	6 (5,7)
Nisam siguran/na	9 (9,5)

Izvor: Autor

Odgovori sudionika ukazuju na to da su naivnost i nepažnja glavni faktori koji dovode do sigurnosnih prijetnji. Iako većina sudionika misli tako, istraživanje koje je provedeno na području cijele hrvatske, a u kojem je sudjelovalo 4859 sudionika pokazuje kako između 31% i 54,2% sudionika kroz svoju naivnost ili nepažnju daju svoju zaporku koju koriste za e-poštu što je zabrinjavajuća činjenica o odavanju osobnih podataka (Šolić , Velki i Galba, 2015; Velki i sur., 2017). To nam pokazuje da ulaganje u edukaciju nikad nije beskorisno, jer svaki dan smo izloženi novim rizicima i prijetnjama.

Tablica 6 - Jeste li ikada bili žrtva *phishing napada*? (*Phishing j*e vrsta kibernetičkog napada u kojem napadač koristi lažne poruke ili web stranice kako bi prevario korisnike da otkriju osjetljive informacije poput lozinki i brojeva kreditnih kartica.)

ODGOVOR	Broj (postotak) ispitanika
Da	43 (41)
Ne	48 (45,7)
Nisam siguran/na	13 (13,3)

Izvor: Autor

Ovi rezultati pokazuju da je značakan broj ispitanika imao iskustva s phishing napadima, dok gotovo polovina ispitanika nije bila izložena. Postotak za one koji nisu sigurni naglašava kako postoji manjak znanja u prepoznavanju znakova phishing napada, što korisnicima ne omogućuje potpuno razumijevanje potencijalnih prijetnji.

Tablica 7 - Koliko često mijenjate lozinke za svoje online račune?

ODGOVOR	Broj (postotak) ispitanika
Svakih nekoliko mjeseci	16 (15,2)
Jednom godišnje	27 (25,7)
Rijetko ili nikada	51 (59)

Izvor: Autor

Manji postotak sudionika mijenja lozinke svojih online računa svakih nekoliko mjeseci ili jednom godišnje, dok većina ispitanika mijenja rijetko ili gotovo nikada. Ovi rezultati se mogu usporediti s istraživanjem koje se provelo među studentima Filozofskog fakulteta u Zagrebu 2013. gdje je većina sudionika kao i ovoj anketi izjavila da nikada ili rijetko mijenaju svoje lozinke. (T. Borovac, 2019.) Svijest o važnosti sigurnosti lozinke postoji, ali postoji i potreba za učenje održavanja sigurnosti računa

Tablica 8- Koristite li iste lozinke za više različitih online računa?

ODGOVOR	Broj (postotak) ispitanika
Da, uvijek	41 (39)
Ponekad	48 (45,7)
Nikada	15 (15,2)

Izvor: Autor

Ovi rezultati pokazuju da će većina ispitanika vjerojatno koristiti istu lozinku za više računa, povećavajući sigurnosne rizike. Vrlo mali broj ispitanika drži se strategije jedinstvene lozinke za svaki račun. Korištenje različitih lozinki za različite račune je važno. Ugrožavanje jedne lozinke može ugroziti sve ostale račune. Na taj su način osjetljivi podaci bolje zaštićeni, a napadačima postaje veći izazov provaliti u korisničke račune.

Tablica 9- Smatrate li da je edukacija ključna za smanjenje rizika od internetskih prijetnji?

ODGOVOR	Broj (postotak) ispitanika
Da, apsolutno	62 (59)
Možda	34 (32,4)
Ne, nije toliko važna	8 (8,6)

Izvor: Autor

Rezultati upućuju na to da većina ispitanika smatra da je obrazovanje ključno u smanjenju rizika od internetskih prijetnji što je pokazatelj interesa za takvo obrazovanje.Manji postotak ispitanika smatra da obrazovanje možda nije toliko važno ili da možda nije dovoljno, što može ukazivati na potrebu za više informacija i resursa o sigurnosnim praksama.

Također, rezultati su pokazali da većina ispitanika barem povremeno koristi antivirusne programe i vatrozid. Ovo je pozitivan znak za kibernetičku sigurnost. No, također značajan postotak ispitanika nikada ga ne koristi, što može biti sigurnosni rizik (Tablica 10).

Tablica 10- Koristite li antivirusne programe i firewall-ove na svom računalu?

ODGOVOR	Broj (postotak) ispitanika
Da, uvijek	44 (42,3)
Ponekad	46 (44,2)
Nikada	13 (13,5)

Izvor: Autor

Tablica 11 - Jeste li ikada koristili višefaktorsku autentifikaciju (MFA) za svoje online račune? (Višefaktorska autentifikacija (MFA) je sigurnosni postupak koji zahtijeva više od jednog oblika provjere identiteta za pristup računu ili sustavu.- uz lozinku najčešće je to kod koji Vam pristigne SMS-om ili na mail.

ODGOVOR	Broj (postotak) ispitanika
Da	70 (67,6)
Ne	34 (32,4)

Izvor: Autor

Ovi rezultati pokazuju da većina ispitanika koristi višefaktorsku autentifikaciju, što je odličan način za poboljšanje sigurnosti na njihovim online računima. Međutim, znatan postotak ne koristi istu. To ukazuje na potrebu za dodatnu edukaciju i neku vrstu poticaja koji su potrebni kako bi se više ljudi potaklo na autentifikaciju s više faktora i zauzvrat bolje zaštitili svoje račune.

Tablica 12 - Koliko često ažurirate svoj softver i aplikacije?

ODGOVOR	Broj (postotak) ispitanika
Uvijek	49 (47,6)
Ponekad	48 (46,6)
Nikada	5 (5,8)

Izvor: Autor

Kao što je vidljivo iz rezultata, veliki dio ispitanika povremeno/redovito ažurira svoj softver i aplikacije, što se smatra povećanjem sigurnosti i stabilnosti sustava. Ažuriranje aplikacija i softvera je korisno jer poboljšava sigurnost uređaja tako što osigurava ispravljanje pogrešaka, osigurava kompatibilnost s novim tehnologijama, nudi nove funkcionalnosti i pomaže u zaštiti podataka. To uključuje zaštitu od prijetnji, poboljšanu stabilnost i bolji rad sustava koje pružaju pravodobna ažuriranja. Međutim, manji dio ispitanika nikad ne ažurira svoj softver. To može predstavljati sigurnosni rizik jer bi napadači mogli iskoristiti nezakrpane ranjivosti.

Tablica 13- Koristite li VPN kada pristupate internetu putem javnih Wi-Fi mreža?

ODGOVOR	Broj (postotak) ispitanika
Da, uvijek	25 (23,8)
Rijetko	48 (45,7)
Nikada	31 (30,5)

Izvor: Autor

Najmanji broj ispitanika uvijek koristi VPN kada pristupaju internetu putem javnih mreža, dok veći postotak rijetko ili nikada ne koriste VPN. Tek kada korisnik koristi VPN, njegova se internetska veza kriptira i usmjerava preko poslužitelja koji pruža VPN uslugu, čime se nudi zaštita podataka od špijuniranja, čineći mrežnu aktivnost anonimnijom i omogućavajući pristup blokiranom ili ograničenom sadržaju. Postoji potreba za boljom edukacijom

Tablica 14- Koliko smatrate važnim korištenje alata za upravljanje lozinkama?

ODGOVOR	Broj (postotak) ispitanika
Važno	50 (48,5)
Umjereno važno	46 (44,7)
Nije važno	6 (6,8)

Izvor: Autor

Rezultati pokazuju da većina ispitanika smatra da su alati za upravljanje lozinkama važni, što zauzvrat ukazuje na to da postoji svijest o prednostima korištenja takvih alata za poboljšanje

sigurnosti u vezi sa lozinkama i olakšavanje upravljanja lozinkama. Manji dio ispitanika smatra da korištenje alata za upravljanje lozinkama nije važno, što nije dobar pokazatelj jer npr. stariji korisnici zapisuju na više mjesta kao što su papiri ili u gorem slučaju računala, što predstavlja rizik za krađu istih i mogućnost „provale“ u račune (Hrvatska udruga banaka, 2017).

10.ZAKLJUČAK

Internetska sigurnost danas je jedno od najvažnijih pitanja digitalnog doba. Gdje su virusi, zlonamjerni softver, *phishing i ransomware* vrlo uobičajene prijetnje s kojima se svakodnevno susrećemo. Poznavanje razlike između internetske i kibernetičke sigurnosti plus osnovnih prijetnji na mreži već uspostavlja bazu za mnogo sigurnije digitalno okruženje. Ali čak i uz dovoljno razvijena tehnološka rješenja zaštite korisnici su i dalje najslabija karika u sigurnosti. Veliku ulogu u očuvanju sigurnosti imaju sami korisnici kao aktivni sudionici internetskog prostora. Budući da je njihova naivnost, nepažnja i nedostatak svijesti ono što često pomaže napadačima (osobito onima koji se bave krađom identiteta uz socijalni inženjering) da uspiju u svom prljavom poslu koji im je prvi na dohvat ruke izazivajući incidente iz stvarnog života zbog ljudske pogreške koji ponekad mogu naštetiti pojedincu, ali također rezultiraju određenom poslovnom štetom ili utjecajem na organizaciju najčešće IT sigurnosne prijetnje dolaze upravo od ponašanja korisnika. Slabe lozinke, otkrivanje osobnih podataka na webu i neoprezno otvaranje sumnjive e-pošte povećavaju vjerojatnost ugrožavanja sigurnosti.

Razumijevanje ovih prijetnji i pridržavanje sigurnijih praksi ključni je aspekt obrazovanja korisnika i podizanja svijesti. To je zato što kroz dobro osmišljene programe obuke i sesije korisnici mogu lako prepoznati prijetnje i primijeniti odgovarajuće sigurnosne mjere. Primjeri najbolje prakse iz industrije pokazuju da su svjesni, ali neobučeni korisnici prva linija obrane od kibernetičkih prijetnji, dok su tehnička rješenja samo dodatni alati: sigurnosne politike kao i antivirusni programi, vatrozidi, mehanizmi multifaktorske autentifikacije (MFA) štite od ljudskog faktora, napadači iskorištavaju pogreške korisnika, ali to ne mogu jamčiti sami bez svijesti o sigurnosti među članovima organizacije kako bi bili sigurni da se te mjere slijede za zaštitu od raznih kibernetičkih napada. Sigurnosni savjeti korisnika, poput ažuriranja lozinki, korištenja antivirusnog softvera i opreza na internetu, mogu u velikoj mjeri pomoći u zaštiti podataka - kako osobnih tako i poslovnih. Svijest o prijetnjama informacijskoj sigurnosti i ispravno korištenje alata pomaže u održavanju integriteta podataka i zaštiti privatnosti u digitalnom okruženju.

Anketni rezultati provedenog istraživanja pokazuju da dok većina korisnika razumije osnovne pojmove i prijetnje povezane sa sigurnošću na Internetu, znatan broj njih je neinformiran ili nepažljiv, ostavljajući se izloženima prijetnjama poput phishinga i zlonamjernih programa, između ostalog. Više od 40% ispitanika priznalo je da koristi slične lozinke za različite račune, dok gotovo 60% rijetko mijenja lozinke ili ih uopće ne mijenja; ova činjenica čini rizik od neovlaštenog pristupa informacijama više nego značajnim. S druge strane, neki ispitanici

koriste višefaktorsku autentifikaciju i redovito ažuriraju svoj softver. Ovo je važno jer se neki korisnici aktivno štite. Međutim, pod alatima koji će se koristiti kao što su VPN i upravitelji lozinki ističe da postoji mnogo prostora za poboljšanje svijesti i prakse sigurnosti na internetu.

Nalazi ovog istraživanja dokazuju da su tehnička rješenja samo jedan dio cjeline, pri čemu edukacija korisnika treba unaprijediti kibernetičku sigurnost. Točnije putem informiranja i obrazovanja te osvješćivanja ljudi o potrebi redovite promjene lozinki, posjedovanju jedinstvenih lozinki za različite račune i korištenjem MFA-a, može se smanjiti rizik od toga da postanete žrtva kibernetičkih napada. Trostruki pristup (svijest korisnika plus tehnička rješenja i stalna edukacija) ključan je za pružanje sigurnog internetskog okruženja. Samo zajedničkim naporima i suradnjom svih članova digitalne zajednice možemo se učinkovito oduprijeti prijetnjama u informacijskom prostoru koji nas okružuje.

11.LITERATURA

1. APNIC (2016) *Network Security Tutorial*. Dostupno na: https://training.apnic.net/wp-content/uploads/sites/2/2016/12/TSEC01.pdf (Pristupljeno: 28. lipnja 2024).

2. Conry-Murray, A. i Weafer, V. (2005) *Sigurni na internetu*.

3. Dangubić, I. (2019) *Zaštita od računalnih virusa*. Dostupno na: https://repozitorij.unipu.hr/islandora/object/unipu:3894/datastream/PDF/download (Pristupljeno: 18. srpnja 2024).

4. Dangubić, I. (2019) *Sigurnost podataka na internetu*. Dostupno na: https://repozitorij.efst.unist.hr/islandora/object/efst:3232/datastream/PDF/download (Pristupljeno: 3. srpnja 2024).

5. Ivezić, B. (2014) 'HNB: Sumnja se da su cyber kriminalci Hrvatima ukrali 1,8 milijuna kuna', *Poslovni dnevnik*, 30. lipnja. Dostupno na: https://www.poslovni.hr/sci-tech/manje-napada-cyber-kriminalaca-ali-opasnost-i-dalje-postoji-27446 (Pristupljeno: 7. kolovoza 2024).

6. *Ransomware and phishing cyberattacks* (2022). Dostupno na: https://uu.diva-portal.org/smash/get/diva2:1678538/FULLTEXT01.pdf (Pristupljeno: 19. kolovoza 2024).

7. Rudeš, I. i Pavelić, I. (2023) 'Cyber-rizik, fenomen koji postoji i ugrožava nas'. Dostupno na: https://hrcak.srce.hr/file/451408 (Pristupljeno: 16. kolovoza 2024).

8. Šimunović, D. (2002) *Zaštita računalnih resursa pomoću internet firewalla*. Dostupno na: https://hrcak.srce.hr/169780 (Pristupljeno: 23. srpnja 2024).

9. Specops Software (2023) *Weak Password Report*. Dostupno na: https://specopssoft.com/wp-content/uploads/2023/03/Specops-Software-Weak-Password-report-2023.pdf (Pristupljeno: 11. srpnja 2024).

10. Velki, T. i Šolić, K. (2019) *Izazovi digitalnog svijeta*, str. 16-55, 203-220, 230.

11. Vukelić, B., Zvonarić, A.D. i Protrka, N. (2023) 'Prepoznavanje phishing napada u poslovnim organizacijama'. Dostupno na: https://hrcak.srce.hr/file/445784 (Pristupljeno: 14. kolovoza 2024).

12. *IT sigurnost - zašto smo sami svoj najveći neprijatelj?* (2022). Dostupno na: IT sigurnost - zašto smo sami svoj najveći neprijatelj? - VENTEX - Poslovna IT rješenja (Pristupljeno: 11. kolovoza 2024).

13. *Sigurnost na Internetu: Najnovije prijetnje i kako se zaštititi?* (2023). Dostupno na: https://geek.hr/clanak/sigurnost-na-internetu-najnovije-prijetnje-i-kako-se-zastititi/ (Pristupljeno: 7. srpnja 2024).

14. *Sigurnost na internetu: Neosvještenost korisnika najveći rizik* (2024). Dostupno na: https://fakta.ba/sigurnost-na-internetu-neosvjestenost-korisnika-najveci-rizik/ (Pristupljeno: 1. srpnja 2024).

15. *From Breach to Fallout: The Story of the 2014 Sony Hack* (2023). Dostupno na: From Breach to Fallout: The Story of the 2014 Sony Hack | HackerNoon (Pristupljeno: 11. srpnja 2024).

16. *Factors Affecting Reputational Damage to Organisations Due to Cyberattacks* (2016). Dostupno na: Informatics | Free Full-Text | Factors Affecting Reputational Damage to Organisations Due to Cyberattacks (mdpi.com) (Pristupljeno: 21. lipnja 2024).

17. *Tech Firm Ubiquiti Suffers $46M Cyberheist* (2015). Dostupno naTech Firm Ubiquiti Suffers $46M Cyberheist – Krebs on Security (Pristupljeno: 8. srpnja 2024).

18. *Linkedin 2012* (2015). Dostupno na: https://www.trendmicro.com/ (Pristupljeno: 22. srpnja 2024).

19. *The Importance of Cybersecurity Awareness, Training, and Education* (2022). Dostupno na: https://dotsecurity.com/ (Pristupljeno: 5. kolovoza 2024).

20. *Public Wi-Fi: An ultimate guide on the risks + how to stay safe* (2021). Dostupno na: Public Wi-Fi: What are the risks? + how to stay safe - Norton (Pristupljeno: 13. kolovoza 2024).

21. *Ways to protect your personal information online* (2024). Dostupno na: 13 ways to protect your personal information online | Proton (Pristupljeno: 7. srpnja 2024).

22. *Zero Trust Security* (2024). Dostupno na: Cyber Security Training | SANS Courses, Certifications & Research (Pristupljeno: 12. lipnja 2024).

23. *Can you spot when you're being phished?* (2024). Dostupno na: Jigsaw | Phishing Quiz (Pristupljeno: 9. srpnja 2024).

24. *Awareness-training* (2024). Dostupno na: https://www.microsoft.com/hr-hr/security/business/security-awareness-training (Pristupljeno: 1. rujna 2024).

25. *IBM Security Learning Academy*. Dostupno na: https://login.ibm.com/ (Pristupljeno: 4. lipnja 2024).

26. *Security and Privacy Controls for Information Systems and Organizations* (2023). Dostupno naSP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov) (Pristupljeno: 16. srpnja 2024).

27. *Multi-Factor Authentication*. Dostupno na: https://www.microsoft.com/en-us/security/business/identity/multi-factor-authentication (Pristupljeno: 11. kolovoza 2024).

12.PRILOZI

12.1. Popis slika

12.2. Popis tablica

IZJAVA O AUTORSTVU RADA

Ja, **Jakov Barišić**, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor završnog/diplomskog rada pod naslovom: **Korisnik kao najslabija karika internetske mreže** te da u navedenom radu nisu na nedozvoljen način korišteni dijelovi tuđih radova.

U Požegi, 05. rujna 2024.

Potpis studenta: