Primljen: 30.11.2024.
Prihvaćen: 12.12.2024.

Stručni rad
UDK: 343.533:004.056.5

STRATEGIJE SOCIJALNOG INŽENJERINGA: ČOVJEK KAO META

SOCIAL ENGINEERING STRATEGIES: HUMAN AS TARGET

Miljenko Vrbanec
Međimursko veleučilište u Čakovcu, Čakovec, Bana Josipa Jelačića 22a, Hrvatska, mvrbanec@mev.hr

Magdalena Zeko
Međimursko veleučilište u Čakovcu, Čakovec, Bana Josipa Jelačića 22a, Hrvatska, mzeko@mev.hr

Sažetak: Socijalni je inženjering dominantan način krađe podataka u današnjem tehnološki razvijenom društvo. Takvi oblici prijevara ciljaju na ljudske slabosti, a ne samo na tehnološke ranjivosti. Glavni je cilj napada krađa povjerljivih informacija putem psihološke manipulacije korisnika. Ova praksa obuhvaća tehnike poput *phishinga, vishinga, smishinga, baitinga i scarewarea*. *Phishing* se ističe kao najčešća metoda, koja uključuje lažne poruke s linkovima za krađu osobnih podataka. Napadači često koriste emocionalne manipulacije, stvarajući osjećaj hitnosti ili straha. Industrijska špijunaža i krađa identiteta sve su češće, potaknute rastom digitalnog marketinga i online kupnje. Pojavljuju se i sofisticirane prijevare usmjerene na menadžere i korporativne sustave. Prevencija uključuje tehničke mjere poput antivirusnih programa, firewalla i sigurnosnih politika, ali ključna je edukacija korisnika. Osobne informacije trebaju se pažljivo čuvati, a lozinke redovito mijenjati. Organizacije trebaju kombinirati fizičku sigurnost, kontrolu pristupa i slojevitu obranu kako bi smanjile rizike. Nacionalni zakonodavni okvir prepoznaje kaznena djela protiv računalnih sustava, a novi Zakon o kibernetičkoj sigurnosti zahtijeva upravljanje rizicima i prijavljivanje incidenata. Kombinacija tehničke zaštite i svijesti korisnika ključna je za suzbijanje napada socijalnog inženjeringa, čime se smanjuje potencijalna šteta za pojedince i organizacije.

Ključne riječi: socijalni inženjering, manipuliranje informacijama, krađa podataka, internetska sigurnost.

Abstract: Social engineering is the dominant method of data theft in today's technologically advanced society. These types of fraud target human weaknesses, not just technological

vulnerabilities. The main goal of the attack is the theft of confidential information through psychological manipulation of users. This practice includes techniques such as phishing, vishing, smishing, baiting, and scareware. Phishing stands out as the most common method, involving fake messages with links to steal personal data. Attackers often use emotional manipulation, creating a sense of urgency or fear. Industrial espionage and identity theft are becoming more frequent, driven by the growth of digital marketing and online shopping. Sophisticated frauds targeting managers and corporate systems are also emerging. Prevention involves technical measures such as antivirus programs, firewalls, and security policies, but user education is crucial. Personal information should be carefully protected, and passwords should be changed regularly. Organizations need to combine physical security, access control, and layered defense to reduce risks. The national legal framework recognizes crimes against computer systems, and the new Cybersecurity Act requires risk management and incident reporting. A combination of technical protection and user awareness is key to combating social engineering attacks, thereby reducing potential damage to individuals and organizations.

Keywords: Social engineering, information manipulation, data theft, internet security.

1. Uvod

Razvojem se tehnologije, danas više no ikada prije, stvorila mogućnost manipuliranja, krađe i drugih zlouporaba podataka. Pritom se, pogotovo u medijima, stavlja naglasak na vrhunske tehnologije kojima je to omogućeno i koje su sredstvo za takve radnje. Međutim, zaboravlja se na to da se i dalje najviše koriste različite tehnike socijalnog inženjeringa. Naglasak je tu na iskorištavanju ljudskih slabosti i/ili emocija za što je potrebna samo određena socijalna inteligencija a ne vrhunsko poznavanje i upravljanje složenim i modernim tehnologijama. Problem predstavlja i to što posljedice takvih povreda nije samo materijalna šteta nego i nematerijalna šteta u vidu emocionalne štete, štete po ugled pojedinca i povredu ostalih prava osobnosti[1].

Glavni je cilj socijalnog inženjeringa krađa podataka iz raznih informacijskih sustava na način da se napada najslabiji sigurnosni element: čovjek kao krajnji korisnik. Današnje informatičke tehnologije stvorile su vrlo moćne, skoro pa neprobojne informacijske sustave. U procesu

[1] Prava osobnosti uređena su člankom 19. Zakona o obveznim odnosima NN 35/05, 41/08, 125/11, 78/15, 29/18, 126/21, 114/22, 156/22, 155/23. Pod pravima osobnosti u smislu toga Zakona razumijevaju se prava na život, tjelesno i duševno zdravlje, ugled, čast, dostojanstvo, ime, privatnost osobnog i obiteljskog života, slobodu i dr.

uporabe raznih podataka postoji hardver, softver i korisnik. Hardver se štiti fizičkim zaštitnim sustavima, ali i softverom. Softver se štiti hardverom, ali i drugim softverom (primjerice kriptografijom). Korisnik je na kraju toga lanca. No prije toga on je i sudionik procesa stvaranja i korištenja softvera i hardvera i kao takav dolazi u posjed mnogih ključnih podataka i informacija. Ta činjenica, da čovjek upravlja informacijama, iskorištava se prilikom planiranja radnji u području socijalnog inženjeringa. Time se neovlašteno i lako dolazi do podataka i informacija kao što su zaporke, pinovi i osobni podaci. Korištenje sofisticirane tehnologije i opreme može biti metoda koja se koristi u takvim kombinacijama ali ona često podrazumijeva znatne troškove kao i određeno vrijeme potrebno za implementaciju. Prema Wangu i sur. (2021), u kontekstu kibernetičke sigurnosti, socijalni inženjering vrsta je napada u kojem napadač iskorištava ljudske ranjivosti (sredstvima kao što su utjecaj, uvjeravanje, obmana, manipulacija i navođenje) za kršenje sigurnosnih ciljeva (kao što su povjerljivost, integritet, dostupnost, mogućnost kontrole i mogućnost revizije) elemenata kibernetičkog prostora (kao što su infrastruktura, podaci, resursi, korisnici i operacije).[2] Socijalni inženjering nije kibernetički napad određenom računalnom opremom već je to psihološko djelovanje na osobu, ali cilj je isti – doći do zaštićenih informacija. Prema Andersonu (2008) socijalni inženjering odnosi se na svaki oblik psihološke manipulacije s ciljem odavanja osobnih i povjerljivih podataka korisnika[3].

Neovlašteno prikupljanje informacija radi stjecanja financijske koristi najčešći je cilj socijalnog inženjeringa i to putem informacija pribavljenih od fizičkih osoba. U kontekstu informacijske sigurnosti, cilj socijalnog inženjeringa je i prisvojiti pravo na pristup osobnim podacima i informacijama koje ima fizička osoba, a kako bi se stvorio pristup informacijskom sustavu određene pravne osobe.

Način na koji se počinitelji žele domoći materijalne, najčešće imovinske koristi su prijevare putem krađa PIN-ova, zaporki i drugih vjerodajnica. Česti su i upadi u mrežu kroz neovlašteni ulazak u memoriju privatnih mobitela, kao i mreža pravne osobe u kojoj žrtva radi putem prisvojenih zaporki i korisničkih imena, a radi stjecanja nekih znanja i informacija za daljnju prodaju (baza korisnika, lozinki i PIN-ova ili *e-mailova*). Sve su češće ciljevi socijalnog inženjeringa i terorističke prirode (npr. upad u sustav elektroprivrede[4]).

[2] Wang, Z., Zhu, H., Liu, P. *et al.* Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecur* 4, 31 (2021).
[3] Anderson, R. J. (2008). Security engineering: a guide to building dependable distributed systems. Indianapolis, IN: Wiley.
[4] Energetika-net. https://www.energetika-net.com/energetsko-gospodarstvo/kako-je-izgledao-kiberneticki-napad-na-hse (1.12.2024.)

Industrijska špijunaža[5] kao oblik socijalnog inženjeringa gdje se iz konkurentskog poduzeća nastoje prisvojiti razne informacije (poput različitih znanstvenih studija unapređenja i razvoja proizvoda ili patenata) s ciljem eliminacije konkurencije isto je sve zastupljeniji način prijevara. Vrlo su česti i razni oblici krađa identiteta u kojima počinitelji iskorištavaju potrošačke trendove da bi izvršili prevaru budućeg kupca. Takve krađe identiteta se prvenstveno događaju na ilegalnim stranicama za *streaming*, neprovjerenim maloprodajnim stranicama i putem društveni medija. Rast takvih prijevara potaknut je i rastom kupnji putem interneta.

Pretpostavka da ljudi postaju žrtve takvih prijevara jer su neupućeni, naivni ili pohlepni kao što tvrde neki autori (King & Thomas, 2008)[6] tijekom vremena je oborena. Danas dobar dio socijalnih inženjera iskorištava ljudske slabosti kako bi dobili željena ponašanja i privilegirane informacije putem psihološki konstruirane komunikacije. Prema Atkinsku i Huangu (2013) Oni vješto manipuliraju žrtvama tako da ih dovode u emocionalno ranjiva stanja.[7]

Prema pozitivnim propisima u nacionalnom zakonodavstvu napadi socijalnih inženjera sankcioniraju se prema odredbama kaznenog zakonodavstva. U Kaznenom zakonu[8] postoji posebna glava: Kaznena djela protiv računalnih sustava, programa i podataka[9]. Bića kaznenih djela definiraju se u osam članaka: Neovlašteni pristup, Ometanje rada računalnog sustava, Oštećenje računalnih podataka, Neovlašteno presretanje računalnih podataka, Računalno krivotvorenje, Računalna prijevara, Zlouporaba naprava i Teška kaznena djela protiv računalnih sustava, programa i podataka. Početkom 2024. godina na snagu je stupio Zakon o kibernetičkoj sigurnosti[10]. On ima dvije osnovne smjernice: jedna je obveza upravljanja sigurnosnim rizicima, a druga je obveza izvješćivanja nadležnih tijela o svim kibernetičkim napadima i novim pojavnim oblicima napada.

2. Strategije socijalnog inženjeringa

Strategije socijalnog inženjeringa dijele se na direktne manipulacije, razne psihološke

[5] Currentware. https://www.currentware.com/blog/corporate-espionage-cases/ (1.12.2024.)
[6] King, A., & Thomas, J. (2009), You can't cheat an honest man: Making ($$$s and) sense of the Nigerian e-mail scams. In F. Schmallegar, & M. Pittaro (Eds.), Crimes of the internet (206-224). Saddle River, New Jersey: Pearson Education.
[7] Atkins, B., Huang, W. (2013), A Study of Social Engineering in Online Frauds. Open Journal of Social Sciences 1, 23-32.
[8] Kazneni zakon. NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24.
[9] Ibid. glava dvadeset peta (XXV) .
[10] Zakon o kibernetičkoj sigurnosti. NN 14/24.

tehnike, fizičke tehnike, te na napredne tehnike.

Phishing je najzastupljenija tehnika direktne manipulacije. Postoji više verzija izvođenja *phishinga*, s karakterističnim značajkama. Glavna je karakteristika da se od žrtve prikupljaju podaci poput imena i prezimena, adrese, OIB-a, datuma rođenja i drugi osobni podaci koji često ni nisu tajni i uglavnom su javno dostupni. I sami korisnici društvenih mreža takve podatke čine dostupnima. Uz to, vrlo često se objavljuju i fotografije koje otkrivaju stil života (npr. interes je planinarenje, vrtlarenje, filatelija)[11]. *Phishing* predstavlja opasnost i jer se putem tako prikupljenih informacija, najčešće e-mailova šalju poruke s linkovima koji preusmjeruju na neku „važnu" stranicu, stranicu za ažuriranje ili na neku važnu informaciju i uputu[12]. Adrese takvih stranica najčešće se razlikuju u jednom slovu ili znaku od iste takve, ali stvarne i autentične[13]. Lažiranje poveznica često je i pomoću znaka @[14]. Lažna poveznica može biti skrivena i ispod slike koja je skinuta sa originalne stranice, nalijepljena u *phishing* e-mail. Ispod takve slike potpuno je druga adresa koja upućuje na lažni *login*, traži da se ponovi prijava (zbog primjerice pogreške kod prijave) i traži da se potvrdi identitet jer je došlo do greške prilikom prijenosa podataka. Važna značajka *phishinga* je stvoriti osjećaj nesigurnosti i potrebe za što bržim djelovanjem jer u protivnom će se propustiti neka pogodnost ili ostati bez nečeg korisnog. Cilj je da se na ponuđene linkove klikne što prije kako se ne bi utrošilo vrijeme na provjeravanje. Ljudska osobina da želimo obaviti nešto brzo, efikasno i uspješno u slučaju socijalnog inženjeringa iskorištena je u korist takvih prijevarnih postupanja. Jedan od problema predstavlja i činjenica da se takve metode *phisinga* u modernom marketingu koriste jako često. Prema podacima Hrvatske udruge digitalnih oglašivača[15] u tržište digitalnog oglašavanja tj. digitalni marketing u Republici Hrvatskoj u 2023. godini uloženo je približno 280 milijuna eura. Vidljiv je i komercijalni rast i utjecaj digitalnog marketinga na cjelokupno tržište. Kao primjer protuzakonitog djelovanja u tome području česta je (dopuštena) praksa da se da se ne vidi izvor ili naručitelj lažnih objava i reklama. Problem nastaje jer pružatelji medijskih

[11] Interes je važan podatak za socijalni inženjering jer se tako mogu ponuditi povoljni proizvodi za prezentirani interes (sad i nikad više), povoljna putovanja (uplata prve rate unaprijed, uplata osiguranja putovanja, još neki naknadno iskrsnuli troškovi).

[12] Više o ranjivostima u bakarskom sektoru vidi 1. Perotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. A formal classification of internet banking attacks and vulnerabilities. Int. J. Compute. Sci. Inf. Technol. 2011, 3, 186–197.

[13] Primjerice https://www.paypal.com vs. https://www.paypol.com, https://internetbanking.pbz.hr/web/logon vs. https://internetbankaing.pzb.hr/web/logon. Linkovi koje šalju počinitelji u takvim phishing email porukama su uglavnom dugi.

[14] Adresa https://www.amazon.com@prijava.com/ izgleda kao poveznica koja vodi na prijavu na Amazon, a zapravo vodi na lažiranu stranicu prijava.com na kojoj ćete ukucati svoje podatke, user i lozinku misleći da se prijavljujete na Amazon.

[15] Istraživanje istraživanja HUDI Digitalni AdEx za 2023. godinu, https://adex.hudi.hr/.

usluga (portali) za audiovizualnu komercijalnu distribuciju, angažiraju treće subjekte (oglašivačke platforme) sa hardverom i softverom i zakupljenim hostovima na kojima se ti sadržaji spremaju. Oglašivačke platforme se pritom smatraju odgovornima samo za sigurno spremanje sadržaja, a ne i sam sadržaj. U samom procesu stvaranja oglašivačkog sadržaja na portalima, sudjeluju četiri strane: oglašivači, oglašivačke platforme, nadležna regulatorna tijela i sami korisnici, čitaoci i konzumenti internetskog sadržaja.[16] Oglašivači bi trebali biti odgovorni za sadržaj koji plasiraju i način na koji ga plasiraju, moralno, prekršajno, ali i kazneno. Oglašivačke platforme bi trebale moderirati sadržaj, ali i razvijati alate i kontrolne mehanizme koji bi onemogućili plasiranje neadekvatnog sadržaja. Prema Sauri i dr. (2020) sasvim je uobičajeno i da poduzeća prikupljaju informacije o svojim kupcima i prate njihovo ponašanje sa svrhom upoznavanja njihovih želja i preferencija. Podaci koje korisnici generiraju kao rezultat aktivnosti na društvenim mrežama, web stranicama, digitalnim platformama ili u interakciji, stvaraju podatkovne točke koje nude važne informacije o demografskim i geografskim karakteristikama potencijalnih kupaca, kao i njihovim interesima i životnim navikama.[17]

Vishing je podmetoda *phishinga* a izvodi se pozivom na mobitel žrtve koji je tako strukturiran da izazove strah kod primatelja (primjerice zbog ugroženog bankovnog računa). Vrlo često se i žrtvu uvjeri da mora nazvati neki ponuđeni broj kako bi riješila određeni (lažni) problem. S druge strane je određena osoba koja se lažno predstavlja, ima pripremljene podatke od žrtve i na taj način pridobije konačno povjerenje i traženi podatak (primjerice PIN). Iza *vishinga* često postoji cijeli scenarij razvijen da bi se na prevaru dobili tajni podaci i informacije. U modele direktne manipulacije spada i *smishing*. Radi se o metodi prijevare SMS porukama. Izvođač socijalnog inženjeringa predviđa što će dalje poduzeti na gotovo svaki dati odgovor[18]. U oblike *phisinga* prema Vukeliću i dr. (2023) [19] spada i *malware phising* koji se odnosi na prijevare koje uključuju instaliranje ili pokretanje zlonamjernog koda, poznatog kao *malware*, na uređajima korisnika žrtava. Zlonamjerni softver također može biti skriven u datoteci privitka nekog privitka. Koristi se i *spear phising* gdje se iskorištavaju podaci koji su prikupljeni istraživanjem o navikama te društvenom i

[16] Vidi više, 1. Ivanković, D., Sjepanović J., Utjecaj oglašavanja i korisnički generiranog sadržaja na doživljaj o proizvodu // 8th International Scientific Conference CRODMA 2023: Book of Papers / Gregurec, Iva (ur.). Varaždin: Hrvatska udruga za direktni i interaktivni marketing (CRODMA), 2023. str. 29-39.

[17] Saura, J., Reyes-Menendez, A., Matos, N., Correia, M., & Palos-Sanchez, P. (2020). Consumer Behavior in the Digital Age. Journal of Spatial and Organizational Dynamics, 8, 190–194.

[18] Primjer smishinga su SMS poruke „Hrvatske pošte“, a koje nude link u kojem se traži potvrda osobnih podataka i plaćanje pritojbe kako bi se mogao podignuti paket koji je zalutao i putovao malo duže do cilja.

[19] Vukelić, B., Zvonarić, A. D., Protrka, N.: The Recognition of an E-Mail Phishing Cyberattack in Business Organizations, Policija i sigurnost, godina 32. (2023), broj 3, str. 304 – 316.

poslovnom životu određene osobe. Ti podaci se iskorištavaju putem lažnih poruka koristeći prava imena i radne uloge kako bi uvjerili žrtvu da je e-mail došao iz poznatog, legitimnog izvora. Prema istim autorima u oblike *phisinga* spada i *whaling* gdje napadači koriste društvene medije ili mrežne stranice raznih poslovnih subjekata kako bi pronašli nazive organizacija, direktore ili druge članove višeg menadžmenta. Zatim glume nekoga koristeći sličnu e-mail adresu. Poruke e-pošte mogu zahtijevati prijenos novca ili zahtijevati primatelja za pregled dokumenata.

Jedna od metoda socijalnog inženjeringa je i mamljenje (*baiting*) u kojoj se prema Chapagain i dr. (2024) napadači služe nuđenjem nečega poželjnog za namamljivanje žrtava[20]. Konkretno, napadač koristi mamac (npr. fizički uređaj, lažnu ponudu ili obećanje nagrade) kako bi naveo žrtvu na određenu akciju, poput otkrivanja poverljivih informacija ili instaliranja zlonamernog softvera. Najčešće se pritom koriste eksterne memorije, kao što su CD, DVD, USB stick, a na kojem su neki primamljivi sadržaji ili sadržaji koji su „besplatni". Cilj je da se medij stavi u računalo i pokrene. *Quid Pro Quo* metoda je slična *baitingu*, ali se uglavnom nudi usluga za uslugu. Najčešće se pristupa službenicima nekih državnih institucija ili kompanija i nudi im se usluga za uslugu. Primjerice dostava podataka o zaposlenicima u zamjenu za korištenje nekog servisa koji se inače plaća[21].

Scareware kao metoda koristi se zastrašivanjem, tj. iskorištavanjem strahova ljudi za sigurnost računala i mobitela. Funkcionira tako da se najčešće u obliku pop-up oglasa dobije poruka da je mobitel u opasnosti. Žrtva odmah instalira najnoviji antivirusni program koji je zapravo *malware*. Putem tog programa se otkrivaju osobni podaci. Nakon *scarewarea* često slijedi i *ransomware*. Žrtve *scarewarea* dobiju prijetnju da će njihove privatne informacije, fotografije biti javno podijeljene ako im se ne plati određena svota novaca[22].

Tailgating (poznati i kao *piggybacking*) metoda je u kojoj se koristi fizički pristup. Namjera je da počinitelj uđe u zaštićene prostorije uz dobru lažnu priču ili na način da koristi nepažnju ostalih osoba. Često se počinitelj žrtvi predstavi kao dostavljač, poštar, električar, uz pokazivanje službene iskaznice i u službenoj odori. Cilj je ući u prostore poput server soba ili ureda u kojima se čuvaju povjerljive informacije. Prema Syafitri i dr. (2022)[23] ključno je da počinitelji mogu slobodno prolaziti kroz sigurnosni perimetar unutar

[20] Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. ArXiv, abs,, str.6.
[21] NordVPN. https://nordvpn.com/cybersecurity/glossary/quid-pro-quo-attack/(1.12.2024.)
[22] Cert. Surfaj sigurnije. https://www.cert.hr/scareware/ (1.12.2024.)
[23] Syafitri, W, Shukur, Z., Mokhtar, U.A., Sulaiman, R. and Ibrahim, M. A.,(2022), Social Engineering Attacks Prevention: A Systematic Literature Review, *IEEE Access*, vol. 10, str. 39325-39343.

organizacija.

U ovo područje spadaju i tzv. prevare menadžera i drugih izvršnih direktora (CEO *Fraud*[24]). U tim je prevarama cilj počinitelja da pridobije povjerenje nekog rukovoditelja, najčešće u financijama ili informatici prethodnom prepiskom e-mailom putem „službenih" dopisa, pa čak i fizičkim kontaktom. Scenarij u ovom slučaju mora biti sofisticiraniji jer je obrazovanje i znanje o sigurnosti žrtava veće.

3. Prevencija socijalnog inženjeringa

Neki su autori stajališta kako su napadi socijalnih inženjera trenutačno najveća prijetnja internetskoj sigurnosti (Arana, 2017; Chargo, 2018)[25]. Često je kao način zaštite dovoljno uložiti osnovne mjere opreza i sumnjičavosti prema neočekivanim i čudnim zahtjevima. Važna je i stalna nadgradnja znanja o informacijskoj sigurnosti. Neki od glavnih indicija da bi se moglo raditi o pokušajima krađe osobnih informacija su sumnjive SMS i e-mail poruke i telefonski pozivi koji se uporno ponavljaju, posebno treba biti oprezan prilikom davanja brojeva kreditnih kartica, lozinka ili drugih osjetljivih osobnih podataka.

Preventivno djelovanje u obrani od socijalnog inženjeringa podrazumijeva dodatan oprez prilikom obavljanja svakodnevnih uobičajenih poslova, primjerice otvaranja privitaka u e-mailovima, ili otvaranje sumnjivih URL adresa, čak i ako dolaze od poznatog pošiljatelja. Isto je tako važno razmisliti prije no što se osobne informacije objave na društvenim mrežama. Potrebno je kreirati jake lozinke sa više od osam znakova, koristiti mješovite znakove, brojeve i slova, velika i mala, redovno mijenjati lozinke, ne koristiti jednu lozinku za sve naše pristupe. Uputno je raditi redovni *update* softvera, pogotovo legitimnih antivirusnih softvera, instalirati *firewall* (vatrozid) te onemogućiti *Windows Autorun*.

Metode zaštite uključuju i sigurnosne politike (eng. *Security policy*) što ne znači samo ulaganje u hardver i softver za zaštitu (antivirusi, *antimalware*) već i ulaganje u znanje i razumijevanje zaposlenika. Kontinuirano se treba educirati sve zaposlenike, a već pri zapošljavanju, treba se postaviti psihološki i obrazovni profil koji budući zaposlenik treba zadovoljiti. Dobro je i osigurati da zaposlenici budu zainteresirani za takvo obrazovanje, odnosno nagrađivati one proaktivne.

[24] https://www.proofpoint.com/au/threat-reference/ceo-fraud

[25] Arana, M. (2017). How much does a cyberattack cost companies? Open Data Security, 1-4.; Chargo, M. (2018). You've been hacked: How to better incentivize corporations to protect consumers' data. Transactions: The Tennessee Journal of Business Law, 20, 115-143.

Važna je i kontrola pristupa koja je moguća na dva načina. Prvi je da se dozvoli pristup svemu, a postave se zabrane samo na određene informacije i resurse. Drugi način je obrnut, odnosno, sve je zabranjeno, i uz propisani zahtjev, dodjeljuju se prava na pristup određenim informacijama i resursima. Drugi način je sigurniji jer tu nema opasnosti da se zaboravi postaviti ograničenje pristupa na neku sigurnosno vrijednu informaciju, dokument ili drugi informatički resurs. U praksi bi bilo najbolje kombinirati ta dva načina, a to je u domeni stručnjaka za informacijsku sigurnost.

Bitan element je i fizička sigurnost koja podrazumijeva zabranu pristupa u prostorije s važnom informatičkom opremom, serverima i mjestima obrade tajnih podataka. Isto tako fizička sigurnost znači i pravilno zbrinjavanje otpadnih materijala, dokumenata, spisa (rezači papira, demagnetizacija diskova i drugih IT medija).

Poželjan način preveniranja je i obrana u više slojeva putem koje je potrebno odrediti koje su potencijalno slabe točke i ranjivosti i koji su mogući napadi. Glavna premisa obrane u više slojeva je ograničenost napadača. Da bi probio slijedeći sloj zaštite napadaču treba određeno vrijeme te ga se može u tom vremenu detektirati i onemogućiti. Važno je brzo prepoznavanje napada, a kako bi se onemogućilo napadaču brzo snalaženje i probijanje slijedećeg nivoa zaštite. Jedna od sofisticiranijih metoda borbe protiv socijalnog inženjeringa je postavljanje klopki (*eng. land mines*). Postavljanje klopki ili minskog polja može se izvoditi na više načina. Jedan od načina je putem središnjeg sigurnosnog dnevnika. To bi trebala biti log datoteka u koju se bilježe svi pozivi i zahtjevi za podacima, a posebno se označavaju oni sumnjivi. Na taj način moguće je uočiti pravilnosti i ponavljanja, npr. telefonskih brojeva ili IP adresa.

Služba za podršku korisnicima jedna je od slabijih točaka sigurnosti, te je tu poznata metoda povratnog poziva, tj. odmah nakon poziva, službenik poziva pozivatelja. Ako pozivatelj nije u službenom imeniku, ili u nekom od dozvoljenih imenika, potencijalno je opasan.

Europol je 2013. godine osnovao *European Cybercrime Centre* (EC3)[26], čiji je osnovni zadatak pomoći zemljama članicama EU u zaštiti građana, institucija i kompanija od *cyber* kriminala. Isto tako postavljeni su i zakonski okviri i osnove, a koje onda zemlje članice implementiraju i prilagođavaju svojoj zakonskoj regulativi u borbi protiv *cyber* kriminala. EC3 pomaže u razvoju strategija, operativno, analitički i forenzikom, na traženje zemlje članice. Zadatak EC3 je također, da svake godine izda IOCTA (*Internet Organised Crime Threat*

[26] Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, (1.12.2024.)

Assessment[27]) dokument kojim se stavlja naglasak na najznačajnije *cyber* prijetnje te godine, ističe nove načine djelovanja u *cyber* i organiziranom kriminalu. Isto tako definira i akcijski plan i protumjere i djelovanja u svakom području *cyber* kriminala. *Joint Cybercrime Action Taskforce* (J-CAT) „specijalci" su unutar EC3, a koordiniraju i sudjeluju u zajedničkim akcijama koje obuhvaćaju više država članica EU, zajedno sa policijom iz matičnih država. Eurojust kao Agencija EU za suradnju u kaznenom pravosuđu podupire pravosudnu koordinaciju i suradnju nacionalnih tijela u borbi protiv terorizma i organiziranog kriminala, pa prema tome i u borbi protiv cyber kriminala.

4. Zaključak

Socijalni inženjering predstavlja ključnu prijetnju informacijskoj sigurnosti, usmjerenu na iskorištavanje ljudskih slabosti i emocionalne ranjivosti radi neovlaštenog pristupa povjerljivim podacima. Napadači koriste različite tehnike poput *phishinga, vishinga, smishinga, baitinga i scarewarea* kako bi manipulirali žrtvama i ostvarili financijsku ili informativnu korist.

Budući da je ljudski faktor najslabija karika u sigurnosnom lancu, prevencija se temelji na edukaciji korisnika, jačanju svijesti o rizicima i uvođenju tehničkih mjera zaštite kao što su slojevite sigurnosne politike, kontrola pristupa i fizička sigurnost. Međutim, ne postoji univerzalna i jedinstvena metoda zaštite od socijalnog inženjeringa, tim više što se tehnike napada svakodnevno usavršavaju i mijenjaju. Važno je kritički pristupati svim sadržajima na internetu i društvenim mrežama. Sa zdravom dozom opreza ulaziti u bilo kakvu elektroničku komunikaciju, zatražiti vjerodajnice „digitalnog" sugovornika i provjeriti te vjerodajnice. Uvođenje dobre prakse kao i europskih i nacionalnih zakona i regulativa, poput Zakona o kibernetičkoj sigurnosti, dodatno jača pravni okvir za borbu protiv ovih prijetnji.

Literatura:

1. Anderson, R. J. (2008). Security engineering: a guide to building dependable distributed systems. Indianapolis, IN: Wiley.
2. Arana, M. (2017). How much does a cyberattack cost companies? Open Data Security, 1-4.
3. Atkins, B., Huang, W. (2013), A Study of Social Engineering in Online Frauds. Open Journal of Social Sciences 1, 23-32.

[27] Europol. https://www.europol.europa.eu/publications-events/main-reports/iocta-report, (1.12.2024.)

4. Cert. Surfaj sigurnije. https://www.cert.hr/scareware/ (1.12.2024.)
5. Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. ArXiv, abs.
6. Chargo, M. (2018). You've been hacked: How to better incentivize corporations to protect consumers' data. Transactions: The Tennessee Journal of Business Law, 20, 115-143.
7. Currentware. https://www.currentware.com/blog/corporate-espionage-cases/ (1.12.2024.)
8. Energetika-net. https://www.energetika-net.com/energetsko-gospodarstvo/kako-je-izgledao-kiberneticki-napad-na-hse (1.12.2024.)
9. Ghafir, I, Prenosil, V, Alhejailan, A. and Hammoudeh, M. (2016), Social engineering attack strategies and defence approaches.
10. Granger S. Social engineering fundamentals, part I: hacker tactics. Security Focus. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4182f6b99e9ca2efe6d3f3e9f3fd59ded36333dd (1.12.2024.)
11. Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), 537-540.
12. International Conference on Future Internet of Things and Cloud, Vienna, Austria, 22–24August 2016, https://www.ficloud.org/2016/ (1.12.2024.)
13. Ivanković, D., Sjepanović J., (2023), Utjecaj oglašavanja i korisnički generiranog sadržaja na doživljaj o proizvodu // 8th International Scientific Conference CRODMA 2023: Book of Papers / Gregurec, Iva (ur.). Varaždin: Hrvatska udruga za direktni i interaktivni marketing (CRODMA), str. 29-39.
14. Kazneni zakon. NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24.
15. King, A., & Thomas, J. (2009), You can't cheat an honest man: Making ($$$s and) sense of the Nigerian e-mail scams. In F. Schmallegar, & M. Pittaro (Eds.), Crimes of the internet (206-224). Saddle River, New Jersey: Pearson Education.
16. Mouton, F.et al. (2014), "Social engineering attack framework," Proc. of Information Security forSouth Africa (ISSA). 1-9.(poglavlje 3.1.)
17. NordVPN. https://nordvpn.com/cybersecurity/glossary/quid-pro-quo-attack/.(1.12.2024.)

18. Peltier, T. R., (2006),“Social engineering: concepts and solutions,” Information Security and RiskManagement, Nov., 13-21.(poglavlje 3.2.)
19. Perotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. (2011), A formal classification of internet banking attacks and vulnerabilities. Int. J. Compute. Sci. Inf. Technol, 3, 186–197.
20. Saura, J., Reyes-Menendez, A., Matos, N., Correia, M., & Palos-Sanchez, P. ,(2020). Consumer Behavior in the Digital Age. Journal of Spatial and Organizational Dynamics, 8, 190–194.
21. Syafitri, W, Shukur, Z., Mokhtar, U.A., Sulaiman, R. and Ibrahim, M. A.,(2022), Social Engineering Attacks Prevention: A Systematic Literature Review, IEEE Access, vol. 10, str. 39325-39343.
22. Wang, Z., Zhu, H., Liu, P. et al. (2021), Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecur 4, 31.
23. Zakon o kibernetičkoj sigurnosti. NN 14/24.
24. Zakon o obveznim odnosima. NN 35/05, 41/08, 125/11, 78/15, 29/18, 126/21, 114/22, 156/22, 155/23.