FAKULTET POLITIČKIH NAUKA
UNIVERZITET U SARAJEVU
MCMXLIX

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

INFORMACIJSKA PISMENOST U SEKTORU INFORMACIJSKE SIGURNOSTI: PRIJEDLOG MODELA U STRATEGIJI KORPORATIVNOG PRISTUPA

- magistarski rad -

Kandidat
Mersudin Šuman
Broj indeksa:
887/II – SPS

Mentor
Prof. dr. Emir Vajzović

Sarajevo, juni 2024.

SADRŽAJ

Skraćenice

IFIP	Međunarodna federacija za obradu informacija (engl. International Federation for Information Processing)
ISO	Međunarodna organizacija za normalizaciju (engl. International Organization for Standardization)
IT	Informacijske tehnologije
MFA	Multifaktorska autentifikacija
PII	Podaci koji otkrivaju identitet (engl. Personally identifiable information)
URL	Putanja do određenog sadržaja na Internetu te se obično naziva link

Popis tabela i slika

Uvod

Data, internet, email, chat, web, link, share, upload, cyber security... ovi anglizmi a ujedno i informacijsko – tehnološki pojmovi su u svakodnevnoj upotrebi, bez potrebe da ih prevodimo jer živimo u vremenu ogromnog tehnološkog napretka, gdje nam je informacija na dohvat ruke a tehnologija svuda oko nas. Globalna povezanost, razvoj tehnologije i digitalnog okruženja znači i da su efekti ovog razvoja sveobuhvatni - od pozitivnih i afirmativnih do onih rizičnih i negativnih efekata, porast broja zloupotreba informacijske tehnologije.[1]

U vremenu kada se informacije posjeduju, kupuju, prodaju a ne samo obrađuju, možemo konstatovati da informacije predstavljaju jednu od najvrijednije imovine u većini korporativnih okruženja, odnosno organizacija. Danas posjedovanje pravovremene, relevantne i tačne informacije može napraviti ogromnu razliku u poslovanju, koja može donijeti finansijsku ili neku drugu korist. Zaštita i sigurnost ovakvih informacija bi trebala biti prioritet u svim organizacijama bilo da su male, srednje ili velike.

Napadi na informacijske sisteme više nisu samo rezultat napadačevih želja pokazivanja svog znanja, demonstracije moći u digitalnom svijetu. Napadi prvenstveno imaju za cilj ostvarivanje financijske ali i neke druge koristi. Incidenti povezani sa informacijskom sigurnošću mogu imati operativne, finansijske, reputacijske i strateške posljedice za organizaciju bilo kratkoročno ili dugoročno. Promijenjena je i meta napada, tako da se više ne napada samo računar ili sistem, nego korisnik, odnosno čovjek.[2] Prijetnje informacijskoj sigurnosti mogu proizlaziti kako iz vanjskih izvora, uključujući cyber napade i zlonamjerne aktivnosti, tako i unutar organizacije, poput neodgovornog rukovanja osjetljivim podacima od strane zaposlenika ili neautorizovanog pristupa internim sistemima.[3]

Prema novijim objavljenim istraživanjima, pandemija koronavirusa kao i rat u Ukrajini, motivisala je cyber kriminalce da pojačano koriste razne vrste cyber napada, sto je dovelo da su troškovi

[1] OSCE. (2019). *Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini*. Sarajevo. Retrieved from https://www.osce.org/files/f/documents/4/8/438386.pdf
[2] Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. *Computer Security*, 28(3-4), 189-198.
[3] Möller, D. P. F. (2023). *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices*. Springer Nature Switzerland.

izazvani povredom podataka u 2022. godini iznosili su 4,35 miliona dolara, što je povećanje od 12,7% u odnosu na 2020. kada je trošak iznosio 3,86 miliona dolara.[4] Ljudski element igrao je ulogu u 82% svih kršenja analiziranih tokom 2022. godine, dok su ransomware napadi porasli za 13%, što je skok veći od proteklih 5 godina zajedno.[5]

I pored navedenog, svjedoci smo da u nekim slučajevima informacijska sigurnost, odnosno zaštita informacija i podataka u korporativnim okruženjima nije na nivou kakvom bi trebala biti. Edukacija zaposlenih o informacijskoj sigurnosti ne postoji ili ukoliko postoji nije prilagođena stvarnim potrebama. Često se stiče dojam da implementirane sigurnosne mjere smetaju uposlenicima u bržem i učinkovitijem obavljanju njihovih zadataka[6]. Opseg napada i ključna uloga ljudi u dopuštanju tih napada, stavlja potrebu za edukacijom zaposlenih o informacijskoj sigurnosti organizacije u prvi plan. Ovakvim programima za izgradnju razumijevanja cyber rizika, uposlenima omogućuju da identifikuju i reaguju na sumnjive aktivnosti kada ih otkriju u svojoj organizaciji kako bi se izbjegle pogreške s osjetljivim podacima. Dokazano je da najveća prijetnja po informacijsku sigurnost organizacije dolazi od samih njenih uposlenika odnosno iznutra. Prema svjedočenju osuđenog hakera (engl. hacker)[7] Kevina Mitnicka, u svjedočenju pred Senatom SAD-a, Komitetom za vladine poslove (Mart, 2000.) "*Ljudska strana kompjuterske sigurnosti lako se iskorištava i stalno se zanemaruje. Kompanije troše milione dolara na firewall-e, enkripciju i uređaje za siguran pristup, a to je bačen novac jer se nijedna od ovih mjera ne odnosi na najslabije karike u sigurnosnom lancu: ljude koji koriste, administriraju, rade na računarskim sistemima koji sadrže zaštićene informacije*." [8]

Puko investiranje u sigurnost mreže, računarskih mreža, servera, itd. bez edukacije zaposlenika pa i u nekim slučajevima korisnika, postalo je nesvrsishodno. Organizacije koje žele da prežive u

[4] IBM Security. (2023). *Cost of a data breach report 2023*. Retrieved from https://www.ibm.com/downloads/cas/E3G5JMBP
[5] Hylender, D. (2022). *Verizon 2022 data breach investigations report*. Verizon. Retrieved from https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report
[6] Alsmadi, I., et al. (2018). *Practical information security: A competency-based education course* (1st ed.). Springer International Publishing.
[7] *haker (engl. hacker), osoba dobro upućena u računala, računalne mreže ili programiranje, no time se bavi na svoju ruku, kadšto i prelazeći granicu dopuštenoga (neovlašteno pristupanje računalnim sustavima, probijanje zaštita programa od kopiranja i sl.)*. Leksikografski zavod Miroslav Krleža. (2013-2024). *Hrvatska enciklopedija, mrežno izdanje*. Retrieved April 25, 2024, from https://www.enciklopedija.hr/clanak/haker
[8] United States Senate, Committee on Governmental Affairs. (2000). *Cyber attack: Is the government safe?: Hearing before the Committee on Governmental Affairs, United States Senate, One Hundred Sixth Congress, Second Session, March 2, 2000*. U.S. Government Printing Office.

budućnosti moraće razviti sveobuhvatan pristup informacijskoj sigurnosti, podjednako posvećujući pažnju kako na razvoj tehničkih tako i ljudskih kapaciteta.

I. TEORIJSKE OSNOVE RADA

U današnjem digitalnom dobu, informacijska pismenost i informacijska sigurnost su ključni aspekti poslovanja koji imaju sve veći uticaj na uspjeh organizacija. Pravilno razumijevanje i integracija ovih elemenata postali su imperativ za sve organizacije koje žele da zaštite svoje podatke, osiguraju integritet informacija i odgovore na sve složenije sigurnosne izazove. Stoga, ovaj rad se fokusira na analizu odnosa između informacijske pismenosti i informacijske sigurnosti kao osnovnih stubova sigurnosti u organizaciji.

U kontekstu informacijske sigurnosti, informacijska pismenost zaposlenika igra ključnu ulogu. Zaposlenici trebaju biti osposobljeni za prepoznavanje i razumijevanje sigurnosnih prijetnji, kao i za primjenu sigurnosnih postupaka i mjera. Informacijska pismenost omogućuje zaposlenima da kritički razmišljaju o informacijama, procjenjuju njihovu pouzdanost i autentičnost te donose informisane odluke o sigurnosnim pitanjima. Osim toga, informacijska pismenost zaposlenika pomaže u jačanju svijesti o sigurnosnim rizicima i promovisanju sigurnosne kulture unutar organizacija. Kroz obrazovanje, treninge i svjesnost o sigurnosnim postupcima, zaposleni postaju aktivni učesnici u zaštiti informacijske sigurnosti i pridonose smanjenju sigurnosnih propusta i incidenata.

Kroz integraciju modela Christine Bruce "The Seven faces of information literacy"[9] u kontekstu informacijske sigurnosti, istraživanje ima za cilj pružiti teorijsku podlogu za razumijevanje važnosti informacijske pismenosti u održavanju informacijske sigurnosti organizacija.

Prvi dio rada pruža uvid u informacijsku sigurnost od njenog nastanka pa do danas. Drugi dio rada pruža uvid u važnost informacijske pismenosti kao temeljnog koncepta za razumijevanje i efikasno upravljanje informacijama unutar organizacija. U trećem dijelu rada, kroz detaljnu analizu

[9] Bruce, C. (1997). *The seven faces of information literacy*. Auslib Press.

sigurnosnih logova, prikupljenih u periodu od januara do augusta 2023. godine, generisanih od različitih sigurnosnih sistema koji su implementirani u organizacijama, dobili smo detaljan uvid u učestalost i vrste sigurnosnih prijetnji. Pored toga, istraživanje je obuhvatilo i kontrolisana phishing[10] testiranja. Cilj ovih testova bio je ocijeniti sposobnost zaposlenika da prepoznaju i adekvatno reaguju na simulirane phishing napade. Analiza rezultata ovih testova pružila je kvantitativne podatke o uspješnosti zaposlenika u borbi protiv phishing napada, što je ključno za evaluaciju postojećih sigurnosnih edukacija i obuka u organizacijama. Kombinacija analize sigurnosnih logova i phishing testiranja pruža sveobuhvatan uvid u sigurnosne prijetnje i sposobnosti organizacije u njihovom suočavanju. Četvrti dio rada fokusira se na model programa obuke za ne-tehničke zaposlenike u korporativnom okruženju. Kroz razmatranje prilagođenih strategija za učenje na daljinu i učenje u razredu, predlaže se kako organizacije mogu učinkovito obučiti svoje osoblje za odgovor na savremene sigurnosne izazove i unaprijediti ukupnu sigurnost informacija.

Ovaj rad ima za cilj pružiti sveobuhvatan pregled odnosa između informacijske pismenosti i informacijske sigurnosti, te predložiti program obuke u cilju unapređenja sigurnosti organizacija u digitalnom okruženju.

II. METODOLOŠKI OKVIR RADA

1. Problem istraživanja

Fokus ovog rada je prevazilaženje nedostatka sveobuhvatnog pristupa informacijskoj sigurnosti u organizacijama, koji uzima u obzir tehničke, organizacijske i ljudske aspekte. Nedostatak informacijske pismenosti zaposlenih može predstavljati rizik za sigurnost organizacije, a postojeći pristupi obuci i svijesti mogu biti nedovoljni. Stoga je potrebno istražiti povezanost između informacijske pismenosti i implementacije informacijske sigurnosti te identifikovati ključne faktore i prepreke u ovom procesu. Također je važno razumjeti kako unaprijediti informacijsku pismenost zaposlenika i implementaciju informacijske sigurnosti radi osiguranja opstanka organizacije u

[10] Phishing ili mrežna krađa identiteta je prevara koja podrazumijeva aktivnosti kojima neovlašteni korisnici korištenjem lažiranih e-poruka ili web stranica pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka.

narednim godinama.

2. Predmet istraživanja

Predmet istraživanja je proučavanje uticaja informacijske pismenosti zaposlenika na proces informacijske sigurnosti u organizacijama. Fokus istraživanja je razumijevanje kako informacijska pismenost zaposlenika utiče na njihovu sposobnost prepoznavanja, sprječavanja i reagovanja na sigurnosne prijetnje. Istraživanje se također bavi proučavanjem različitih aspekata informacijske pismenosti, uključujući znanje o sigurnosnim postupcima, vještine kritičkog razmišljanja, svjesnost o sigurnosnim rizicima i spremnost za usvajanje sigurnosnih praksi. Cilj je identifikovati ključne faktore informacijske pismenosti koji doprinose poboljšanju informacijske sigurnosti te razviti preporuke i smjernice za unapređenje informacijske pismenosti zaposlenika u svrhu jačanja sigurnosti organizacija.

2.1. Kategorijalno pojmovni sistem

Da bi se mogli organizovati i sistematizovati ključni elementi istraživanja kako bi se obezbijedila jasna i koherentna analiza, kategorijalno pojmovni sistem za istraživanje „Informacijska pismenost u sektoru informacijske sigurnosti: prijedlog modela u strategiji korporativnog pristupa“ može se strukturisati kroz nekoliko ključnih kategorija i pojmova.

Informacijska pismenost - skup vještina, stavova znanja potrebnih za rješavanje problema i donošenja odluka, oblikovanje informacijske potrebe u izraze za pretraživanje, učinkovito pretraživanje, interpretaciju, razumijevanje, organiziranje, vrednovanje vjerodostojnosti i autentičnosti te relevantnost informacija.[11] Komponente: kritičko razmišljanje, procjena pouzdanosti informacija, donošenje informiranih odluka.

Informacijska sigurnost - obuhvata zaštitu informacija i informacijskih sistema od neovlaštenog pristupa, upotrebe, otkrivanja, ometanja, izmjene ili uništavanja kako bi se obezbijedila povjerljivost, integritet i dostupnost.[12] Aspekti: sigurnosne prijetnje, sigurnosni incidenti,

[11] Horton, F. W. (2008). Understanding information literacy: A primer. Paris: UNESCO.
[12] National Institute of Standards and Technology. (n.d.). NIST SP 1800-10B under information security from FIPS 199, 44 U.S.C., Sec. 3542 of NIST. Američki Nacionalni Institut za Standarde i Tehnologiju.

sigurnosne politike i procedure.

Korporacija (engl. corporation, franc. corporation < kasnolat. corporatio: tjelesna građa, od lat. corporare: oblikovati u tijelo; udružiti, od corpus: tijelo; udruženje, savez), - u suvremenom pravu i ekonomskim sustavima, udruga ili organizacija koja kao pravna osoba zastupa interese svojih pripadnika, štiti njihova prava, ostvaruje svojom djelatnošću određene zajedničke gospodarske, socijalne, vjerske ili koje druge ciljeve.[13]

Organizacija - ukupnost osoblja neke ustanove, poduzeća, kolektiva uopće, kao i organizacijska struktura njihove ukupne ili djelomične djelatnosti (radna organizacija, organizacija prodaje, organizacija gradilišta i dr.)[14]

Edukacija (lat. educatio), - temeljni uvjet postojanja i opstanka ljudske zajednice. Na individualnoj razini obuhvaća proces stjecanja znanja, umijeća i navika, razvijanje tjelesnih, intelektualnih, moralnih, estetskih i radnih sposobnosti i dr.[15]

3. Ciljevi istraživanja

Ciljevi istraživanja u ovom radu su:

1. Ispitati povezanost između informacijske pismenosti i implementacije informacijske sigurnosti u organizacijama.
2. Analizirati uticaj informacijske pismenosti zaposlenika na efektivnost informacijske sigurnosti u organizacijama.
3. Prepoznati ključne faktore i prepreke u implementaciji informacijske sigurnosti u organizacijama.
4. Pružiti preporuke za unapređenje informacijske pismenosti i implementaciju informacijske sigurnosti u organizacijama.

[13] Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. <https://www.enciklopedija.hr/clanak/korporacija>.
[14] Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. <https://www.enciklopedija.hr/clanak/organizacija>.
[15] Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. <https://www.enciklopedija.hr/clanak/edukacija>

3.1. Naučni cilj

Naučna opravdanost istraživanja ima za cilj unaprijediti naučno saznanje i razumijevanje implementacije informacijske sigurnosti u organizacijama, sa naglaskom na sveobuhvatnom pristupu informacijskoj pismenosti u kontekstu informacijske sigurnosti. Ovo istraživanje doprinosi razumijevanju promjena u tehnologijama i rizicima, te zahtijeva primjenu sistematskih teorijskih i empirijskih istraživanja. Također, provjera i usavršavanje metoda istraživanja igraju važnu ulogu u naučnoj kritici i razvoju naučnih saznanja u ovoj oblasti.

Kada govorimo o informacijskoj pismenosti u sektoru informacijske sigurnosti, naučni cilj istraživanja je istražiti i razumjeti razinu informacijske pismenosti zaposlenika u pogledu razumijevanja i primjene sigurnosnih praksi i politika. Drugi cilj istraživanja je identifikovati nedostatke u informacijskoj pismenosti zaposlenika u vezi s informacijskom sigurnošću te razviti strategije i metode za poboljšanje njihove informacijske pismenosti. Rezultanta ova dva cilja je u razvoju novih pristupa koji će osnažiti zaposlenike da bolje razumiju i primjenjuju sigurnosne mjere u svom radnom okruženju.

3.2. Društveni cilj

Društveni cilj ovog rada je izrada modela implementacije programa informacijske pismenosti u oblasti informacijske sigurnosti namijenjen ne-tehničkim uposlenicima u korporativnom okruženju temeljeći se na tri fundamentalna koncepta: informacijsko opismenjavanje, informacijsko ponašanje i informacijska pismenost sa ciljem podizanja nivoa cyber-sigurnosti u svakodnevnom poslovanju. Dodatni razlog leži u činjenici da se profesionalci u oblasti informacijske sigurnosti obrazuju u procesu formalnog obrazovanja odabirući ovu oblast kao karijerno opredijeljenje, a programi informacijske sigurnosti namijenjeni širokoj populaciji su gotovo nepostojeći, ili su visoko fragmentirani unutar opštih programa informacijske pismenosti.

4. Sistem hipoteza

4.1. Generalna hipoteza

Nedostatak adekvatne edukacije zaposlenih o informacijskoj sigurnosti značajno doprinosi povećanju rizika od cyber napada i zloupotreba unutar korporativnih okruženja, što implicira da sveobuhvatni pristup informacijskoj sigurnosti mora podjednako uključivati razvoj tehničkih sistema i unapređenje ljudskih kapaciteta.

4.2. Posebne hipoteze:

a) Obavezan trening uposlenih o informacijskoj sigurnosti tokom godine dovodi do značajnog smanjenja unutrašnjih sigurnosnih prijetnji.
b) Redovno provođenje treninga o informacijskoj sigurnosti smanjuje broj sigurnosnih incidenata u organizaciji izazvanih ponašanjem zaposlenih.
c) Redovno provođenje treninga o informacijskoj sigurnosti smanjuje broj phishing napada koji uspješno prevare korisnike.
d) Redovno provođenje simuliranih phishing sigurnosnih testova povećava sposobnost zaposlenika da prepoznaju phishing napade i druge oblike socijalnog inženjeringa.

4.3 Sistem varijabli

Nezavisna varijabla:

- Obuka i edukacija o informacijskoj sigurnosti (prisutnost ili odsutnost obuke).
- Vremenski period tokom kojeg se mjerenje vrši (npr. januar, februar, mart, itd.).

Zavisne varijable:

- Broj sigurnosnih incidenata u organizaciji (broj zabilježenih cybersecurity incidenata).
- Sposobnost prepoznavanja phishing napada i socijalnog inženjeringa (broj neuspješno prepoznatih napada).
- Broj unutrašnjih sigurnosnih prijetnji u organizaciji.

4.4 Sistem indikatora

1. Indikatori informacijske obuke zaposlenika:
    - Prisustvo Treninga: 1 (da), 0 (ne)

2. Indikatori vremenskog perioda tokom kojeg se mjerenje vrši:
    - Vrijednosti koje predstavljaju mjesece prije i poslije održane edukacije.
3. Indikatori sigurnosnih incidenata u organizaciji:
    - Apsolutni broj incidenata.
4. Indikatori prepoznavanja phishing napada i socijalnog inženjeringa:
    - Apsolutni broj neuspješno prepoznatih phishing napada u testiranju.
5. Indikatori prepoznavanja unutrašnjih prijetnji:
    - Apsolutni broj unutrašnjih prijetnji.

5. Način istraživanja

Ovo istraživanje je teorijsko – empirijskog karaktera. U teorijskom pogledu, oslanja se na postojeća teorijska saznanja o informacijskoj sigurnosti i informacijskoj pismenosti. Empirijski dio uključuje prikupljanje i analizu stvarnih podataka kako bi se utvrdili ključni faktori i prepreke u implementaciji informacijske sigurnosti u organizacijama.

Pristup ovom istraživanju je integralno-sintetički, gdje se ne favorizuje niti jedan teorijsko-metodološki pravac, te predstavlja jedan sveobuhvatan pogled na temu istraživanja.

Osnovne metode naučnog saznanja koje su primijenjene u naučnom istraživanju su analiza, apstrakcija, dedukcija, indukcija, sinteza. Posebno će biti stavljen fokus na analizu sadržaja sigurnosnih logova i postojećih podataka, a onda i sinteza, kako bi se stekao kompletan uvid o cijelosti ovog pitanja.

Za potrebe naučnog istraživanja, primijenjene su osnovne i opšte-naučne metode naučnih istraživanja. Za potrebe empirijskog istraživanja, koristile su se metode pribavljanja podataka: analiza sigurnosnih logova, metod ispitivanja (testiranje socijalnog inženjeringa), analiza postojećih podataka.

6. Naučna i društvena opravdanosti istraživanja

Naučna opravdanost istraživanja informacijske sigurnosti i informacijske pismenosti zaposlenika leži u potrebi za proširenjem postojećeg naučnog saznanja u ovom području. Studija će doprinijeti teorijskom i empirijskom razumijevanju veze između informacijske pismenosti zaposlenika i implementacije informacijske sigurnosti u organizacijama. Identifikacija i analiza ključnih faktora informacijske pismenosti i njihov utjecaj na sigurnost podataka pomoći će u razvoju efikasnih strategija za unapređenje informacijske sigurnosti.

Društvena opravdanost istraživanja leži u važnosti informacijske sigurnosti u današnjem digitalnom dobu. Sa sve većim brojem sigurnosnih prijetnji i incidenta, organizacije se suočavaju sa sve većim rizicima gubitka osjetljivih podataka i povrede privatnosti. Informacijska pismenost zaposlenika igra ključnu ulogu u zaštiti organizacija od takvih prijetnji. Ovaj rad će pružiti uvid u važnost informacijske pismenosti u kontekstu informacijske sigurnosti, što će pomoći organizacijama da razviju politike, obuke i strategije koje će osigurati bolju zaštitu podataka i smanjenje rizika.

Istraživanje informacijske sigurnosti i informacijske pismenosti zaposlenika ima naučnu opravdanost jer doprinosi postojećem znanju u ovom području, dok ima društvenu opravdanost jer pruža smjernice za zaštitu organizacija od sigurnosnih prijetnji i očuvanje povjerenja u digitalnom okruženju. Ovim istraživanjem također se može doprinijeti unapređenju informacijske pismenosti u širem društvenom kontekstu. Poboljšanje informacijske pismenosti zaposlenika može značajno unaprijediti njihovu sposobnost suočavanja s digitalnim informacijama, razumijevanje privatnosti, prepoznavanje lažnih vijesti i ostalih izazova digitalne ere. Ukratko, naučna opravdanost istraživanja leži u doprinosu teoriji informacijske sigurnosti, dok društvena opravdanost proizlazi iz potencijalnih koristi za organizacije i društvo u cjelini u pogledu jačanja informacijske sigurnosti i unapređenja informacijske pismenosti.

7. Vremensko i prostorno određenje istraživanja

Vremensko određenje istraživanja je period od dvije godine, 2022-2023. u različitim zemljama u Evropi, Bliskom istoku i Africi, s ciljem dobivanja reprezentativnih rezultata na globalnoj razini.

Prvi dio

INFORMACIJSKA SIGURNOST

Informacijska sigurnost (engl. Information Security) obuhvata zaštitu informacija i informacijskih sistema od neovlaštenog pristupa, upotrebe, otkrivanja, ometanja, izmjene ili uništavanja kako bi se obezbijedila povjerljivost, integritet i dostupnost.[16] Međunarodna organizacija za normizaciju (engl. International Organization for Standardization, ISO) također ima definiciju informacijske sigurnosti. Prema njihovoj definiciji, informacijska sigurnost se odnosi na „*očuvanje povjerljivosti, integriteta i dostupnosti informacij*a."[17] Obje definicije naglašavaju važnost očuvanja povjerljivosti, integriteta i dostupnosti informacija, što su osnovni ciljevi informacijske sigurnosti.

Prije nego definišemo i elaboriramo informacijsku sigurnost, korisno je postaviti opštu definiciju sigurnosti, za koju možemo reći da „općenito podrazumijeva stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države" i međunarodnih odnosa, pa i na kosmičkom i planetarnom nivou života općenito, ljudskoga roda u cjelini „od svih vidova ugrožavanja"[18]. Sigurnost podrazumijeva stepen zaštićenosti od ugrožavanja, uz naglasak da ne postoji apsolutna i potpuna sigurnost, već možemo govoriti o većem ili manjem stepenu sigurnosti. „U tom kontekstu moguće je zaključiti da informacijska sigurnost jeste stanje i praksa zaštite infrastrukture, informacijsko-komunikacijskih sistema, mreža, uređaja i informacija od ugrožavanja, u cilju zaštite ljudi, materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države i međunarodnih odnosa."[19]

Iako postoje mnoge definicije informacijske sigurnosti, sve naglašavaju važnost očuvanja sigurnosti informacija i informacijskih sistema, što je ključno za zaštitu od štetnih posljedica koje nastaju iz

[16] National Institute of Standards and Technology. (n.d.). *NIST SP 1800-10B under information security from FIPS 199, 44 U.S.C., Sec. 3542 of NIST*. Američki Nacionalni Institut za Standarde i Tehnologiju.
[17] International Organization for Standardization. (2018). *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
[18] Beridan, I. (2007). Politika i sigurnost - sadržaj i obilježja pojmova. U Fakultet političkih nauka – Godišnjak 2007 (str. 99-121).
[19] Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti = Media and information literacy in cyber security system. *Kriminalističke Teme,* (5), 529-543. http://krimteme.fkn.unsa.ba/index.php/kt/article/view/240

neovlaštenog pristupa, zloupotrebe ili krađe informacija sa naglaskom na povjerljivost, integritet i dostupnost informacija.

Šta tačno podrazumijevaju povjerljivost, integritet i dostupnost i kako oni pomažu u zaštiti organizacija od sigurnosnih incidenata objasnićemo pomoću CIA trijade[20], modela informacijske sigurnosti osmišljenog za zaštitu osjetljivih informacija. Principi na kojim počiva CIA trijada (eng. CIA triad) široko je prihvaćeno načelo unutar industrije. Tako ISO/IEC 27001 međunarodni standard za upravljanje sigurnošću informacija koji specificira zahtjeve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sistema upravljanja sigurnošću informacija (ISMS), dizajniran je da osigura **povjerljivost, integritet i dostupnost** informacija unutar organizacije.[21] Ovi principi se spominju i u Opštoj uredbi o zaštiti podataka (GDPR), u članu 32. koji između ostalog navodi da organizacije moraju „*provesti odgovarajuće tehničke i organizacijske mjere kako bi osigurale* ***povjerljivost, integritet, dostupnost*** *i otpornost sustava i usluga obrade.*“[22]

Ilustracija 1. CIA trijada

Prema (Nikander, Jussi & Manninen, Onni & Laajalahti, Mikko. (2020). Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture. 179. 105776.

[20] National Institute of Standards and Technology. (2009). *NIST IR 7609, Cryptographic key management workshop summary June 8-9, 2009*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7609.pdf
[21] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems—Requirements*. Retrieved from https://www.iso.org/standard/27001
[22] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Članak 32 Sigurnost obrade. *Official Journal of the European Union, L 119*, (2016, May 4). Retrieved from https://gdprinfo.eu/hr/hr-article-32

Povjerljivost (engl. Confidentiality) se odnosi na zaštitu informacija od neovlaštenog pristupa.[23] To znači da samo ovlašteni korisnici imaju pristup osjetljivim informacijama, a da neovlašteni korisnici ne mogu doći do njih. Ovo opisuje sposobnost organizacije da čuva osjetljive informacije privatnim i sigurnim. Povjerljivost podataka će se najvjerovatnije primjenjivati u odnosu na lične podatke, kao što su imena klijenata, kontakt podaci i detalji platne kartice. Ovi detalji bi trebali biti pohranjeni u relevantnim bazama podataka i dostupni samo onima kojima su potrebni.

To može značiti zaštitu datoteka lozinkom ili postavljanje kontrola pristupa. Također je nužno razmotriti pohranjivanje različitih dijelova informacija u odvojenim bazama podataka. Na primjer, ne bi trebalo pohraniti detalje korisničkog računa, kao što su njihovo korisničko ime i lozinka, u iste datoteke kao i druge lične informacije. Potrebno je izolirati vrlo osjetljive podatke, kao što su podaci o kreditnoj kartici i zdravstveni kartoni. Međutim, povjerljivost se ne odnosi samo na lične podatke već uključuje sve informacije osjetljive prirode. Ovo može uključivati stvari poput intelektualnog vlasništva i korporativnih zapisa, koji moraju biti adekvatno zaštićeni kako bi se osiguralo da samo ovlašteno osoblje može dobiti pristup.

Integritet (engl. Integrity) se odnosi na zaštitu informacija od neovlaštenih promjena.[24] To znači da se informacije moraju očuvati u ispravnom obliku i da ne smiju biti mijenjane bez odobrenja. Integritet podataka igra bitnu i jedinstvenu ulogu u zaštiti podataka. Često razmišljamo o tome ko ima (ili nema) pristup informacijama. Međutim, jednako je važno razmotriti jesu li same informacije tačne. Primjer integriteta podataka pojavio bi se u odnosu na zdravstvenu ustanovu koja pacijentu e-mailom šalje informacije o njegovom zdravlju. Organizacija mora biti sigurna da je njihova evidencija tačna, inače će primalac dobiti netačne informacije o svom zdravstvenom statusu ili možda neće dobiti ažurirane podatke. U međuvremenu, osoba koja je nehotice primila poruku bit će obaviještena o zdravstvenom stanju treće strane. Integritet podataka može se primijeniti i na korporativne podatke.

Dostupnost (engl. Availability) se odnosi na osiguranje pristupa informacijama kada su potrebne ovlaštenim korisnicima.[25] To znači da informacije moraju biti dostupne kada su potrebne, a da

[23] Andress, J. (2011). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (Online-ausg.). Syngress. Accessed May 6, 2024. http://site.ebrary.com/id/10477252
[24] Ibid.
[25] Ibid.

korisnici ne smiju biti spriječeni da pristupe informacijama. Primjeri informacija koje bi trebale biti dostupne uključuju poslovne podatke, medicinske zapise i naučne podatke. Sistemi, aplikacije i podaci organizacije moraju biti dostupni ovlaštenim korisnicima na zahtjev. Ako se, na primjer, organizacija suoči sa nestankom struje zbog čega se gase njeni sistemi, njene operacije će se zaustaviti. Isto tako, ako cyber kriminalci šifriraju datoteke organizacije u napadu na ransomware, suočit će se s velikim poremećajem. Dostupnost se može odnositi na sposobnost zaposlenog da pregleda informacije, ako postoji problem s njihovim računom ili hardverom neće moći pristupiti informacijama koje su im potrebne za obavljanje svog posla.

Sve tri kategorije su jednako važne za osiguravanje informacijske sigurnosti, a mnogi sigurnosni postupci se fokusiraju na osiguravanje svake od njih. Primjerice, za osiguranje povjerljivosti informacija koriste se metode autentifikacije i autorizacije, za osiguranje integriteta koriste se metode provjere i enkripcije, dok se za osiguranje dostupnosti koriste metode redundancije i osiguravanje kontinuiteta poslovanja.

Da bi smo praktično prikazali kako jedna organizacija osigurava **povjerljivost, integritet i dostupnost,** uzećemo za primjer bankomat banke koji korisnicima omogućuje pristup njihovim bankovnim računima. Kako bi se osigurala povjerljivost, bankomat zahtijeva dvostruku autentifikaciju - fizičku karticu i PIN kod - prije nego što dopusti pristup podacima. Ovo sprječava neovlašten pristup računu, čime se osigurava povjerljivost bankovnih podataka. Da bi se osigurao integritet podataka, bankomat i bankovni softver provjeravaju ispravnost prijenosa novca i isplata. Svaka se transakcija zabilježi u računovodstvu korisnika kako bi se spriječile neovlaštene ili neispravne isplate. To osigurava integritet podataka o financijskim transakcijama i sprječava bilo kakve pokušaje krađe novca. Bankomat osigurava dostupnost tako što se nalazi na javnom mjestu i dostupan je čak i kada je poslovnica banke zatvorena. To omogućuje korisnicima da pristupe svojim finansijskim sredstvima 24 sata dnevno, što je bitno za osiguravanje dostupnosti bankovnih usluga.[26] Dakle, ovaj primjer pokazuje kako bankomat banke koristi sva tri principa CIA trijade kako bi se osigurala zaštita korisničkih podataka i pružila pouzdana i sigurna bankarska usluga.

[26] Fruhlinger, J. (2020, February 10). The CIA triad: Definition, components and examples. *CSO Online*. Retrieved from https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

Razvoj informacijske sigurnosti kroz istoriju

Istorija informacijske sigurnosti počinje sa razvojem računara prve generacije 1940. te obuhvata period od nekoliko decenija tokom kojih su se prijetnje i izazovi u ovoj oblasti mijenjali. Ujedno razvijale su se nove tehnologije, standardi i zakonska regulativa u cilju obezbjeđivanja sigurnosti informacija. Jedna od ključnih tačaka u istoriji informacijske sigurnosti je razvoj ARPANET-a (The Advanced Research Projects Agency Network), preteče interneta, koji je nastao 1969. godine kao projekt američke vlade.[27] *Creeper* je bio prvi poznati virus koji se pojavio u ranim danima kompjuterskih mreža.[28] Bio je to program kojeg je kreirao Bob Thomas 1971. godine. Creeper se replicirao po ARPANET-u, prethodniku današnjeg Interneta, i zarazio računare na mreži. Kada bi se virus instalirao na računar, ispisao bi poruku "*Ja sam puzavac, uhvati me ako možeš!*" (engl. "I'm the creeper, catch me if you can!") na ekranu, a zatim bi bio prebačen na drugi računar na mreži, koristeći ARPANET za prenos. Iako je Creeper bio benigni virus i nije izazvao veću štetu, bio je to prvi primjer širenja zlonamjernog softvera (engl. malware) na kompjuterskim mrežama. To je bila i motivacija za razvoj prvog antivirusnog programa - Reaper[29], koji je kreirao Ray Tomlinson kako bi uklonio Creeper sa zaraženih računara. Međutim, njegovo otkriće je bilo ključno za razvoj svijesti o sigurnosti računarskih sistema, kao i za razvoj programa za detekciju i uklanjanje virusa. Creeper se smatra prethodnikom računarskih virusa i drugih oblika zlonamjernih aktivnosti, a njegova pojava je označila početak potrebe za razvojem mjera sigurnosti u računarskim sistemima.

Postoji mnogo načina za opisivanje razvoja informacijske sigurnosti u posljednjim desetljećima. Jedan od tih načina je mapiranje razvoja kroz faze koje označavaju specifične trendove. *„Pet valova informacijske sigurnosti - od Kristiana Bekmana do danas*“[30] je rad napisan od strane S. H. (Basie) von Solmsa koji prikazuje evoluciju informacijske sigurnosti kroz godine, razdvajajući je u pet različitih valova, svaki sa svojim jedinstvenim karakteristikama i izazovima. Ovih pet valova sigurnosti informacija predstavljaju kontinuirani razvoj koji se odvijao posljednjih 30 do 40 godina,

[27] Merkow, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices* (2nd ed.). Pearson IT Certification.
[28] Shinde, A. (2021). *Introduction to cyber security: Guide to the world of cyber security*. Notion Press.
[29] Ibid.
[30] von Solms, S.H.(. (2010). The 5 Waves of Information Security – From Kristian Beckman to the Present. In: Rannenberg, K., Varadharajan, V., Weber, C. (eds) Security and Privacy – Silver Linings in the Cloud. SEC 2010. IFIP Advances in Information and Communication Technology, vol 330. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15257-3_1

a ne kao zasebne cjeline koje su započele i završile u određenom trenutku. I pored toga što je svaki novi val stavio novi naglasak na aspekte vezane za sigurnost informacija, oni nisu samo jednokratni događaji, već su kontinuirani procesi te ih stoga treba posmatrati kao da postoje paralelno jedan s drugim. Tako von Solms definiše: *Prvi val trajao je do ranih 1980-ih i naziva se Tehnički val. Drugi val je bio od ranih 1980-ih do sredine 1990-ih i naziva se Val upravljanja (menadžmenta). Treći Val je bio od sredine 1990-ih do otprilike 2005. godine i naziva se Institucionalni Val. Četvrti val započeo je oko 2005. godine i naziva se Val upravljanja sigurnošću informacija. Peti val, koji se naziva val sajber sigurnosti, započeo je oko 2006. godine.*[31]

Prvi val – Tehnički

Prvi „Tehnički val" opisuje evoluciju informacijske sigurnosti od njenih najranijih dana s pojavom prvih računara i kasnijom pojavom tzv. glupih terminala, kada je informacijska sigurnost bila ograničena na jednostavne oblike identifikacije i autentifikacije za prijavu na glavni računarski (engl. Mainframe) sistem. Fizička sigurnost prvih kompjutera bila je osnova na kojoj se zasnivala sva informacijska sigurnost. Mainframe računari su bili nezavisne jedinice, a pristup sistemu bio je zasnovan na principu „jedan računar - jedan korisnik", a najveća briga je bila da računar ne bude fizički oštećen ili ukraden. Računarske mreže nisu postojale, a za prijenos programa i podataka između računara korišteni su kuriri ili pošta. Stoga je jedina prijetnja vezana za prijenos informacija bila da bi medij za pohranu podataka tog vremena mogao biti izgubljen ili ukraden.

Početkom 1970-ih pojavili su se pasivni terminali, gdje je pristup sistemu bio zasnovan na principu „jedan računar = više korisnika" i korištenje udaljenih podataka. Sa novim fenomenom dolazi i novi rizik za udaljene podatke jer je sada postojala mogućnost pristupa podacima od strane neovlaštene osobe ili osobe izvan organizacije. Jednostavna fizička sigurnost nije mogla odgovoriti na nove rizike, pa se uvodi novi koncept identifikacije i provjere autentičnosti.

Aspekti kao što su sigurnosna politika, svijest o procedurama, itd. gotovo da i nisu postojali. Zabrinutost za sigurnost informacija počela je da se pojavljuje početkom 1980-ih. Kristian Beckman bio je pionir u ovoj oblasti, prepoznavši potrebu za sveobuhvatnijim pristupom informacijskoj

[31] Ibid.

sigurnosti, organizujući Prvu međunarodnu konferenciju o informacijskoj sigurnosti (IFIP/Sec 83) i predloživši IFIP-u da uspostavi tehnički komitet za aspekte sigurnosti informacija. Beckmanova vizija budućnosti informacijske sigurnosti prekinuta je njegovom preranom smrću 1984. godine, ali je njegov doprinos postavio temelj razvoju sofisticiranijih i sveobuhvatnijih pristupa informacijskoj sigurnosti.

Drugi val – Menadžment

Drugi val razvoja informacijske sigurnosti obuhvata period od kraja 1970-ih godina do sredine 1990-ih godina. U tom periodu razvijene su distributivne računarske mreže i personalni računari, što je stvorilo nove rizike u pogledu sigurnosti informacija. Umjesto da su se informacije čuvale na jednom centralnom računaru, sada su se slale na mnogo računara povezanih u mrežu, što je stvorilo ozbiljne sigurnosne probleme koji su morali biti riješeni.

U drugom valu, sigurnost informacija postaje važna briga za menadžment, pa su imenovani menadžeri za sigurnost informacija koji su počeli kreirati politike i procedure za sigurnost informacija. Organizacijske strukture su stvorene kako bi se smjestio odjel za sigurnost informacija, a izvještavanje o stanju sigurnosti informacija u organizaciji postalo je izazov.

Ovaj razvoj je prirodno poboljšao opštu sigurnost informacija i naglasio važan aspekt da sigurnost informacija ima vrlo snažnu dimenziju upravljanja koja se mora u potpunosti iskoristiti za stvaranje sigurnog okruženja.

Zbog ovog razvoja tokom Drugog vala, kompanije su počele istraživati aspekte povezane s najboljim praksama i standardizacijom u oblasti sigurnosti informacija. Mnoge kompanije su željele znati koje su osnovne karakteristike dobrog plana sigurnosti informacija. Postavljena su pitanja poput:

- Kako se uspoređujemo sa sigurnošću konkurencije?
- Što treba biti u politici sigurnosti informacija?
- Kako bismo mogli dobiti neku vrstu formalne potvrde o statusu sigurnosti informacija u organizaciji?

Uloga zaposlenika kao krajnjeg korisnika sistema dolazi u fokus, te se prihvatila važnost ljudske

dimenzije u sigurnosti informacija. Drugi val bio je važna prekretnica u razvoju informacijske sigurnosti jer je naglasio važnost upravljanja sigurnosti informacija, potrebu za standardizacijom i najboljim praksama.

Treći val - Institucionalizacija

Treći val razvoja informacijske sigurnosti, poznat kao institucionalizacija, počeo je da se javlja krajem 1990-ih godina. Ovaj talas bio je karakterističan po tome što su organizacije počele da shvataju da je informacijska sigurnost neophodna za postojanje i uspjeh njihovog poslovanja. Informacijska sigurnost više nije bila samo pitanje tehničke prirode koje se bavilo zaštitom podataka od zlonamjernog softvera, već je postala ključna poslovna funkcija koja se morala integrisati u sve aspekte poslovanja.

Jedan od pokretača bila je ideja dobre međunarodne prakse za sigurnost informacija i dolazak međunarodnih standarda (BS 7799). Još jedan pokretač bio je sve veći naglasak na svijesti o informacijskoj sigurnosti i rizik da neupućeni zaposlenici mogu ugroziti mjere informacijske sigurnosti. Organizacije su počele da shvataju da informacijska sigurnost nije samo stvar tehnologije, već je jednako važna i ljudska dimenzija. Sve više pažnje počelo se posvećivati obuci i osnaživanju zaposlenih u pogledu informacijske sigurnosti, što je dovelo do razvoja novih metoda i edukacija za osvještavanje zaposlenih o prijetnjama i rizicima. Razvijeni su opsežni kursevi za podizanje svijesti, a zaposleni su obučavani da informacijska sigurnost postane dio njihove kulture, odnosno kulture organizacije. Organizacije su počele stvarati tehnike za mjerenje statusa i razine svoje usklađenosti s informacijskom sigurnošću, te podnositi izvještaje najvišem menadžmentu.

Ukupno gledano, institucionalizacija informacijske sigurnosti označila je prelazak iz izolovane funkcije u ključnu funkciju u organizaciji koja se odnosi na sve aspekte poslovanja. To je dovelo do povećanja svijesti o informacijskoj sigurnosti na svim nivoima u organizacijama i povećanja ulaganja u oblast informacijske sigurnosti. Ova promjena dovodi nas do četvrtog vala koji se može okarakterisati kao upravljanje informacijskom sigurnošću.

Četvrti val – Upravljanje informacijskom sigurnošću

Četvrti val, poznat kao Upravljanje informacijskom sigurnošću, pojavio se početkom 2000-ih. Tokom ovog vremena, važnost dobrog organizacijskog upravljanja postajala je sve jasnija i počele su se pojavljivati najbolje međunarodne prakse za to. U okviru ovih najboljih praksi, naglašen je značaj upravljanja rizicima na strani informacijskih, pri čemu je implementacija informacijske sigurnosti kritična komponenta dobrog upravljanja informacijskom tehnologijom.

Finansijske i druge važne informacije organizacije bile su čuvane i obrađivane na računarima. Ako čuvanje i obrada tih informacija nisu bile pravilno osigurane i zaštićene, moglo je doći do ozbiljnih kompromitacija. Potencijalni rizici neadekvatne sigurnosti i zaštite finansijskih informacija koje se čuvaju i obrađuju na računarima su postali očigledni, uključujući rizik od prevare i zloupotrebe finansijskih sredstava kroz neovlašćenu manipulaciju elektronskim podacima. Bilo je jasno da je najviše rukovodstvo na kraju odgovorno za ove rizike. Kao rezultat nastaje je koncept upravljanja sigurnošću informacija, koji prepoznaje da je to sastavni dio korporativnog upravljanja. To znači da informacijska sigurnost nije samo tehničko, već i poslovno pitanje koje zahtijeva pažnju i angažman najvišeg menadžmenta. Upravljanje sigurnošću informacija uključuje razvoj politika, procedura i struktura kako bi se osiguralo da je informacijska sigurnost integrisana u cjelokupni upravljački okvir organizacije. Takođe uključuje praćenje i izvještavanje o stanju informacijske sigurnosti u organizaciji i osiguravanje da su resursi pravilno raspoređeni za upravljanje rizicima po sigurnost informacija.

Ova sve veća važnost i naglasak na informacijskoj sigurnosti rezultirali su pojavom koncepta upravljanja informacijskom sigurnošću. Činjenica da je "Upravljanje informacijskom sigurnošću sastavni dio korporativnog upravljanja" postaje dobro prihvaćena.

S.H. von Solms (2010) ističe dva važna aspekta zajednička za prva četiri talasa. Prvo, očigledno je da se četiri talasa u osnovi 'usmeravaju ka unutra', tj. imaju veze sa osiguranjem podataka i informacija kompanije. Odgovornost je na kompaniji i njenim zaposlenima, a sve mjere se sprovode u tom cilju. Glavna svrha je osigurati da se povjerljivost i integritet podataka i informacija kompanije održava u svakom trenutku od strane kompanije. To je dovelo do toga da su kompanije uvele vrlo dobre sigurnosne mjere, što je otežavalo kriminalnim elementima koji su željeli pristup

takvim podacima i informacijama da to učine – u mnogim slučajevima IT infrastruktura kompanije postala je dobro zaštićena tvrđava. Drugo, kompanije su uvodile sve više sistema zasnovanih na Internetu omogućavajući milionima klijenata i kupaca da koriste takve sisteme. Direktan rezultat ova dva aspekta bio je da su kriminalci sada skrenuli pažnju na krajnjeg korisnika. Koristeći internet kao medij za pristup, kriminalci su iskoristili činjenicu da milioni krajnjih korisnika imaju nizak nivo svijesti i znanja o informacijskoj sigurnosti. Počeli su provoditi napade koristeći širok spektar mehanizama usmjerenih na krajnje korisnike, pri čemu su se oslanjali uglavnom na društveni inženjering. Njihov moto je bio: Ne pokušavajte da hakujete IT sisteme kompanije; može biti veoma teško - idite na naivnog krajnjeg korisnika! To je dovelo do petog talasa informacijske sigurnosti – obezbjeđivanja bezbjednosti informacija u cyber prostoru, nazvanog Cyber Security.

Peti val – Cyber sigurnost

Internet je bez sumnje jedan od najvećih izuma koje je čovječanstvo ikada razvilo, ali je sa sobom donio izuzetno ozbiljne rizike. Implementacija bilo kojeg sistema temeljenog na Internetu znači oglašavanje tog sistema ostatku svijeta i time pružanje prilike cyber kriminalcima da napadnu isti. Cyber kriminalci iskorištavaju sve veću upotrebu interneta od strane organizacija za pružanje usluga svojim klijentima kako bi počinili štetu golemih razmjera. Prijetnje poput ucjenjivačkog softvera (engl. ransomware), socijalnog inženjeringa, napada s ciljem krađe identiteta i druge tehnike koje koriste takvi kriminalci čine život svakom korisniku interneta izuzetno riskantan. Internet je kriminalnoj strani pružio koristan način počinjenja njihovih zločina, a stručnjacima za informacijsku sigurnost najveći izazov – osigurati da se takvi zločini spriječe.

Kako tvrdi S.H. von Solms[32] „*Ovaj talas nas izaziva kao stručnjake za informacijsku sigurnost da preispitamo našu ulogu i da osiguramo da djelujemo kao profesionalci, a ne kao praktičari informacijske sigurnosti. To znači da bi trebalo da budemo glasniji u izražavanju naše zabrinutosti za sigurnosti mnogih sistema zasnovanih na internetu*."

U zaključku, cyber sigurnost je suštinska komponenta informacijske sigurnosti u modernoj eri, jer se sve više ljudi i kompanija, odnosno organizacija oslanja na internet i tehnologiju za obavljanje

[32] Cf. supra ref. 25

svojih svakodnevnih aktivnosti. Osiguravanje cyber sigurnosti zahtijeva zajednički napor između kompanija, krajnjih korisnika i vlada kako bi se stvorilo sigurno i osigurano cyber okruženje.

Odnos informacijske i cyber sigurnosti

Informacijska sigurnosti i cyber sigurnost su dva pojma koja su međusobno povezana, ali imaju i razlike u značenju, primjeni i fokusu.

Prema ISO/IEC 27000 standardu, Informacijska sigurnost se definiše kao „*Očuvanje povjerljivosti, integriteta i dostupnosti informacija*“.[33] Drugim riječima, informacijska sigurnost se bavi zaštitom informacija koje organizacija posjeduje, obrađuje ili prenosi. Sa druge strane, ISO/IEC 27032 standard definiše cyber sigurnost kao „*Očuvanje povjerljivosti, integriteta i dostupnosti informacija u cyber prostoru*.“[34] Poredeći ove standarde, informacijska sigurnost se odnosi na zaštitu informacija uopšte, dok se cyber sigurnost odnosi samo na zaštitu podataka u cyber prostoru.

U oba slučaja, zajedničko im je osigurati povjerljivost, integritet i dostupnost informacija, sto smo objasnili na primjeru CIA trijade.

Kako primjećuje Vajzović (2019): *termin „cyber sigurnost“ treba u datom terminosistemu razumijevati kao složen pojam koji ove dvije riječi spaja u navedenu sintagmu: Cyber se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, a posebno Internetom i informacijskim tehnologijama (OSCE 2019), dok termin Sigurnost ima korijene u starolatinskom izrazu securus (bezbrižan, pouzdan, siguran; Klaić, 1985 u Beridan, 2007) što u „znanosti, i u političkoj praksi (...) podrazumijeva dva svoja osnovna aspekta: – znači istodobno: a) funkciju, djelatnost države, društva i pojedinca, a potom i b) stanje u odnosima među državama, stanje unutar jedne države, među ljudima, odnosno stanje u prirodi i kosmosu spram života općenito“ (Beridan 2007: 100) Na osnovu Beridanove izvedbe definicije sigurnosti (2007: 101), može se reći da sigurnost „općenito podrazumijeva stepen zaštićenosti ljudi od različitih*

[33] International Organization for Standardization. (n.d.). ISO/IEC 27000 family: Information security management. Retrieved from https://www.iso.org/standard/iso-iec-27000-family
[34] International Organization for Standardization (2023). ISO/IEC 27032:2023 - Cybersecurity - Guidelines for Internet security. Retrieved from https://www.iso.org/standard/76070.html

oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države" i međunarodnih odnosa, pa i na kosmičkom i planetarnom nivou života općenito, ljudskoga roda u cjelini „od svih vidova ugrožavanja". Sigurnost podrazumijeva stepen zaštićenosti od ugrožavanja, uz naglasak da ne postoji apsolutna i potpuna sigurnost, već možemo govoriti o većem ili manjem stepenu sigurnosti. U tom kontekstu moguće je zaključiti da cyber sigurnost jest stanje i praksa zaštite infrastrukture, informacijsko-komunikacijskih sistema, mreža, uređaja i informacija od ugrožavanja, u cilju zaštite ljudi, materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države i međunarodnih odnosa.[35]

Takođe, možemo reći da je fokus informacijske sigurnosti da se bavi zaštitom informacija na nivou organizacije, u šta spada organizacijska imovina koja se čuva ili prenosi bez informacijske i komunikacijske tehnologije, dok se cyber sigurnost fokusira na zaštitu podataka na mrežama i drugim sistemima koji su povezani sa internetom.

U svom radu von Solms i van Niekerk (2013) tvrde „*danas, u cyber sigurnosti, ljudi i ljudska društva su narasli da postanu dio imovine koju treba zaštititi. Iako se ljudi i dalje smatraju prijetnjom, danas se smatraju i imovinom koju treba zaštititi u cyber prostoru. U svjetlu gore navedenog, cyber sigurnost se može definisati kao zaštita samog cyber prostora, elektronskih informacija, informacijskih sistema koji podržavaju cyber prostor i korisnika cyber prostora u njihovom ličnom, društvenom i nacionalnom svojstvu, uključujući bilo koji njihov interes, bilo materijalne ili nematerijalne, koji su ranjivi na napade koji potiču iz cyber prostora*."[36]

Iako može postojati određena debata oko tačnih definicija i granica cyber sigurnosti i informacijske sigurnosti, opšte je prihvaćeno da je cyber sigurnost podskup informacijske sigurnosti, fokusirana posebno na zaštitu cyber prostora.

[35] Vajzović, Emir. Op cit.
[36] von Solms R., van Niekerk J. (2013) From information security to cyber security, Computers & Security, Volume 38, Pages 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

Izazovi informacijske sigurnosti

Mnogobrojni su izazovi sa kojim se suočava informacijska sigurnost danas. Jedan od najvećih izazova su sigurnosne prijetnje koje se stalno razvijaju, sa novijim i sofisticiranijim napadima. Drugi izazov je sve veća složenost IT sistema i mreža, sa sve više uređaja i aplikacija povezanih na Internet što otežava osiguranje svih ulaznih tačaka. Osim toga, korištenje usluga vanjskih kompanija koje pružaju određene usluge ili podršku, poput *hostinga*[37] podataka, upravljanja infrastrukturom ili održavanja IT sistema, znači da organizacije moraju povjeriti svoje osjetljive podatke i sisteme tim vanjskim stranama.

Ljudska greška i *insajderske prijetnje*[38] također predstavljaju značajne izazove za sigurnost informacija. Zaposleni, saradnici i drugi insajderi mogu izložiti osjetljive informacije ili ugroziti sigurnosne mjere, bilo zlonamjernim radnjama ili jednostavnim greškama. Ovo zahtijeva od organizacija da implementiraju snažne sigurnosne politike i programe obuke kako bi podigle svijest i smanjile rizik od insajderskih prijetnji.

Konačno, usklađenost sa zakonskim i regulatornim zahtjevima predstavlja izazov stručnjacima za sigurnost informacija. Različite industrije i jurisdikcije imaju svoja pravila i propise o zaštiti podataka, a nepoštivanje tih pravila i propisa može dovesti do značajnih pravnih i finansijskih posljedica. Zakoni i propisi o sigurnosti informacija i privatnosti postaju sve strožiji, što zahtijeva od kompanija i organizacija da usklade svoje prakse s novim zahtjevima. Na primjer, Opšta uredba o zaštiti podataka (GDPR)[39] ima velik utjecaj na organizacije koje obrađuju lične podatke građana Europske unije, jer ispunjavanje ovih zahtjeva uz obezbjeđivanja efikasnih sigurnosnih mjera predstavlja veliki izazov.

Izvori sigurnosnih incidenata se ugrubo mogu podijeliti na:

[37] Hosting u oblaku čini aplikacije i web stranice dostupnim koristeći tvz. cloud resurse. Za razliku od tradicionalnog hostinga, rješenja se ne postavljaju na jedan server. Umjesto toga, pružatelj usluga u oblaku je vlasnik mreža povezanih virtualnih i fizičkih servera koji podržavaju aplikaciju ili web stranicu, osiguravajući veću fleksibilnost i skalabilnost.
[38] Insajdersku prijetnju kao prijetnju da će zaposlenik koristiti svoj ovlašteni pristup, svjesno ili nesvjesno, da nanese štetu organizaciji, resursima, osoblju, objektima, informacijama, opremi, mrežama ili sistemima.
[39] Cf. supra ref. 15

Prirodne katastrofe i tehnički kvarovi - uključuju poplave, požare, potrese, udare munje, strujne udare i druge slične događaje koji mogu utjecati na sigurnost i dostupnost podataka. Također uključuju tehničke probleme kao što su kvarovi hardvera i softvera, softverski bugovi[40] i greške u programiranju.

Unutrašnji, insajderski (engl. Insider)[41] izvori – su vrsta prijetnje informacijskoj sigurnosti koja proizlazi iz aktivnosti osoba unutar organizacije koje su autorizovane za pristup osjetljivim podacima ili informacijama. To mogu biti trenutni ili bivši zaposlenik, izvođač ili poslovni partner koji ima ili je imao ovlašteni pristup mreži, sistemu ili podacima organizacije i namjerno je prekoračio ili zloupotrijebio taj pristup na način koji je negativno uticao na povjerljivost, integritet ili dostupnost informacija organizacije ili informacijskih sistema.[42]

Insajderske prijetnje mogu biti namjerne ili nenamjerne. Namjerne prijetnje dolaze od zaposlenika koji namjerno krše politike organizacije i koriste svoj pristup osjetljivim podacima ili informacijama u nezakonite svrhe. Nenamjerne prijetnje su posljedica nepažnje ili neznanja zaposlenika, poput slučajnog brisanja podataka ili slanja osjetljivih informacija nekom ko nije ovlašten za pristup tim informacijama.

Vanjski izvori – prijetnje informacijskoj sigurnosti organizacije su različite vrste napada koje provode pojedinci, skupine ili organizacije izvan kompanije. Ovdje ćemo navesti neke od najčešćih vanjskih izvora prijetnji:

Zlonamjerni softver (engl. malware), koji se također naziva zlonamjerni kod ili zlonamjerna logika, je sveobuhvatni izraz koji se koristi za opisivanje bilo kojeg softvera ili firmvera namijenjenog izvođenju neovlaštenog procesa koji će imati negativan utjecaj na povjerljivost, integritet ili dostupnost sistema. Primjeri zlonamjernog koda uključuju viruse, crve, trojanske konje ili druge

[40] Softverski bugovi su programerske greške ili neispravnosti u softverskim aplikacijama koje mogu dovesti do neočekivanih ponašanja ili nedostataka u funkcionalnosti softvera. Li, Z., Zhang, H., & Mei, H. (2016). A survey on software bug prediction. Journal of Software Engineering and Applications, 9(9), 421-444.
[41] Osoba priznata ili prihvaćena kao član grupe, kategorije ili organizacije
[42] Claycomb, W. R., & Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. In 2012 IEEE 36th Annual Computer Software and Applications Conference (pp. 387-394). Izmir, Turkey. doi:10.1109/COMPSAC.2012.113

entitete bazirane na kodu koji inficiraju računarski sistem korisnika.[43] Komponente zlonamjernog softvera koje se koriste u napadu zavise od cilja aktera prijetnje. Ovo može varirati od preuzimanja kontrole nad sistemima i mrežama (posrednici inicijalnog pristupa, botnetovi) do preuzimanja kontrole nad podacima (akteri prijetnji ransomware-a, krađa informacija).

Društveni ili socijalni inženjering (engl. *Social Engeneering*) je širok spektar aktivnosti koje pokušavaju da iskoriste ljudsku grešku, odnosno da manipuliraju ljudima sa ciljem dobijanja pristupa informacijama ili uslugama.[44] U cyber sigurnosti, socijalni inženjering je vještina koja se više temelji na psihologiji nego na računarskoj nauci. Napadači iskorištavaju karakteristike ljudskog ponašanja, kao što su spremnost za pomoći, poštivanje autoriteta ili strah, kako bi prikupili informacije koje kasnije mogu koristiti za pokretanje napada. Napadi iskorištavaju ljudski faktor kako bi postigli uspjeh, manipulišući korisnicima da otvore sumnjive dokumente, datoteke ili e-mailove, posjete zlonamjerne web stranice ili omoguće neovlašten pristup osobama, sistemima ili uslugama.

Iako se napadi socijalnog inženjeringa razlikuju jedni od drugih, imaju zajednički obrazac sa sličnim fazama. Uobičajeni obrazac uključuje četiri faze: (1) prikupiti informacija o meti; (2) razviti odnos sa ciljem; (3) iskoristiti dostupne informacije i izvršiti napad; i (4) izlaz bez tragova.[45]

Napadi socijalnog inženjeringa mogu se svrstati u nekoliko kategorija zavisno o nekoliko perspektiva. Analizom različitih postojećih klasifikacija napada socijalnog inženjeringa, te napade možemo svrstati u dvije glavne kategorije: direktne i indirektne.

Napadi svrstani u prvu kategoriju koriste direktne kontakte između napadača i žrtve da izvedu napad. Oni se odnose na napade izvedene putem fizičkog kontakta ili kontakta očima ili glasovne interakcije. Oni također mogu zahtijevati prisustvo napadača u radnom prostoru žrtve da bi izvršili napad. Primjeri ovih napada su: fizički pristup, virenje preko ramena (engl. *Shoulder Surfing*),

[43] National Institute of Standards and Technology. (n.d.). Malware. Glossary of Key Information Security Terms. Retrieved from https://csrc.nist.gov/glossary/term/malware
[44] National Institute of Standards and Technology. (n.d.). Social engineering. Glossary of Key Information Security Terms. Retrieved from https://csrc.nist.gov/glossary/term/social_engineering
[45] Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209.

kopanje po smeću (engl. *Dumpster diving*), stvaranje scenarija - lažne priče (engl. *Pretexing*), praćenje u stopu (engl. *Tailgating*).

Napadi svrstani u indirektnu kategoriju ne zahtijevaju prisustvo napadača da bi pokrenuo napad. Napad se može pokrenuti na daljinu putem zlonamjernog softvera koji se prenosi putem priloga e-maila ili SMS poruka. Primjeri ovih napada su: krađa identiteta (engl. *Phishing*), ucjenjivački softver (engl. *Ransomware*), BEC prevare (engl. *Business e-mail compromise*) i drugi.[46]

Phishing je tehnika društvenog inženjeringa koju koriste napadači kako bi prevarili korisnike da otkriju svoje osjetljive informacije, kao što su korisnička imena, lozinke i druge osobne podatke.[47] Ovi napadi obično dolaze u obliku lažnih e-mail poruka, web stranica, ili drugih oblika digitalne komunikacije koji se čine autentičnim, ali su zapravo stvoreni kako bi prevarili korisnika. Najčešći primjeri phishing napada su lažne e-mail poruke koje se prikazuju kao legitimne poruke od poznatih tvrtki, banaka, ili drugih organizacija. Te poruke obično traže od korisnika da klikne na lažni link ili da podijeli svoje osjetljive podatke na lažnoj web stranici koja se čini autentičnom. Cilj phishing napada je ukrasti identitet korisnika ili dobiti pristup njihovim osjetljivim informacijama. Napadači koriste ove informacije kako bi ostvarili financijsku korist, kao što je krađa novca sa bankovnog računa, ili kako bi izveli druge vrste prevara.

BEC prevare ili kompromitovanje poslovne e-pošte (engl. *Business e-mail compromise*) smatra se jednom od najopasnijih financijskih prijevara na internetu, s obzirom na činjenicu da se većina organizacija svakodnevno oslanja na e-mailove za poslovnu komunikaciju. Napadač se obično predstavlja kao osoba od povjerenja ili kao nadređeni, te zatim traži plaćanje lažnih faktura, uplate novca na lažne račune ili otkrivanje osjetljivih podataka. Ključni dio ove prevare je društveno inženjerstvo, gdje napadač istražuje metu kroz društvene mreže kako bi prikupio informacije o njihovim profesionalnim aktivnostima i ponašanju. Koristeći te informacije, napadač izrađuje uvjerljive e-mailove koje mogu zavarati žrtvu da klikne na zlonamjerni link ili preuzme zaraženi dokument. Ovo može dovesti do kompromitovanja sigurnosti mreže i sistema organizacije, krađe identiteta, gubitka novca ili osjetljivih podataka. Napadači često ciljaju određene visoko profilirane

[46] Salahdine, F.; Kaabouch, N. (2019) Social Engineering Attacks: A Survey. Future Internet 2019, 11, 89 https://doi.org/10.3390/fi11040089
[47] Ibid.

zaposlenike kako bi povećali uspjeh svoje prevare. Koristeći taktike poput lažnih hitnih slučajeva ili prepravki prethodnih e-poruka, napadači pokušavaju stvoriti osjećaj nužnosti ili hitnosti kako bi žrtva brzo djelovala bez razmišljanja.[48] Ova vrsta prevare zahtijeva pažljivo osmišljene sigurnosne mjere i kontinuiranu edukaciju zaposlenika kako bi se smanjio rizik od uspješnih napada.

Ransomware je vrsta zlonamjernog softvera (malware), definisan kao vrsta napada u kojem akteri prijetnje preuzimaju kontrolu nad imovinom mete i traže otkupninu u zamjenu za povratak dostupnosti imovine. Ova definicija je potrebna kako bi obuhvatila različite prijetnje ransomware-a koje se stalno mijenjaju, uključujući širok spektar tehnika ucjena i različite motive počinitelja, ne ograničavajući se samo na finansijske motive. Ransomware je jedna od glavnih prijetnji posljednjih godina, s nekoliko incidenata visokog profila i visoko publiciranih incidenata.

Ransomware napad uključuje šest faza: (1) stvaranje zlonamjernog softvera; (2) raspoređivanje; (3) instalacija; (4) komandovanje i upravljanje; (5) uništenje; i (6) iznuda. Kreiranje zlonamjernog softvera sastoji se od razvoja ransomware-a ili korištenja postojećeg za otkrivanje bilo kakve ranjivosti u sistemu žrtve kako bi se stvorila backdoor. Implementacija se sastoji od isporuke ransomware-a zaobilaženjem sigurnosnih kontrola kroz kreirana pozadinska vrata. Instalacija se sastoji od pokretanja ransomware-a i inficiranja sistema. U fazi komandovanja i kontrole, ransomware je aktivan kada žrtva ima internetsku vezu za komunikaciju sa komandnim centrom ili je pasivan kada je van mreže. U fazi uništenja, ransomware počinje blokirati ili šifrirati podatke i zamrzavati ekrane. Iznuda se sastoji od kontaktiranja žrtve tražeći otkupninu u zamjenu za oslobađanje blokiranih datoteka uz upozorenje o vremenskom ograničenju. Vraćanje fajlova nakon uplate žrtve nije zagarantovano. Jednom kada se napad ransomware-a pokrene na računaru, žrtve imaju samo tri izbora: (1) plaćanje otkupnine kako bi povratile šifrirane datoteke; (2) pokušaj vraćanja datoteka iz rezervnih kopija ako ih ima; ili (3) gubitak podataka nakon odbijanja plaćanja otkupnine.[49]

[48] Ibid.
[49] Ibid.

Drugi dio

INFORMACIJSKA PISMENOST

Koncept, pa i samo pojmovno određenje *informacijske pismenosti* prvi put koristi i uvodi Paul Zurkowski, koji je još davne 1974. godine govorio o temeljnim kompetencijama koje su potrebne savremenom čovjeku[50], vezanim uz rješavanje problema na radnom mjestu i industriji u Sjedinjenim Američkim Državama. Nakon prvobitno postavljenog termina koncept doživljava brojne razrade, prilagođavanja i izvedenice, tako da danas, skoro pedeset godina od inauguracije termina, opšteprihvaćene sastavnice koncepta navode da se *informacijsko […] opismenjavanje sastoji od usvajanja primjerenog informacijskog ponašanja u svrhu dolaženja do one informacije koja će zadovoljiti informacijsku potrebu i to bez obzira na medij, a uključuje i kritičku osviještenost o važnosti mudrog i etičkog korištenja informacija. Važno je da informacijska pismenost ne bude reducirana na bibliotečke ili računalne vještine već poimana kao odgovor na kulturni, društveni i ekonomski razvoj informacijskog društva.*[51] Programi opismenjavanja i pismenosti ne provode se u vakumu i zavise od ukupnog ponašanja pojedinca u informacijsko-komunikacijskom okruženju. Čovjekovo informacijsko ponašanje se može opisati kao *ljudska aktivnost u procesu mijenjanja informacijskog okruženja koje se sastoji od procesiranja informacija od strane ljudi i interakcije sa izvorima informacija i tehnološkim sistemima.*[52] Iz ovih sastavnica, odnosno gradivnih elemenata izvode se brojne definicije informacijske pismenosti kao aplikativne oblasti nastale na bazi ova dva koncepta, a za potrebe ovog rada koristiće se Hortonova, koji tako informacijsku pismenost definiše kao *skup vještina, stavova znanja potrebnih za rješavanje problema i donošenja odluka, oblikovanje informacijske potrebe u izraze za pretraživanje, učinkovito pretraživanje, pronalaženje, interpretaciju, razumijevanje, organiziranje, vrednovanje vjerodostojnosti i autentičnosti te relevantnost informacija.*[53]

---

[50] Zurkowski, P. G. (1974). The information service environment: Relationships and priorities. National Commission on Libraries and Information Science.

[51] Webber, S., & Johnston, B. (2000). Conceptions of information literacy: New perspectives and implications. Journal of Information Science, 26(6), 381-397.

[52] „Human information behaviour can be described as human activity in a changing information environment, It compprises both information processing by humans and interaction with information sources and technological systems“, Steinerova, J., & Šušol, J. (2005). Library users in human information behaviour. Online Information Review, 29(2), 139-156.

[53] Horton, F. W. (2008). Understanding information literacy: A primer. Paris: UNESCO.

Iz ovog proizilazi da informacijska pismenost pruža mogućnost čitanja kao organskog koncepta dajući mogućnost reinterpretacije i integracije u sve sfere ljudskog djelovanja i rada, uvažavajući specifičnosti svake struke, kao i prilagodbe potrebama ciljne populacije. Fokus ovog rada je na izradi modela informacijske pismenosti za sektor informacijske sigurnosti u korporativnom okruženju, odnosno modeliranje programa koji bi pružio obuku svim zaposlenicima u korporativnom okruženju koji koriste informacijski sistem i doprinose razvoju informacijskog ekosistema a nisu tehničke struke, slijedeći model informacijske pismenosti zasnovan na potrebi na koju ukazuje Vajzović: *važno [je] još jedanput ukratko potcrtati da bi kao temelj daljnjeg razvoja i podizanja nivoa cyber sigurnosti, trebalo biti podizanje nivoa medijske i informacijske pismenosti, kao strateškog opredjeljenja opšteg razvoja cyber-sigurnosnog domena*[54] naglašavajući da je *digitalna transformacija društva donijela velike izazove u informisanju i obrazovanju, pa time i u razvoju kritičkog mišljenja - osjetljivost građana (pa i cijelog društvenog sistema) na hibridne asimetrične distorzije i napade (vanjske i unutrašnje) proporcijalno se povećala, te su i izazovi za sigurnost postali značajniji.*[55]

Uzimajući u obzir naglašenu potrebu odgovora na sigurnosne izazove, nužno je izraditi model informacijske pismenosti u oblasti informacijske sigurnosti sa ciljem podizanja svijesti o potrebi kreiranja informacijski sigurnog okruženja. Okvir za izradu programa su postojeći modeli informacijske pismenosti. Pored standardnih modela koji se nalaze u širokoj primjeni (SCONUL[56], ACRL[57], ANZIL[58]), postoje i specifični modeli usmjereni na modus izvedbe, te će za potrebe ovog rada biti primijenjen *Relacijski model* autorice Catherine Bruce.[59]

[54] Vajzović, Emir. Op cit.
[55] Ibid.
[56] SCONUL Working Group on Information Literacy. (April 2011). The SCONUL Seven Pillars of Information Literacy Core Model for Higher Education. Retrieved from https://access.sconul.ac.uk/sites/default/files/documents/coremodel.pdf
[57] ACRL Framework for Information Literacy Advisory Board. (2017). The ACRL Framework for Information Literacy Toolkit [Website]. Retrieved from https://acrl.libguides.com/framework/toolkit
[58] Bundy, A. (Ed.). (2004). Australian and New Zealand Information Literacy Framework: Principles, Standards and Practice (2nd ed.). Adelaide: Australian and New Zealand Institute for Information Literacy. Retrieved from https://www.library.qut.edu.au/about/policies/information-literacy-framework/documents/anz-info-lit-policy.pdf
[59] Bruce, Christine. Op. cit.

MODEL SEDAM LICA INFORMACIJSKE PISMENOSTI NA RADNOM MJESTU

Relacijski model informacijske pismenosti C. Bruce nastao je u fenomenografskom istraživanju iskustava stručnjaka iz raznih disciplina pri korištenju informacijama.[60]

Model Sedam lica informacijske pismenosti pruža okvir za razumijevanje različitih aspekata informacijske pismenosti. Prema ovom modelu, informacijska pismenost sastoji se od sedam različitih "lica" ili načina doživljavanja i korištenja informacija. Svako lice predstavlja jedinstveni aspekt informacijske pismenosti i ima svoje karakteristike.

Dva ključna elementa prisutna su u svim kategorijama informacijske pismenosti - informacijska tehnologija i korištenje informacija. Treći element, koji čini svaku kategoriju različitom, varira zavisno o kontekstu i situaciji. Model ističe da pojedinci često koriste više pristupa informacijskoj pismenosti zavisno o situaciji u kojoj se nalaze.

C. Bruce[61] je u svome istraživanju navela da postoji sedam različitih dimenzija ili "lica" (Faces) iskustva u odnosu s informacijama, tj. sedam različitih načina interakcije između čovjeka i informacije:

Lice 1. - Informacijska tehnologija

Odnosi se na korištenje informacijskom tehnologijom radi informacijskog pristupa i komunikacije. Informacijska pismenost ovisi o mogućnostima korištenja tehnologije.

Lice 2. - Informacijski resursi

Odnosi se na pronalaženje informacija lociranih u raznim izvorima. Informacijska pismenost shvaćena je kao znanje o informacijskim izvorima te sposobnost pristupa izvorima. Neophodno je poznavati informacijske izvore i njihovu strukturu te ih samostalno koristiti.

[60] Ibid.
[61] Ibid.

Lice 3. - Informacijski procesi

Informacijska pismenost podrazumijeva i izvođenje određenih procesa. Informacijski procesi su strategije koje provode korisnici kad se nalaze u novim situacijama i nastoje riješiti problem.

Lice 4. - Informacijska kontrola

Informacijski pismene osobe su one koje se znaju koristiti raznim medijima kako bi "ovladale" relevantnim informacijama te ih stavile pod svoj utjecaj, kako bi ih mogli koristiti kada se ukaže potreba. Ključni element ove dimenzije je organizacija informacija.

Lice 5. - Konstruisanje znanja i izgradnja korpusa znanja

Obuhvata kritičko korištenje informacijama radi kreiranja lične baze znanja. Ovde je učenje, u smislu izgradnje baze znanja, svrha korisnika. To podrazumeva razvoj ličnih perspektiva o stečenom znanju i u potpunosti zavisi od kritičkog mišljenja ili analize.

Lice 6. - Proširivanje znanja

Pismenost se doživljava kao rad sa znanjem i ličnim perspektivama usvojenim na takav način da se steknu novi uvidi. Ovo šesto iskustvo zasnovano je na opsežnom ličnom znanju i iskustvu zajedno sa kapacitetom za kreativni uvid ili intuiciju. Ostaje misteriozna za one koji ga doživljavaju, ali oni su u velikoj mjeri zavisni od uvida u razvoj novih oblika znanja, novih pristupa zadacima ili novih rešenja.

Lice - 7. Mudrost

Informacijska pismenost promatra se u kontekstu mudrog korištenja informacijama za dobrobit drugih. Mudrost je lična kvaliteta koja se unosi u korištenje informacijama, a pojedinac mora voditi računa o širem kontekstu i okolini, što uključuje etičke procjene.

Za razliku od ostalih modela informacijske pismenosti, ovih sedam dimenzija informacijske pismenosti je izvedeno iz perspektive i istraživanja iskustava korisnika, a postupak informacijskog

opismenjavanja podrazumijeva izgradnju i razvijanje svijesti svih sedam vidova koji karakteriziraju informacijsko ponašanje.

Kroz model Sedam lica informacijske pismenosti pojedinci mogu razviti sveobuhvatnu informacijsku pismenost. To znači da će biti sposobni odabrati najprikladniji pristup za upotrebu informacija u različitim situacijama. Model naglašava važnost tumačenja iskustva i kompetencija u kontekstu informacijske pismenosti, što omogućuje razumijevanje informacija na dubljoj razini.

Model pruža okvir za analizu i razumijevanje različitih aspekata informacijske pismenosti te sugeriše da je idealno postizanje iskustva sa svih sedam lica informacijske pismenosti. Implementacija ovog modela može pružiti temelje za obrazovanje informacijske pismenosti i olakšati razvoj informacijski pismenih pojedinaca u različitim kontekstima. Za obrazovne institucije i nastavnike to znači da Model sedam lica informacijske pismenosti ukazuje na neke nove pravce u obrazovanju, ali potvrđuje i neke postojeće pristupe. Razna iskustva mogu biti povezana s ključnim informacijskim procesima na radnom mjestu, pružajući još jedan dokaz da je Model sedam lica generalizovan i da se može primjeniti i na druge situacije, a ne samo u odgojno-obrazovnim ustanovama.

Pa tako C. Bruce prikazuje odnos između Modela sedam lica i procesa u organizaciji.[62]

- Prvo lice: informacijska tehnologija pomaže korisnicima da ostanu informisani i da komuniciraju s kolegama unutar organizacije i širom svijeta
- Drugo lice: važno je poznavanje izvora informacija — uključujući organizacijski, ljudski, digitalni i printani izvor. Ljudi naglašavaju potrebu oslanjanja na informatičke stručnjake koji će ubrzati proces. Mislim da ljudi nemaju vremena sjesti i naučiti svaki novi paket koji izađe, i mislim da biste trebali moći koristiti osoblje koje ima to iskustvo.
- Treće lice: Zamršeno je povezano s iskustvom rješavanje problema ili donošenje odluka. Sami informacijski procesi nisu jednostavni. Neki ih smatraju kreativnom umjetnošću koju različiti provode na različite načine ljudi u različitim kontekstima.
- Četvrto lice: ljudi se fokusiraju na dovođenje relevantnih informacija u svoju ličnu sferu uticaja i upravljanje njima na takav način da ih je moguće pronaći. Ova kategorija govori o

[62] Bruce, Christine Susan (1999) Workplace experiences of information literacy. International Journal of Information Management, 19 (1). 33 - 47.

povezivanju informacija, projekata i ljudi pomoću mehaničkih alata (kao što su kartoteke), elektroničkih alata ili ljudskog mozga. Projekti koji se provode utiču na strukturu organizacija. Na taj se način stvaraju veze između informacija i pojedinih aspekata projekta.

- Peto lice: Informacijska pismenost se doživljava kao izgradnja lične baze znanja u novoj oblasti interesovanja. To uključuje razvoj ličnih perspektiva o stečenom znanju i u potpunosti ovisi o kritičkom razmišljanju ili analizi.
- Šesto lice: informacijska pismenost se doživljava kao rad sa znanjem i perspektivama usvojenim na takav način da se stiču novi uvidi. Ovo šesto iskustvo temelji se na opsežnom ličnom znanju i iskustvu zajedno sa sposobnošću kreativnog uvida ili intuicije. Ono ostaje tajanstveno za one koji ga iskuse, ali oni uvelike ovise o uvidima za razvoj novih oblika znanja, novih pristupa zadacima ili novih rješenja.
- Sedmo lice: informacijska pismenost se doživljava kao mudro korišćenje informacija u korist drugih. Profesionalno etičko ponašanje pojedinca prilikom rada sa drugima.

Model sedam lica namjenjen implementaciji u organizacijama obuhvata različite aspekte informacijske pismenosti kao što su osnovno znanje o informacijama, digitalna pismenost, kritičko razmišljanje, etičko korištenje informacija, kao i sposobnost komunikacije i kolaboracije putem informacijskih tehnologija. Model ističe važnost svjesnosti o sigurnosti informacija. Organizacije mogu koristiti ovaj model kako bi edukovale zaposlenike o sigurnosnim praksama i mjerama zaštite informacija. To uključuje prepoznavanje potencijalnih prijetnji, pravilno upravljanje lozinkama, zaštitu osjetljivih podataka i sprječavanja društvenog inženjeringa.

Implementacija ovog modela može pomoći organizacijama da osiguraju da njihovi zaposlenici imaju potrebne vještine i znanja za efikasno korištenje informacija u svakodnevnom radu. Na bazi Modela sedam lica biće izrađen model programa obuke ne-tehničkih lica zaposlenih u korporativnom okruženju, prilagođen za online učenje, kao i za učenje u fizičkom okruženju, kako bi bili u prilici odgovoriti na sigurnosne izazove današnjice.

Treći dio

ISTRAŽIVANJE - informacijske pismenosti i implementacije informacijske sigurnosti u organizaciji

U današnjem digitalnom okruženju, sve veći broj organizacija suočava se sa izazovima vezanim za sigurnost informacija i borbu protiv raznih cyber prijetnji. Organizacijski sigurnosni sistemi postaju neizostavni alati u zaštiti informacijskih resursa organizacija od zlonamjernog softvera, phishing napada i drugih sigurnosnih prijetnji. Istraživanje sigurnosnih sistema te ponašanja zaposlenih je sprovedeno u nekoliko organizacija u više od 15 država u Europi, Bliskom istoku i Africi, sa preko 2000 zaposlenih. U ovom istraživanju korišten je metod analize, pri čemu su analizirani logovi navedenih sigurnosnih sistema, kao i rezultati phishing testiranja.

Cilj ovog istraživanja je prezentovati rezultate analize da bi se identifikovale potencijalne cyber prijetnje u sigurnosnom okruženju organizacija. Provodi se i analiza rezultata phishing testiranja kako bi se utvrdila pripremljenost zaposlenika na prepoznavanje i izbjegavanje phishing napada. Fokus će biti na identifikovanju uzroka i faktora koji utiču na sigurnosne rizike te načina na koje zaposlenici pristupaju i upravljaju informacijskom sigurnošću u radnom okruženju. Kroz detaljnu analizu, istraživanje će pružiti uvid u ključne aspekte ponašanja zaposlenika koji mogu doprinijeti ranjivostima u cyber sigurnosti.

Na temelju dobijenih saznanja, cilj je kreirati društvene programe zaštite koji će edukovati zaposlenike o važnosti cyber sigurnosti, osvijestiti ih o potencijalnim prijetnjama i posljedicama neodgovornog ponašanja te ih podstaći na primjenu sigurnosnih praksi i procedura. Ovo istraživanje će unaprijediti sigurnosnu svijest zaposlenika i doprinijeti stvaranju sigurnijeg radnog okruženja u kontekstu informacijske sigurnosti.

Sistem prikupljanja podataka

Metodologija ovog istraživanja temelji se na kvantitativnoj analizi podataka prikupljenih u periodu od januara do augusta 2023. godine. Podaci su dobijeni iz anonimiziranih sigurnosnih logova iz različitih organizacija, specifično putem implementiranih sigurnosnih sistema kao što su

SentinelOne[63], Zscaler[64], Cisco Meraki[65], BigFix[66], Cisco Email Securty Gateway[67] i iZOOlogic[68]. Ovi sistemi su omogućili detaljno razumijevanje učestalosti i vrsta sigurnosnih prijetnji koje su trenutno prisutne. Dodatno, sprovedena su kontrolisana phishing testiranja uz pomoć sistema kompanije "KnowBe4"[69] kako bi se ocijenila sposobnost zaposlenika da identifikuju i adekvatno reaguju na simulirane phishing napade. Rezultati ovih testova pružili su kvantitativne podatke o uspješnosti zaposlenika, što je ključno za evaluaciju postojećih sigurnosnih edukacija.

Analiza prikupljenih podataka izvedena je koristeći napredne statističke metode. Statistička obrada uključivala je analizu frekvencije pojavljivanja različitih vrsta sigurnosnih incidenata, kao i procjenu efikasnosti zaposlenika u prepoznavanju potencijalnih phishing napada. Kroz ovu analizu, prepoznati su ključni obrasci i trendovi koji su vitalni za razumijevanje i mitigaciju trenutnih i budućih sigurnosnih rizika.

SentinelOne je specijalizovan za razvoj naprednih rešenja za zaštitu od napada, otkrivanje prijetnji i odgovor na incidente. Ova platforma pruža sveobuhvatnu zaštitu od različitih vrsta cyber prijetnji, uključujući malware, ransomware, i druge sofisticirane napade. U svojoj suštini pruža zaštitu na nivou uređaja (endpointa), identifikujući i neutrališući prijetnje prije nego što izazovu štetu.

Zscaler platforma pruža siguran pristup internetu i aplikacijama iz bilo kog uređaja i bilo kog mjesta. Ova platforma omogućuje organizaciji da osigura sigurnost i zaštitu svojih mreža, podataka i aplikacija putem cloud-based rješenja. U svrhu ovog istraživanja analizirali smo logove sigurnosnih funkcija, sigurnost web prometa, filtriranje internetskog prometa, sprječavanje neovlaštenog pristupa.

Cisco Meraki servis je korišten za upravljanje organizacijskim računarskim mrežama, odnosno za upravljanje i konfiguraciju mrežne opreme (Wireless Access Point, Ethernet switch, firewall),

[63] SentinelOne. (n.d.). Retrieved from https://www.sentinelone.com/
[64] Zscaler. (n.d.). Retrieved from https://www.zscaler.com/
[65] Cisco Meraki. (n.d.). Retrieved from https://meraki.cisco.com/
[66] HCL Software. (n.d.). BigFix. Retrieved from https://www.hcl-software.com/bigfix
[67] Cisco. (n.d.). Cisco Secure Email Advanced Email Protection Data Sheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html
[68] Izoologic. (n.d.). Retrieved from https://izoologic.com/
[69] KnowBe4. (n.d.). Retrieved from https://www.knowbe4.com/

kontrole saobraćaja, generisanja detaljnih analitičkih izvještaja.

BigFix platforma omogućuje organizacijama da centralizirano upravljaju i nadziru svoje IT resurse, uključujući računare, mobilne uređaje, servere, aplikacije i sigurnosne politike. BigFix se koristi za automatizaciju instaliranja, konfiguraciju, upravljanje zakrpama i sigurnosnim politikama. Ova platforma je korištena za analizu potencijalnih insajderskih sigurnosnih prijetnji.

Cisco Email Security Gateway (CES) koristi Cisco tehnologiju sigurnosti e-maila za blokiranje neželjenih (spam) i naprednih prijetnji e-maila kao što su ransomware, BEC i phishing napadi. Bilo da se radi o internoj ili eksternoj komunikaciji, svaka poruka koja ulazi ili izlazi iz poštanskog sandučića se tretira sa istim nivoom kontrole. Na ovaj način organizacija minimizira širenje insajderskih prijetnji, bilo da se radi o zlonamjernom akteru unutar organizacije ili kompromitovanom poštanskom sandučiću. Tačnije, ova tehnologija skenira sve emailove koji prolaze kroz mail servere u svim smjerovima – dolazne, odlazne ili interne.

iZOOlogic platformu odnosno servis, organizacije koriste za cyber odbranu digitalne imovine. Usluga zaštite brenda je pristup koji klijenti koriste kako bi zaštitile svoj brend od negativnih uticaja, prevara i zloupotreba na internetu. To uključuje aktivnosti poput praćenja online aktivnosti i komunikacija koje se odnose na brend, suzbijanje lažnih ili neovlaštenih predstavljanja brenda, zaštitu intelektualnog vlasništva i autorskih prava, što osigurava da se brend predstavlja na internetu na način koji odgovara njegovoj reputaciji i vrijednostima. Izoologic zaštita brenda može uključivati korištenje alata za praćenje društvenih medija, analitičkih alata, praćenje online recenzija i komentara, te suradnju s pravnim timovima kako bi se reagiralo na prijetnje i kršenja prava brenda.

U organizacijama gdje je provedeno testiranje, pored kompleksne infrastrukture i sigurnosnih sistema, postoji i poseban ured koji se bavi informacijskom sigurnosti. Viši direktor za informacijsku sigurnost (engl. Chief information security officer, CISO) ili menadžer informacijske sigurnosti rukovodi uredom. Postoje jasna pravila i procedure o informacijskoj sigurnosti unutar organizacija, a to su ključni elementi u održavanju visokog standarda te pomažu u sprječavanju sigurnosnih incidenata i zaštiti osjetljivih informacija. Pravila o informacijskoj sigurnosti postavljaju temeljna pravila i očekivanja vezana za određene aktivnosti ili situacije u organizacijama. Na primjer, jedna od politika definiše kako se podaci trebaju čuvati i dijeliti unutar

ureda. Procedure su detaljni koraci ili postupci koje zaposlenici slijede kako bi ispunili zahtjeve politike. Na primjer, za politiku u organizaciji koja definiše kako se podaci trebaju čuvati, procedura opisuje kako i gdje sačuvati, dijeliti i koristiti podatke u skladu sa politikom. Kombinacija politika i procedura osigurava da organizacije imaju jasna pravila i puteve djelovanja kako bi se osigurala usklađenost, sigurnost i učinkovitost u poslovanju.

Za potrebe ovog istraživanja potpisan je pravni dokument (eng. Non-disclosure Agreement - NDA) koji se koristi za zaštitu povjerljivih informacija i podataka između istraživača i organizacija. Ovaj ugovor postavlja pravila i ograničenja o tome kako se povjerljive informacije mogu koristiti, dijeliti i otkrivati. Ugovor postavlja ograničenja da se informacije koriste isključivo u svrhu istraživanja i da ih se neće dijeliti s trećim stranama. Ova ograničenja uključuju i neotkrivanje određenih informacija koje bi mogle otkriti identitet organizacija ili druge osjetljive detalje. Naziv organizacija, te u kojim zemljama posluju i ostale informacije koje bi mogle otkriti identitet organizacija neće biti javno dostupne u ovom istraživanju.

Vanjske prijetnje informacijskoj sigurnosti organizacije

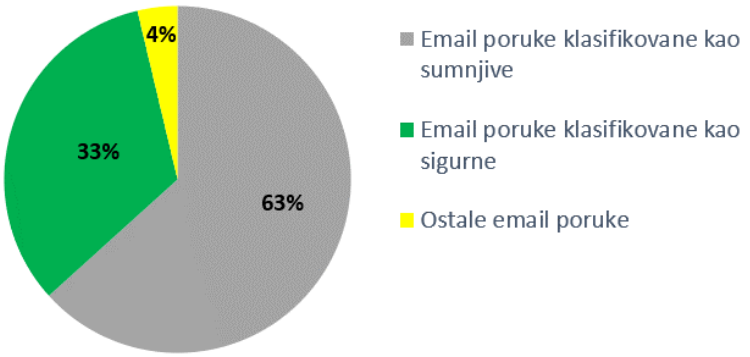
U ovom dijelu istraživanja fokus će biti na istraživanju i analizi različitih vanjskih prijetnji koje organizacije susreću u području informacijske sigurnosti. Posebno će biti posvećena pažnja prijetnjama koje dolaze izvana, poput napada na email, zlonamjernog softvera, fizičkih napada, socijalnog inženjeringa i zloupotrebe brenda. Kroz analizu relevantnih informacija, dobivenih za period januar – august 2023. ovaj dio rada će pružiti pregled trenutnog stanja informacijske sigurnosti. Velik broj sigurnosnih prijetnji koji dolaze izvan organizacija zabilježen je kroz sigurnosne servise, što nam govori o važnosti njihovog praćenja, registriranja i adekvatnog procesuiranja u cyber sigurnosnom okruženju.

Analizirane su sve sigurnosne prijetnje i rizici koji su se desili u tom vremenskom periodu, te obuhvataju različite vrste prijetnji kao što su phishing, malware, i slično. Ovdje napominjem da podaci prikupljeni u periodu od januara do augusta 2023. ne prikazuju broj cyber napada sa ili bez posljedica po organizacije, već prikazuju događaje u cyber prostoru u vlasništvu organizacija sa

ciljem podizanja svijesti o svakodnevnim opasnostima s kojim se organizacije i njihovi zaposleni susreću.

Najveći dio od ukupnog broja registrovanih sigurnosnih prijetnji povezan je sigurnosti e-maila, što obuhvata potencijalno blokiranje neželjene komunikacije i naprednih e-mail prijetnji. U posljednjem mjesecu promatranog perioda, augustu, detaljna analiza je pokazala da 63% od svih generisanih e-mail poruka predstavljaju sumnjivi saobraćaj.

Grafikon 1. Kompletan e-mail saobraćaj izražen u postocima za august 2023.

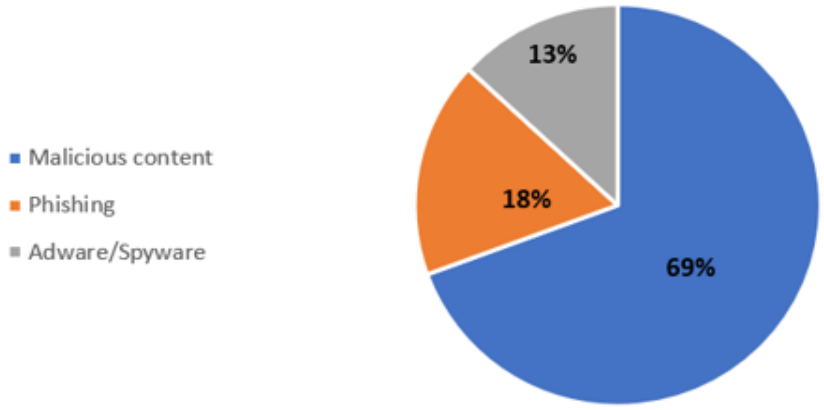


Izvor: Autor

Daljom analizom svih sumnjivih poruka, dolazimo do zaključka da njih 3.22% su sigurnosne prijetnje. Izdvojiću statistički najznačajnije: 2.04% e-mailova koji su identifikovani i blokirani kao spam, 0.52% su blokirani na osnovu autentifikacije e-mailova kako bi se spriječile lažne poruke i 0.35% koji su blokirani zbog sadržaja koji nije dopušten. Generalno, najviši postotak je kod anti-spam zaštite, što sugeriše da je spam najčešći problem. Ostali tipovi zaštite, kao što su anti-virus i napredna zaštita od malwarea, nisu identifikovali značajan broj prijetnji u ovom setu podataka. Ovi podaci najbolje ilustruju koliko je bitno da organizacija ima mogućnost korištenja naprednih odbrambenih alata u svom poslovanju, s obzirom na to da se događaji odvijaju brzo u stvarnom vremenu. Iako se prosječnom korisniku može činiti da je ovo velik postotak napada na e-mail servise organizacije, za IT stručnjake ovo nije iznenađenje.

Drugi najveći broj prijetnji, u mjesecu augustu 2023. bilježimo putem servisa Zscaler. Izraženo u postocima, od ukupnog broja napada 69% su pokušaji iz kategorije zlonamjernog sadržaja. U ovu kategoriju zlonamjernog sadržaja spadaju web stranice koje pokušavaju preuzeti opasan sadržaj u internetski preglednik (engl. Internet browser) prilikom posjete.[70] Zlonamjerne web stranice uključuju komplete za eksploataciju, ugrožene web stranice i zlonamjerno oglašavanje.

Grafikon 2. Registovani napadi za august 2023. od servisa Zscaler u postocima.



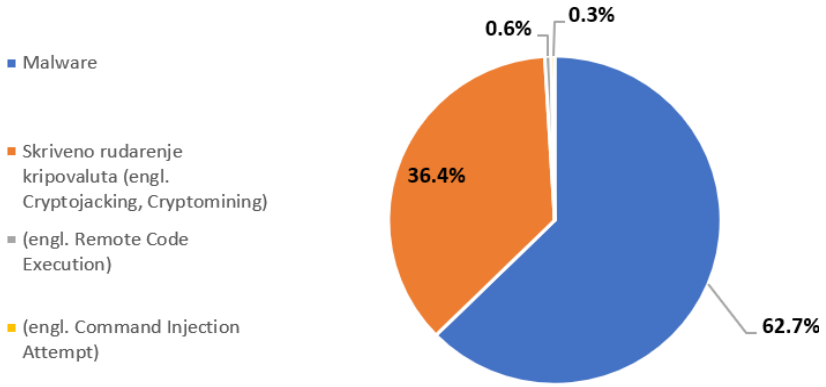
Izvor: Autor

Sljedeći po obimu napada su napadi na lokalnu infrastrukturu organizacija su zabilježeni na Cisco Meraki servisima. Od ukupnog broja napada na Cisco Meraki servisima, više od 60% napada registrovano je kao malver. Druga relativno nova vrsta prijetnje sa 36,4% je skriveno rudarenje kriptovaluta, u kojoj zlonamjerni korisnici pokušavaju iskoristiti računarske resurse posjetitelja u rješavanju složenog algoritma za rudarenje kriptovaluta. U idealnom slučaju, to bi se moglo nazvati „krađom računarskih resursa“. Ono što ovaj napad čini veoma rizičnim je činjenica da krajnji korisnik uglavnom nije ni svjestan napada. Koncept pristanka „krajnjeg korisnika“ se ne primjenjuje što izaziva ozbiljne etičke zabrinutosti po ovom pitanju. U poslovnom okruženju, ovo bi moglo predstavljati značajne troškove ako bi veliki broj korisničkih mašina postao žrtva skrivenog rudarenja.[71]

[70] Rezultati dobijeni prema predefinisanoj kategorije prijetnji unutar Zscaler Sistema, gdje se grupišu zajedničke prijetnje (npr. virusi, botnetovi, eksploatacije). Zscalerov sistem za prevenciju upada (IPS) koristi detekciju zasnovanu na potpisu za identifikaciju i kontrolu ovih pretnji. Zlonamjerni sadržaj uključuje web stranice koje pokušavaju preuzeti opasan sadržaj u vaš preglednik kada ih posjetite. Ovaj sadržaj se preuzima tiho bez znanja ili svijesti korisnika.

[71] Cisco Systems, Inc. (2017) Cryptojacking: Hijacking your computer resources. Retrived from

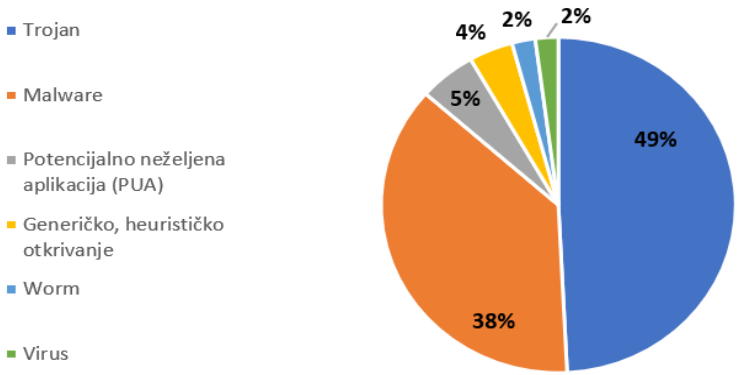
Grafikon 3. Registovani napadi za august 2023. od servisa Cisco Meraki u postocima.



Izvor: Autor

Cyber prijetnje zabilježene od sistema SentinelOne kao zadnja linija odbrane zaposlenih i uređaja koji zaposleni koriste 89% čini zlonamjerni softver, od čega 49% su napadi povezani sa Trojancima, dok 38% su ostali napadi svrstani u malver.

Grafikon 4. Registovani napadi za august 2023. od servisa SentinelOne u postocima

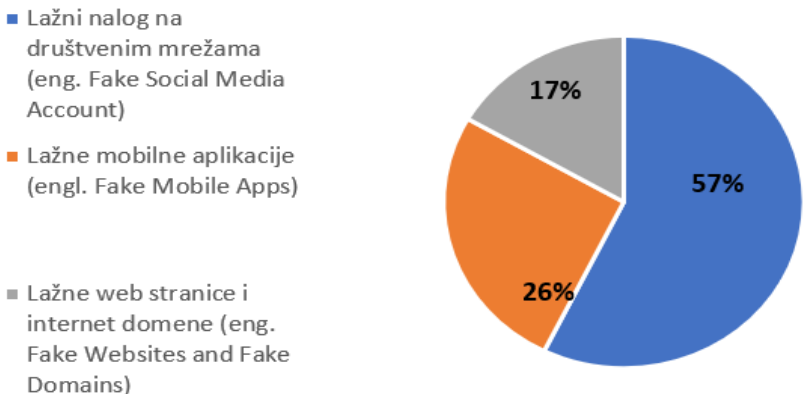


Izvor: Autor

Zloupotreba imena odnosno brenda organizacije, pored direktnih napada na infrastrukturu i servise organizacije, sve češći je cilj napadača. Tako za posljednji mjesec posmatranog perioda, putem iZoologic servisa bilježimo desetine napada.

https://blogs.cisco.com/security/cryptojacking-hijacking-your-computer-resources

Grafikon 5. Registovane zloupotrebe brenda organizacije za august 2023. od iZoologic servisa u postocima



Izvor: Autor

Posebno zabrinjavajuće je da od ukupnog broja pokušaja zloupotrebe imena ili reputacije kompanija, 57% su potencijalno opasne aktivnosti na društvenim mrežama koje mogu imati za cilj promjenu javnog mijenja ili rasplamsavanje diskursa vezanih za velike nacionalne ili globalne događaje. Ništa manje ne zabrinjava podatak da 43% su pokušaji zloupotrebe putem lažnih web stranica i mobilnih aplikacija, koje napadači koristi se za krađu podataka ili instaliranje malicioznih kodova sa ciljem sticanja finansijske koristi. Ovo može uključivati ransomware ili krađu sredstava s bankovnih računa korisnika, a sve to bez njihovog pravovremenog saznanja o ovim aktivnostima.

Praćenje vanjskih prijetnji i adekvatna reakcija na njih igraju kritičnu ulogu očuvanja integriteta, povjerljivosti i dostupnosti informacijskih sistema. Cyber napadi često ciljaju na povjerljive informacije i intelektualnu svojinu. Implementacija strategija za praćenje vanjskih prijetnji može pomoći u zaštiti ovih kritičnih resursa, osiguravajući kontinuitet poslovanja i zaštitu od krađe podataka. Incidenti u vezi sa cyber sigurnošću mogu ozbiljno narušiti ugled organizacije. Praćenje i reagovanje na vanjske cyber sigurnosne prijetnje predstavlja temeljni aspekt moderne cyber sigurnosne strategije. Implementacija proaktivnih mjera, baziranih na akademskim, industrijskim istraživanjima i najboljoj praksi, može značajno smanjiti rizik od cyber incidenata, zaštititi integritet organizacijskih podataka i osigurati kontinuitet poslovanja. Ovo je ključno za očuvanje povjerenja klijenata i partnera, te za usklađenost s regulatornim zahtjevima.

Unutrašnje prijetnje informacijskoj sigurnosti organizacije

Unutrašnja odnosno insajderska prijetnja se odnosi na mogućnost insajdera da iskoristi svoj ovlašteni pristup ili znanje da nanese štetu kompaniji. Ova šteta može uključivati zlonamjerne, nedozvoljene ili nenamjerne radnje koje negativno utiču na integritet, povjerljivost, dostupnost i privatnost podataka, resursa, informacija, sistema, osoblja ili sredstava kompanije. U ovom dijelu rada ću istražiti i analizirati različite unutrašnje prijetnje s kojima se organizacije susreću u kontekstu informacijske sigurnosti.

Indikatori za definisanje insajderskih prijetnji u ovom istraživanju su:

- Sigurnosne prijetnje registrovane filtriranjem URL-ova
- Neovlaštena promjena ili konfiguracija sigurnosnih kontrola.
- Igre – aktivno igranje na računaru i/ili mreži.
- Torrent – Program za ilegalno preuzimanje sadržaja zaštićenog autorskim pravima.

Analiza unutrašnjih prijetnji je rađena uz pomoć servisa filtriranje URL-ova, koji otkriva i blokira dio ili kompletan sadržaj web stranica prema definisanim kategorijama, tipa sadržaje vezane za kockanje i drugo[72]. Važno je napomenuti da u organizacijama gdje sam radio istraživanje, URL filtriranje ima kontrolu nad kompletnim web prometom, te registruje i/ili blokira najmanju sigurnosnu prijetnju, poput neprikladnih reklama na web stranici ili rezultate pretraživanja. Servis Bigfix identificira manipulaciju sigurnosnih kontrola na računarima, neovlaštene programe i igre.

Nakon analize logova, prečišćavanja i kreiranja skupina podataka (dataset) urađena je standardizacija različitih skupova podataka radi boljeg poređenja i analize, pomoću statističke Z-score normalizacija tehnike[73]. Z-score normalizacija, poznata i kao standardizacija, primenjena je na svaki dataset. Ova tehnika transformiše podatke tako da imaju srednju vrijednost (mean) 0 i standardnu devijaciju 1. Računa se prema formuli prikazanoj $z = (x - \mu) / \sigma$ gdje je σ standardna

[72] URL filtriranje omogućava organizaciji da konfiguriše način na koji korisnici pristupaju web stranicama preko svoje mreže ili drugih sistema, što ga čini ključnim načinom zaštite korisnika i podataka od krađe identiteta, ransomware-a i drugih prijetnji; kontrola korištenja propusnog opsega; održavati produktivnost zaposlenih; i ograničiti odgovornost organizacije ograničavanjem pristupa neprikladnom sadržaju.

[73] Christmann, E. P., Badgett, J. L. (2009). Interpreting Assessment Data: Statistical Techniques You Can Use. Washington DC. NSTA Press.

devijacija, a x aritmetička sredina promatrane varijable. Kao i u drugim tehnikama skaliranja podataka, x označava vrijednost varijable dok je z skalirana, odnosno standardizovana x vrijednost.

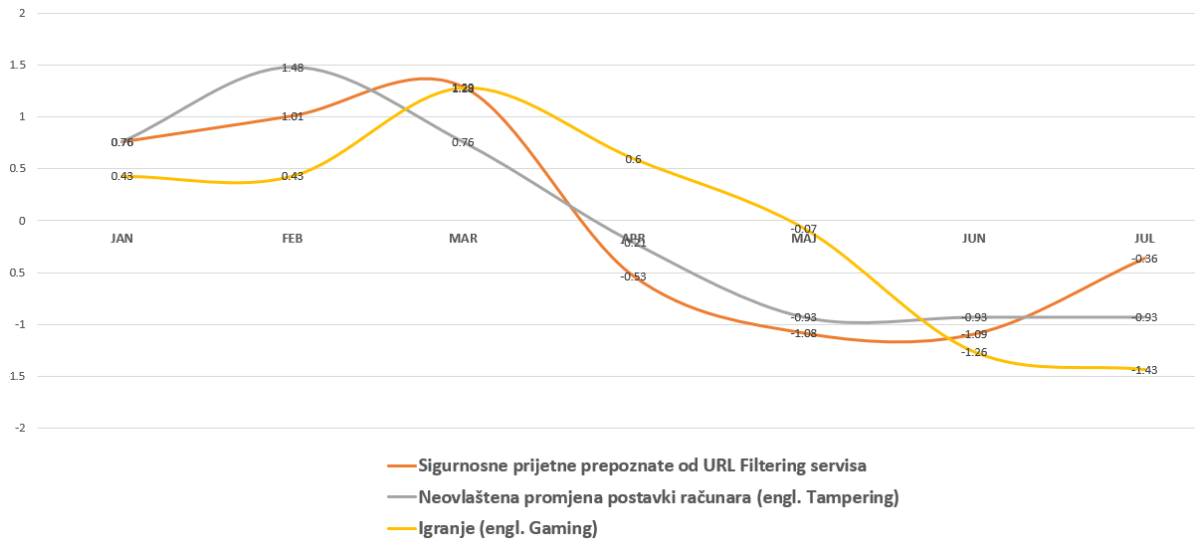
Na osnovu informacija iz sistema za kontrolu kompletnog web prometa, kao i centralizovanog upravljanja i nadzora IT resursa, dobili smo sljedeće sažete informacije o unutrašnjim prijetnjama, fokusirajući se na događaje sistema, korisnika i aplikacija za period od januara do jula 2023.

Tabela 1. Unutrašnje prijetnje po mjesecima za period januar – juli 2023.

Indicators	JAN	FEB	MAR	APR	MAJ	JUN	JUL
Sigurnosne prijetne prepoznate od URL Filtering servisa	0.76	1.01	1.29	-0.53	-1.08	-1.09	-0.36
Neovlaštena promjena postavki računara (engl. Tampering)	0.76	1.48	0.76	-0.21	-0.93	-0.93	-0.93
Igranje (engl. Gaming)	0.43	0.43	1.28	0.6	-0.07	-1.26	-1.43
Neovlašten program - Torrent or similar	-	-	-	-	-	-	-

Izvor: Autor

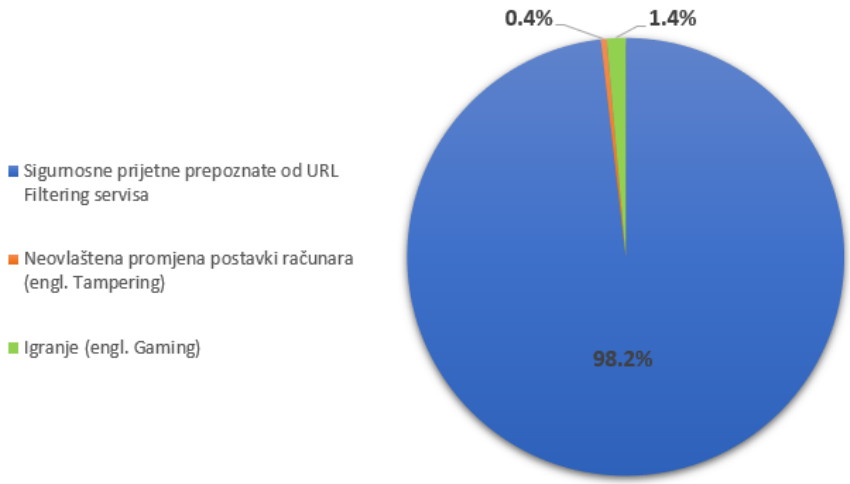
Grafikon 6. Unutrašnje prijetnje po mjesecima za period januar – juli 2023.



Izvor: Autor

Analizom svih unutrašnjih prijetnji za period januar - juli 2023. najveći dio prijetnji dolazi iz kategorije URL filtriranja.

Grafikon 7. Unutrašnje prijetnje po mjesecima za period januar – juli 2023 u postocima



Izvor: Autor

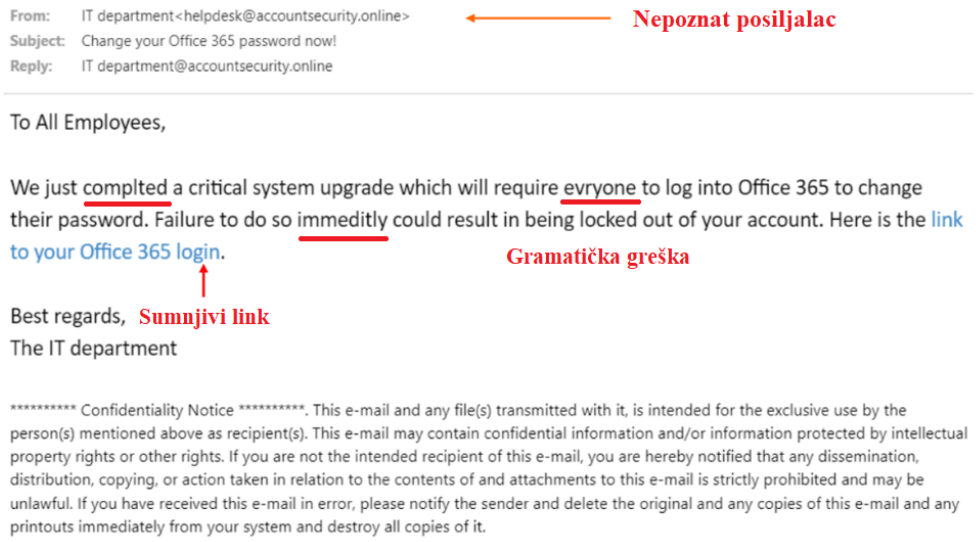
Detaljnom analizom svih zabilježenih sigurnosnih incidenata, tim stručnjaka za informacijsku sigurnost otkrio je da je od ukupnog broja unutrašnjih prijetnji, prijetnje u kategorijama neovlaštena promjena postavki računara i gaming izazvano je direktno od strane uposlenih. Kako bi se suočila s ovim internim prijetnjama, organizacije su pokrenule disciplinski postupak (u ovim slučajevima upozorenje) protiv zaposlenika u skladu sa svojim pravilima i pravilnikom o radu.

Ovi podaci jasno pokazuju važnost praćenja i analize sigurnosnih prijetnji i incidenata, te pravovremene reakcije na internu prijetnju informacijskoj sigurnosti.

Izvještaj o Phishing Testiranju Uposlenih

U periodu od januara do jula 2023. provedeno je testiranje na krađu identiteta, odnosno simulirano phishing testiranje, kako bi se procijenio nivo svjesnosti i reakcija zaposlenih na potencijalne phishing prijetnje. Svim zaposlenim jednom mjesečno je poslan simuliran phishing e-mail koji je imao oblik i sadržaj sličan stvarnim phishing porukama.

Ilustracija 2. Primjer poruke koja je poslana u februaru 2023



Izvor: Autor, Organizacije u kojima je rađeno istraživanje

Praćena je stopa odziva i klikanja na sumnjivi link u phishing e-mailu, kroz 7 mjeseci testnog perioda. Najviše „*upecanih*" je bilo u februaru, kada je 240 korisnika otvorilo e-mail i kliknulo na sumnjivi link.

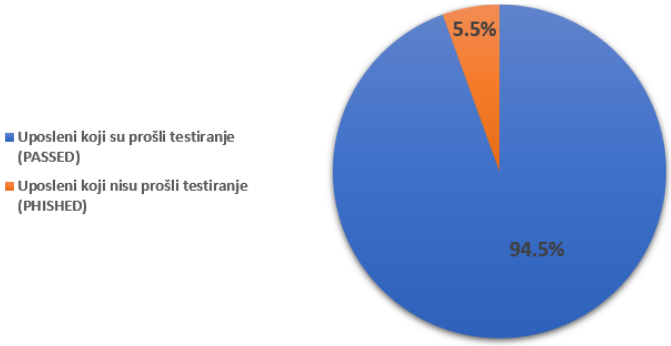
Tabela 2. Rezultati simuliranog phishing testiranja po mjesecima za period januar – juli 2023

Izvori	JAN	FEB	MAR	APR	MAJ	JUN	JUL
Uposleni koji su prošli testiranje (PASSED)	1,565	1486	1647	1717	1667	1622	1709
Uposleni koji nisu prošli testiranje (PHISHED)	161	240	79	9	59	104	17
Total	**1,726**	**1,726**	**1,726**	**1,726**	**1,726**	**1,726**	**1,726**

Izvor: Autor

Analizirajući prosjek za navedeni period, od svih stalno zaposlenih koji su testirani na phishing, 5.5% zaposlenih nisu prošli testiranje.

Grafikon 8. Prosječni rezultati simuliranog phishing testiranja u postocima za period januar – juli 2023.



Izvor: Autor

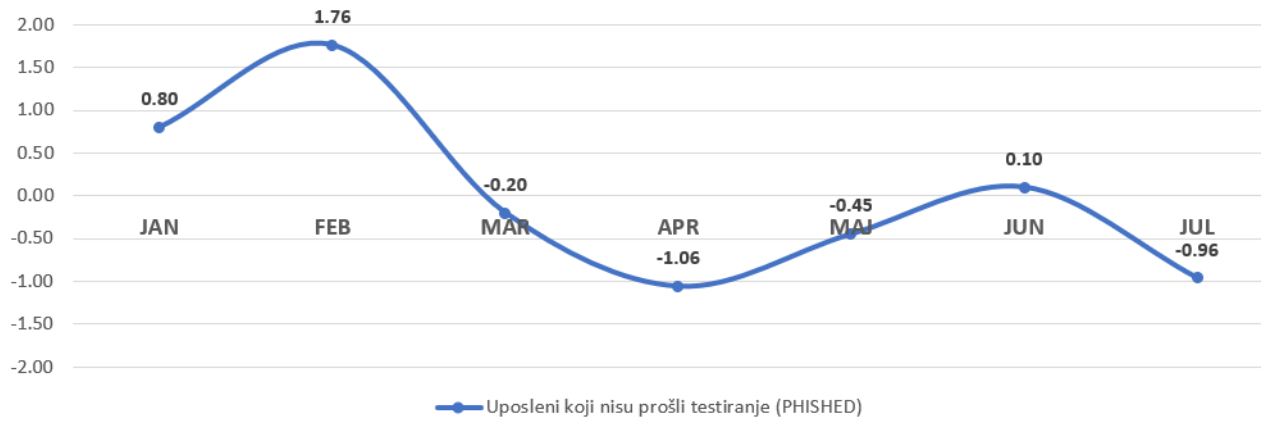
Radi boljeg poređenja i analize, pomoću statističke Z-score normalizacija metode i za ovaj skup podataka urađena je standardizacija.

Tabela 3. Normalizovani rezultati za kategoriju “phished”

Izvori	JAN	FEB	MAR	APR	MAJ	JUN	JUL
Uposleni koji nisu prošli testiranje (PHISHED)	0.80	1.76	-0.20	-1.06	-0.45	0.10	-0.96

Izvor: Autor

Grafikon 9. Rezultati za kategoriju “phished” po mjesecima za period januar – juli 2023.



Izvor: Autor

Svi zaposleni, nakon što su kliknuli na sumnjivi link, dobili su obavijest da su postali žrtve lažnog phishing napada, uz dodatne savjete za podizanje svijesti o informacijskoj sigurnosti. Phishing testiranje je važan alat za procjenu i poboljšanje sigurnosne svijesti uposlenika. I pored relativno malog procenta broja „upecanih“, potrebno je kontinuirano raditi na edukaciji zaposlenih i primjeni sigurnosnih procedura kako bi se zaštitili od potencijalnih cyber prijetnji.

Obuka o informacijskoj sigurnosti i zaštiti podataka

U sklopu strategije zaštite informacijske sigurnosti, u organizacijama u kojima je provedeno istraživanje, obavezan je trening za sve zaposlenike iz područja informacijske sigurnosti. Obuka o informacijskoj sigurnosti i zaštiti podataka ima za cilj edukovati zaposlene o važnosti sigurnosti podataka, prepoznavanju cyber prijetnji, te pravilnom postupanju u slučaju incidenta ili napada. Ova

obuka se izvodi online, jednom godišnje u drugoj polovini februara.

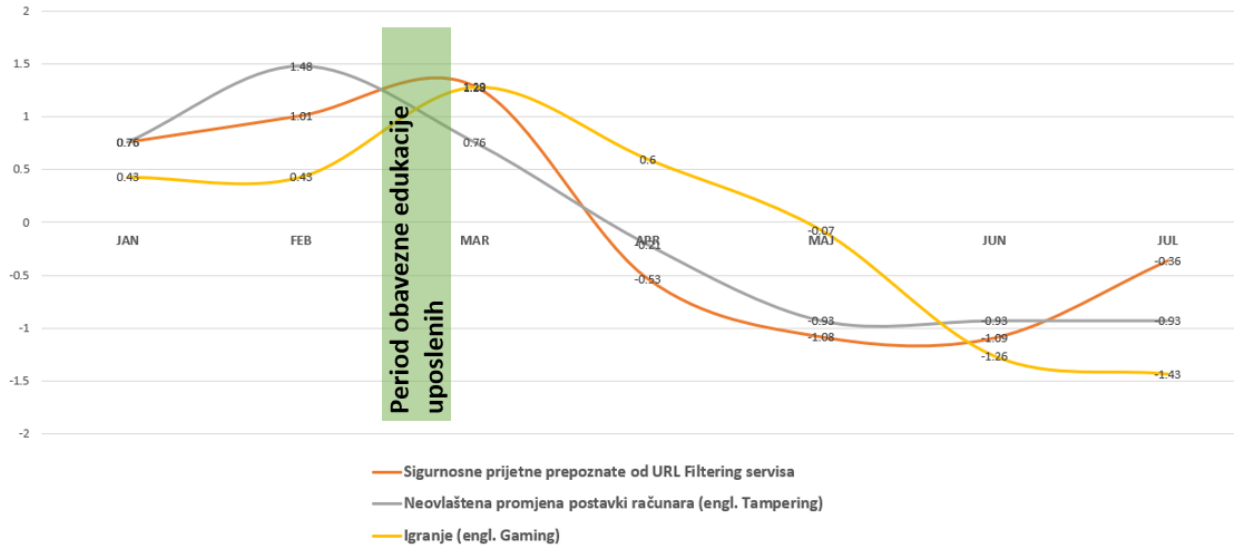
Kroz obavezni trening, organizacijski cilj je osposobiti zaposlene kako prepoznati phishing napade, zaštititi svoje korisničke račune i lozinke, te kako pravilno postupati s osjetljivim podacima. Također, trening će ih uputiti u korištenje sigurnosnih alata i praksi koje organizacije preporučuju za očuvanje sigurnosti informacija.

Rezultati istraživanja

Kada uporedimo dobijene rezultate istraživanja vezanih za unutrašnje prijetnje, prepoznavanje phishing prijetnji i incidenata u organizaciji, evidentan je trend smanjenja broja svih prijetnji nakon perioda obavezne edukacije, koja je završena početkom marta 2023.

Pogledajmo trendove na grafikonima:

Grafikon 10. Cybersecurity – Unutrašnje prijetnje za period januar – juli 2023. promjene nakon perioda obavezne edukacije.



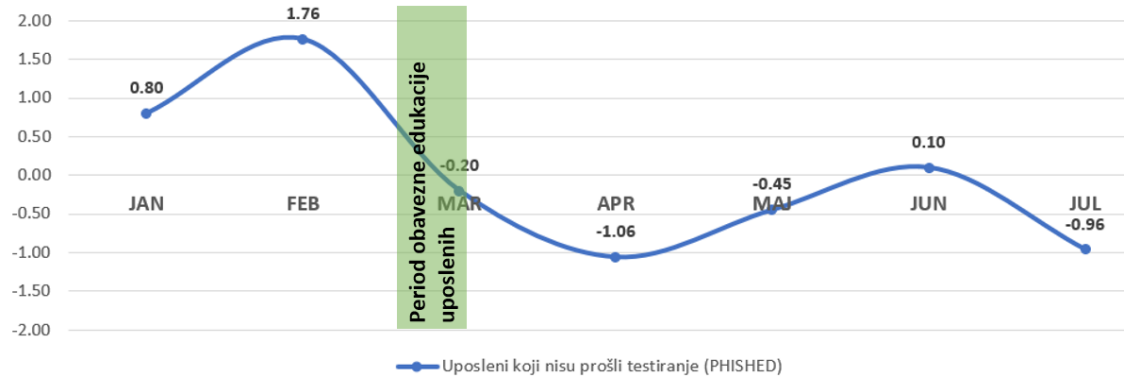
Izvor: Autor

U kategoriji „Sigurnosne prijetnje prepoznate od URL Filtering servisa“, broj prijetnji se znatno smanjuje od aprila do jula u odnosu na mart 2023. Nakon treninga, broj unutrašnjih prijetnji značajno opada, što može ukazivati na pozitivan utjecaj treninga na smanjenje svih unutrašnjih prijetnji. U kategoriji „Neovlaštena promjena postavki računara (engl. Tampering)“ prije treninga, broj prijetnji je najviši u februaru. Nakon treninga, broj prijetnji opada i ostaje konzistentno nizak, što može ukazivati na pozitivan utjecaj treninga. U kategoriji „Igranje (engl. Gaming)“ prije treninga, broj prijetnji je konzistentno iznad prosjeka. Tokom treninga, one dostižu vrhunac u martu 2023. Nakon treninga, broj unutrašnjih sigurnosnih prijetnji opada značajno u junu i julu 2023. što može ukazivati na pozitivan utjecaj treninga na smanjenje rizika zloupotrebe resursa organizacije.

Na osnovu ovih rezultata možemo zaključiti da redovno, obavezno provođenje treninga o informacijskoj sigurnosti smanjuje broj unutrašnjih prijetnji, što potvrđuje posebnu hipotezu a) *Obavezan trening uposlenih o informacijskoj sigurnosti tokom godine dovodi do značajnog smanjenja unutrašnjih sigurnosnih prijetnji.*

Prijetnje u kategorijama neovlaštena promjena postavki računara i gaming izazvane direktno od uposlenika smatramo sigurnosnim incidentima. Analizom dobijenih rezultata istraživanja o sigurnosnim incidentima za navedene kategorije, evidentan je trend smanjenja broja incidenata informacijske sigurnosti nakon perioda obavezne edukacije, što potvrđuje posebnu hipotezu b) *Redovno provođenje treninga o informacijskoj sigurnosti smanjuje broj sigurnosnih incidenata u organizaciji izazvani ponašanjem zaposlenih*.

Grafikon 11. Cybersecurity – Phishing testiranje, broj „upecanih“ za period januar – juli 2023. promjene nakon perioda obavezne edukacije.



Izvor: Autor

Primjetno je da prije treninga za kategoriju phishing testiranje, broj „upecanih“ je konzistentno iznad prosjeka. Nakon treninga, rizik od phishing napada opada značajno u aprilu i maju 2023. što ukazuje na pozitivan uticaj treninga. Analizom podataka za phishing testiranje, sposobnost zaposlenika da prepoznaju phishing napade i druge oblike socijalnog inženjeringa značajno je povećana nakon provođenja treninga.

U izvještaju o otpornosti na phishing napade (engl. Phish-prone™) kompanije KnowBe4,[74] analiziran je skup podataka od preko 12,5 milijuna korisnika, u 35,681 organizacija, s više od 32,1 milijuna simuliranih phishing sigurnosnih testova, u 19 različitih industrija. Ukupni osnovni prosjek otpornosti na phishing napade za 2023. u svim industrijama i organizacijama iznosio je 33,2%. U fazi gdje su mjerene vještine podizanja svijesti o sigurnosti nakon 12 mjeseci ili više kontinuiranog osposobljavanja i simuliranih phishing sigurnosnih testova, pokazuje da je dosljedan, zreli program obuke za podizanje svijesti osnovni prosijek se smanjio sa 33,2% na 5,4%. Ti su rezultati dosljedno dokazani u svim industrijskim veličinama i vertikalama. Nakon godinu dana ili više obuke o sigurnosnoj svijesti u kombinaciji s čestim simuliranim phishing testovima, organizacije svih veličina i industrija drastično su se poboljšale. Za velike organizacije preko 1,000 zaposlenih vidjeli smo prosječnu ocjenu poboljšanja od 82% od osnovnog testiranja do jedne godine, odnosno prosječni rezultati testiranja sigurnosti krađe identiteta nakon godinu dana i više kontinuiranog osposobljavanja iznose 5,9%.

Upoređujući rezultate našeg istraživanja u periodu od januara do jula 2023. provedenog za testiranje na krađu identiteta, odnosno phishing testiranje, sa rezultatima iz izvještaja o otpornosti na phishing napade (engl. Phish-prone™)[75] prema referentnim industrijskim vrijednostima za 2023. vidimo da su prosječni rezultati od 5,5% zaposlenih koji nisu prošli testiranje, u industrijskom standardu.

Na osnovu ovih rezultata možemo zaključiti da redovno provođenje treninga o informacijskoj sigurnosti i redovno phishing testiranje povećava sposobnost zaposlenika da prepoznaju phishing napade i druge oblike socijalnog inženjeringa. Dalje, na osnovu ovih rezultata, mogu se potvrditi posebne hipoteze: c) *Redovno provođenje treninga o informacijskoj sigurnosti smanjuje broj*

[74] KnowBe4. (2023). 2023 Phishing By Industry Benchmarking [Report]. Retrieved from https://info.knowbe4.com/en-us/phishing-by-industry-benchmarking-report
[75] Ibid.

phishing napada koji uspješno prevare korisnike i d) *Redovno provođenje simuliranih phishing sigurnosnih testova povećava sposobnost zaposlenika da prepoznaju phishing napade i druge oblike socijalnog inženjeringa.*

Na osnovu analize podataka o unutrašnjim sigurnosnim prijetnjama, incidenata izazvanih ponašanjem zaposlenih, simuliranih phishing napada, zabilježili smo značajno smanjenje broja svih unutrašnjih prijetnji nakon obavezne edukacije zaposlenika. Pored relativno malog uzorka podataka i kratkog vremenskog perioda, vizualizacija i z-score normalizacija jasno pokazuju trend smanjenja broja incidenata informacijske sigurnosti nakon perioda obavezne edukacije. Opaženi trendovi i vizualna analiza pružaju dovoljno dokaza za donošenje praktičnih odluka i potvrđivanja posebnih hipoteza.

Na osnovu analize podataka o vanjskim sigurnosnim prijetnjama, primijetili smo da je neophodno da organizacije razviju tehničke sisteme koji će omogućiti praćenje vanjskih prijetnji i adekvatnu reakciju, kako bi očuvale integritet, povjerljivost i dostupnost informacijskih sistema i informacija. Praćenje i reagovanje na vanjske prijetnje informacijskoj sigurnosti predstavljaju ključni aspekt moderne strategije informacijske sigurnosti.

Na temelju svih dobijenih rezultata istraživanja, možemo zaključiti da je generalna hipoteza potvrđena, odnosno da *nedostatak adekvatne edukacije zaposlenih o informacijskoj sigurnosti značajno doprinosi povećanju rizika od cyber napada i zloupotreba unutar korporativnih okruženja, što implicira da sveobuhvatni pristup informacijskoj sigurnosti mora podjednako uključivati razvoj tehničkih sistema i unapređenje ljudskih kapaciteta*.

Ograničenja ove analize uključuju relativno mali uzorak podataka koji smanjuje statističku snagu rezultata, te kratak vremenski okvir koji može uticati na pouzdanost dugoročnih zaključaka. Preporučujem nastavak edukacije zaposlenih o informacijskoj sigurnosti i prikupljanje dodatnih podataka za dalju analizu.

Četvrti dio: Model programa obuke ne-tehničkih lica zaposlenih u korporativnom okruženju

Sigurnost organizacije je od najveće važnosti i svaki član osoblja organizacije igra vitalnu ulogu u odbrani od cyber prijetnji. Jedan od najboljih načina za zaštitu organizacije je pokretanje inicijative za podizanje svijesti o sigurnosti u cijeloj kompaniji. Ovaj kurs je kompletan osnovni program obuke za podizanje svijesti o sigurnosti koji pokriva širok spektar tema za gotovo sve vrste krajnjeg korisnika i nivoa učenika. Sadržaj je osmišljen tako da omogući organizacijama da pruže sveobuhvatan program obuke koji će im pomoći da zaštite svoja informacijska sredstva od prijetnji.

Ova obuka ne traje više od 2 sata, osmišljena je da bude zanimljiva i zasnovana je na stvarnim scenarijima sa kojima se zaposlenici mogu suočiti. Obuka se treba završiti u jednoj sesiji, da bi se stekao osjećaj cjeline. Ovaj program razvija svijest o značaju informacijske sigurnosti nakon kojeg učesnici obuke osvještavaju značaj svakodnevne izloženosti mogućim prijetnjama sigurnosti.

Naziv obuke	Program obuke ne-tehničkih lica zaposlenih u korporativnom okruženju iz informacijske sigurnosti	
Način izvođenja obuke	Uživo i/ili online	
Broj sati vođene edukacije	Min. 60 min.	Max. 120 min.
Cilj modela		
Program informacijske pismenosti u oblasti informacijske sigurnosti namijenjen je ne-tehničkim uposlenicima u korporativnom okruženju temeljeći se na tri fundamentalna koncepta: informacijsko opismenjavanje, informacijsko ponašanje i informacijska pismenost sa ciljem podizanja nivoa cyber-sigurnosti u svakodnevnom poslovanju.		
Opis programa		
Program informacijske pismenosti u oblasti informacijske sigurnosti ističe važnost svjesnosti o sigurnosti informacija. Organizacije mogu koristiti ovaj model kako bi educirale zaposlenike o sigurnosnim praksama i mjerama zaštite informacija. To uključuje prepoznavanje potencijalnih prijetnji, pravilno upravljanje lozinkama, zaštitu osjetljivih podataka i sprječavanje društvenog inženjeringa.		

Modul 1.

Naziv modula	Uvod u informacijsku sigurnost	
Način izvođenja obuke	Uživo i/ili online	
Broj sati vođene edukacije	Min. 10 min.	Max. 20 min.
Cilj modula		
Upoznavanje sa osnovama informacijske sigurnosti. Cilj je naglasiti značaj i komponente informacijske sigurnosti.		
Sadržaj modula		

Šta je sigurnost informacija?

Sigurnost informacija obuhvata sve načine na koje štitimo našu informacijsku imovinu i mogućnosti od neovlaštenog pristupa, modifikacije ili uništenja i drugih oblika napada. U suštini, to je način na koji branimo naše računarske sisteme i sve naše vrijedne informacije u digitalnom ili štampanom formatu, što je u današnjem informatičkom dobu apsolutno kritično za našu organizaciju.

Lični podaci ili podaci za ličnu identifikaciju (engl. Personally Identifiable Information, PII)

Informacija koja se može identificirati (PII) definiše se kao svaka informacija koja dozvoljava direktan ili indirektan zaključak o identitetu pojedinca. Na primjer, lični broj koji je izdala vlada direktno će identificirati pojedinca i predstavlja identifikacij, ali dovoljno indirektnih informacija za identifikaciju pojedinca (npr. datum rođenja, mjesto rođenja, spol, rasa, itd.) se smatra PII, čak i ako svaka informacija sama po sebi ne identificira pojedinca.

Vrste privatnih podataka

PII, medicinski kartoni i lični finansijski podaci najčešći su tipovi privatnih podataka kojima možete imati pristup. Ako niste sigurni da li su neke od informacija kojima rukujete privatne, pitajte svog pretpostavljenog.

Zaštita privatnih podataka

Digitalni privatni podaci uvijek bi trebali biti zaštićeni lozinkom i šifrirani kada se pohranjuju ili prenose. Šifriranje je proces kodiranja podataka tako da ih može pročitati samo osoba s odgovarajućim ključem. Primjer zaštite dokumenta lozinkom u Wordu: idite na Datoteka > informacije > zaštitite dokument > šifrirajte lozinkom. Upišite lozinku, pritisnite *U redu*, ponovno je upišite i pritisnite *U redu* da biste je potvrdili. Spremite datoteku da biste bili sigurni da će lozinka na snazi. Privatne podatke u štampanom obliku uvijek treba čuvati zaključane.

Klasifikacije podataka

Osiguravanje zaštite podataka je kritičan aspekt sigurnosti informacija i područje u kojem možete napraviti veliku razliku. Najbolje prakse koje trebate primijeniti ovise o klasifikaciji podataka s kojima radite: ***povjerljivi***, ***osjetljivi*** (samo za internu upotrebu) ili ***javni***.

Povjerljivi podaci su podaci čiji bi gubitak, korupcija ili neovlašteno otkrivanje prekršili zakone, propise ili ugovore i eventualno oštetili našu reputaciju. Primjeri uključuju privatne zdravstvene, finansijske ili bilo koje druge podatke koji mogu biti zaštićeni zakonima o privatnosti, poslovnim tajnama, vlasničkim podacima i strateškim planovima.

Svi podaci koji se ne smatraju povjerljivim, ali također nisu odobreni za javnu upotrebu smatraju se osjetljivim. Osjetljivi podaci su podaci čiji bi gubitak doveo do neugodnosti našoj organizaciji, ali ne bi nanio finansijsku štetu ili štetu našoj reputaciji. Primjeri uključuju izvještaje, rasporede ili poruke e-pošte bez povjerljivih informacija.

Javni podaci su podaci koji su odobreni za javnu upotrebu, na primjer, godišnji izvještaji, sadržaj web stranice i saopštenja za javnost.

Dobra praksa za sigurnost podataka

Hakeri i cyber kriminalci ciljaju na krajnje korisnike jer imaju pristup korisničkom imenu,

lozinkama, pravima pristupa i traženim informacijama poput internih povjerljivih ili poslovnih tajni. Oni mogu biti zainteresovani za informacije o vašem bankovnom računu ili kreditnoj kartici, koje mogu iskoristiti za krađu novca ili lažne kupovine u vaše ime. Dobra vijest je da postoji mnogo stvari koje možete učiniti da spriječite sigurnosne incidente i zaštitite svoj identitet.

Najbolji primjeri iz prakse: Lozinka

Prije svega, da biste zaštitili svoj identitet, trebali biste kreirati jaku lozinku i čuvati je u tajnosti. Jaku lozinku čine najmanje 12 znakova u kombinaciji velikih slova, malih slova, brojeva i simbola. Osim toga, vaše lozinke bi trebale biti što je moguće duže, da ne sadrže lične podatke koje je lako pogoditi, kao što su vaš rođendan ili ime vašeg ljubimca.

Može biti veoma teško zapamtiti jake lozinke. Međutim, možete koristiti i duge fraze, kao što su "Danas je 1 od onih dana kad je sve dobro!" Pazite da ne koristite popularnu frazu jer to može olakšati cyber kriminalcu da „hakira“ vašu lozinku.

Što je lozinka duža, to je duže potrebno vrijeme da napadač kompromituje lozinku.

LOZINKA	JAČINA LOZINKE
Sun#an0	Srednje
Danas0bla#nO	Jaka
DanasJe1OdOnihDanaKadJeSveDobro!	Vrlo jaka

Jeste li znali da većina korisnika interneta koristi istu lozinku za online bankarstvo kao i za sve svoje druge račune, poput e-maila i društvenih medija? To znači da ako im je lozinka e-maila ukradena, haker bi mogao ukrasti i njihov bankovni račun.

Kako biste to spriječili:

- Koristite jedinstvenu lozinku na poslu.
- Koristite posebnu, jedinstvenu lozinku za internet bankarstvo.
- Koristite barem još jednu posebnu, jedinstvenu lozinku za druge sisteme.

Dobar način za jednostavno upravljanje višestrukim, jakim lozinkama je korištenje softvera za upravljanje lozinkama (npr. Dashlane, LastPass). Ovi programi čine kreiranje i upravljanje više jakih lozinki lakim i sigurnim, dok vam omogućavaju da zapamtite samo jednu "glavnu lozinku". Kreiranje i pohranjivanje jakih lozinki uz pomoć "upravljača lozinkama" jedan je od najlakših načina da se zaštitimo od toga da se neko prijavi na naše račune i ukrade osjetljive informacije, podatke, novac ili čak naše identitete.

I ne zaboravite da omogućite Multi-faktorsku autentifikaciju (MFA) gdje god je to moguće, posebno za svoju e-poštu, račune društvenih medija i finansijske račune. Multi-faktorska autentifikacija (MFA) nam pruža dodatnu sigurnost potvrđivanjem našeg identiteta prilikom prijavljivanja na naše račune, kao što je unošenje koda poslanog SMS-om na telefon ili koda koji je generisala aplikacija za autentifikaciju.

Modul 2.

Naziv modula	Zaštita informacija	
Način izvođenja obuke	Uživo i/ili online	
Broj sati vođene edukacije	Min. 10 min.	Max. 20 min.
Cilj modula		
Cilj modula je upoznavanje sa prijetnjama informacijskoj sigurnosti.		
Sadržaj modula		

Prijetnje

Kako bismo osigurali svoje podatke i osigurali privatnost, prvo moramo razumjeti prijetnje s kojima se suočavamo. Prijetnja je osoba, okolnost ili događaj koji bi mogao oštetiti našu informacijsku imovinu ili infrastrukturu ili prekršiti naše sigurnosne kontrole.

Može li neko izaći s internom bazom podataka pohranjenom na Micro SD kartici ili USB disku? Može li neko fotografisati osjetljive podatke ili predmete pametnim telefonom?

Nažalost, odgovor je da. Budite oprezni i zaštitite sve osjetljive podatke kojima upravljate sa svojih uređaja.

Zlonamjerni softver (engl. Malware)

Svaki računarski program koji pokušava nanijeti štetu ili ukrasti podatke korisnika zovemo Zlonamjerni softver ili Malware.

Kada pokušava ukrasti informacije ili identitet osobe, zlonamjerni haker često koristi prevaru kako bi vas natjerao da otkrijete osjetljive informacije umjesto da direktno „hakira“ vaš računar. Ova tehnika se naziva **Socijalni inženjering** i često se provodi putem telefona.

Phishing napadi obično uključuju slanje lažnih e-poruka koje izgledaju kao da dolaze od pouzdane institucije ili web stranice kojoj vjerujete, kao što su banke, osiguravajuće kuće ili popularne platforme. U tim e-porukama se može zatražiti "potvrda podataka o računu" i preusmjeriti vas na web stranicu koja izgleda autentično, ali je zapravo namijenjena krađi podataka. Ukoliko unesete svoje podatke na takvoj lažnoj stranici, cyber kriminalci ih mogu iskoristiti za krađu identiteta ili za neovlaštene financijske transakcije sa vašim sredstvima.

Virus je zlonamjerni program koji može "zaraziti" druge programe, izvršiti neku misiju poput brisanja datoteka ili krađe informacija, te se samoumnožavati.

Crv je sličan virusu, ali je program za sebe i ne mora zaraziti drugi program, te se može replicirati preko mreže bez ikakve interakcije korisnika.

Ransomware je vrsta zlonamjernog softvera koji korisniku ograničava pristup sistemu/ima ili datotekama, obično enkripcijom, a zatim zahtijeva otkupninu za vraćanje pristupa. Često se sistemi zaraze ransomwareom putem veze u lažnoj e-pošti. Kada korisnik klikne vezu, ransomware se preuzima na korisnikov računar, pametni telefon ili drugi uređaj. Većina ransomwarea također će se širiti bilo kojom povezanom mrežom, kriptirajući datoteke i čineći ih nečitljivima.

Kako kriptovaluta, poput Bitcoina ili Monera, postaje sve popularnija, tako raste i "rudarenje" kriptovalute, koje omogućuje osobi da zaradi novac otključavanjem valute kroz vrlo intenzivno računanje. Kriptorudarenje zahtijeva značajne računarske resurse, a nažalost, to je dovelo do toga da cyber kriminalci zaraze korisničke računare kodom koji im kolektivno pomaže (Botnet) u njihovim naporima rudarenja. Ova praksa se zove **cryptojacking** i u stalnom je porastu posljednjih godinu dana. Ne samo da to može značajno opteretiti vaš računar i mrežu, već može i oštetiti zaražene uređaje poput pametnih telefona zbog intenzivnog opterećenja baterije.

Najbolji primjeri iz prakse: Izbjegavanje zlonamjernog softvera

Postoje, naravno, mnoge odbrane (antivirusni programi, firewall itd.) koji vas štite od zlonamjernog softvera, ali ovi vas alati ne mogu zaštititi ako nesvjesno sarađujete sa zlonamjernim softverom. S toga **razmislite prije nego kliknete** - *#ThinkB4Click!*

- Izbrišite sumnjive e-mail poruke bez otvaranja, poput onih nepoznatih korisnika s prilozima.
- Ako vam određeni dodaci za web preglednik, kao što su JAVA, Flash ili Acrobat, stvarno nisu potrebni, onemogućite ih kako biste spriječili infekcije zlonamjernim softverom.
- Ako mislite da vaš računar nema ažuriran operativni sistem ili antivirusni ili antispyware program ili je zaraženo zlonamjernim softverom, odmah to prijavite.
- Instalirajte samo odobrene aplikacije kako biste izbjegli slučajno instaliranje zlonamjernog softvera.
- Izbjegavajte klikanje na oglase na web stranicama. Umjesto toga potražite službenu web stranicu dobavljača.

Najbolji primjeri iz prakse: Socijalni inženjering, u kontekstu informacijske sigurnosti

Socijalni inženjeri su stručnjaci za obmanu. Kako biste spriječili njihove taktike:

- Provjerite identitet onih koji traže osjetljive informacije lično ili putem telefona prije nego što ih objavite.
- Nemojte davati informacije o drugim zaposlenicima, udaljenom pristupu mreži,

organizacijskim praksama ili strategijama nijednoj nepoznatoj osobi.

- Ako mislite da vas je kontaktirao socijalni inženjer, prikupite što više informacija, kao što su ime osobe, telefonski broj i ono što traži te odmah prijavite incident.

Najbolji primjeri iz prakse: za sprječavanje internetskih krađa identiteta

- Nikada ne odgovarajte na neželjene e-mail poruke koje traže lične podatke. Ugledna organizacija nikada neće tražiti vašu lozinku ili druge osjetljive informacije putem e-maila.
- Budite sumnjičavi prema e-mailovima koje vam se ne obraćaju imenom ili su pogrešno napisane ili jednostavno ne izgledaju profesionalno.
- Imajte na umu da se lažne phishing poruke također mogu slati putem SMS tekstualnih poruka, faksova, pa čak i automatiziranih glasovnih sistema.
- Imajte na umu da e-poruke za krađu identiteta nisu uvijek osmišljene za krađu vaših podataka. Umjesto toga, njihov cilj može biti instaliranje zlonamjernog softvera na vaš računar. To se može dogoditi jednostavnim klikom na zaraženu vezu, odnosno link ili otvaranjem zaraženog priloga.

Primjer e-mail poruke: *Poštovani korisniče banke: otkrili smo neobičnu aktivnost. Hitno vas molimo da slijedite poveznicu za pregled računa: http://cli.ba/yourbank*

Identificiranje zlonamjernih URL-ova

Drugi način da se obranite od phishing napada je da prepoznate kada se nalazite na lažiranoj web stranici gledajući URL (Uniform Resource Locator). Ključno je zapamtiti da je kraj URL-a, prije prve kose crte ("/"), ono što je važno. Trebali biste zanemariti poddomenu, mapu i naziv stranice.

Zadržite pokazivač miša iznad linka u e-mailu, SMS-u i trenutnim porukama te na web-mjestima da biste provjerili stvarni URL, čak i ako veza dolazi iz pouzdanog izvora.

Da biste to učinili na većini mobilnih uređaja, jednostavno držite prst na linku (dugi pritisak) koja će iskočiti i otkriti željenu adresu.

Ipak, imajte na umu da je uvijek sigurnije doći do svoje banke ili drugih web stranica upisivanjem adrese web stranice, umjesto klikanjem na link.

Krađa identiteta

Phisheri obično šalju svoje lažne poruke na bilo koju e-mail adresu koju mogu pronaći. Međutim, ti napadi su puno uspješniji kada ciljaju odabranu skupinu ili pojedince s vrlo prilagođenom porukom. Ova tehnika poznata je kao spear phishing i mnogo je teže prepoznati te poruke jer mogu izgledati izuzetno autentično.

Na primjer, napadač bi mogao izvršiti online pretragu, brzo sastavljajući popis imena, e-mail adresa i naziva poslova. Napadač tada može poslati e-poruku koja izgleda kao da dolazi od kolege, raspravljajući o relevantnoj temi. Zbog toga je mnogo teže odoljeti otvaranju zaraženog priloga ili klikanju na zaraženu poveznicu.

Spriječite Spear Phishing napade

Ako sumnjiva e-poruka stigne od nekoga kome vjerujete, nazovite tu osobu ili joj pošaljite e-poruku odvojeno i pitajte prije nego što otvorite e-poruku, kliknete bilo koju poveznicu ili otvorite bilo koji prilog.

Imajte na umu da se sve što ste objavili na društvenim mrežama može koristiti u e-porukama za krađu identiteta kako bi izgledale legitimne.

Kompromitovanje poslovne e-pošte (engl. Business Email Compromise, BEC)

BEC prevara predstavlja posebno smišljenu prevaru putem e-maila. Ne sadrži zlonamjernu vezu ili prilog koji bi mogao pokrenuti antispam ili antivirusni softver da ga blokira. Obično uključuje cyber kriminalca koji se predstavlja kao izvršni direktor ili menadžer i šalje e-mail zaposlenicima tražeći prijenos sredstava ili dostavu povjerljivih podataka. Često se ova komunikacija šalje putem

"lažnih" adresa koje nalikuju stvarnoj adresi e-maila osobe za koju se predstavljaju. Mogu čak i preoteti stvarni račun e-maila izvršnog direktora ili menadžera, što otežava procjenu radi li se o legitimnom zahtjevu ili potencijalnoj prijevari.

Da biste se obranili od BEC-a, slijedite ove najbolje prakse:

- Nazovite izvršnog direktora ili menadžera da provjerite je li zahtjev legitiman.
- Još jednom provjerite adresu e-maila pošiljatelja kako biste bili sigurni da nije lažirana.
- Izbjegavajte odgovaranje pošiljatelju, pogotovo ako je to primljeno sa lične e-mail adrese. Umjesto toga, proslijedite svoj odgovor na stvarnu poslovnu e-mail adresu direktora ili menadžera.
- Budite oprezni s promjenama u načinu komunikacije, posebno ako se od vas traži da čuvate tajnost ili ako je ton hitan.

Ako ipak postanete žrtva BEC-a, vrlo je važno brzo obavijestiti svog nadređenog. Ako su sredstva prenesena, možda postoji mogućnost zamrzavanja procesa i povrata sredstava.

Online prijevare

Krađa identiteta jedan je od popularnih načina na koje cyber kriminalci kradu vaš identitet. No, nažalost, to nije jedini način na koji vas mogu pokušati opljačkati.

Račune na društvenim mrežama može oteti ili iskoristiti cyber kriminalac koji vas može pokušati prevariti lažnim molbama za pomoć ili donacijama ili vam poslati zaražene poveznice s člancima o "lažnim vijestima".

Također će "zatrovati" rezultate pretraživanja zaraženim web stranicama na popularne teme ili značajne medijske događaje, poput smrti slavne osobe, prirodne katastrofe ili izbora. Kada stignu velike vijesti, držite se poznatih stranica sa vijestima kako biste izbjegli ove prijevare.

Modul 3.

Naziv modula	Uloga i obaveze uposlenika	
Način izvođenja obuke	Uživo i/ili online	
Broj sati vođene edukacije	Min. 10 min.	Max. 20 min.
Cilj modula		
Cilj modula je ukazati na značaj uloge i obaveza uposlenika u kontekstu informacijske sigurnosti.		
Sadržaj modula		

Vaše odgovornosti

Kao zaposlenik, od vas se očekuje da koristite informacijske resurse na odgovoran i zakonit način u svrhe povezane s radom, pokazujući poštovanje sigurnosti, etike i politike privatnosti, prava intelektualnog vlasništva i prava svakog pojedinca na slobodu od zastrašivanja i uznemiravanja.

Pristup internetu je omogućen kako bi vam pomogao da radite efikasnije. Ipak, upotreba interneta je ograničena za ličnu svrhu i NE smije:

- Ometati radne obaveze.
- Uključivati opscene, seksualno eksplicitne, prijeteće ili nezakonite aktivnosti.
- Kršiti bilo koju politiku ili zakone.
- Trošiti previše vremena ili resursa.

E-mail i trenutne poruke (IM) ne bi trebalo da se koriste za sledeće:

- Pretjeranu ličnu komunikaciju.
- Prenos ili distibuciju neprikladnog sadržaja.
- Lične poslove

Društveni mediji

Ako pristupate stranicama društvenih medija, slijedite ove najbolje prakse kako biste povećali sigurnost:

- Nemojte objavljivati lične podatke koje bi kradljivci identiteta mogli koristiti, kao što su vaš broj telefona, rođendan itd.
- Dozvolite samo "prijateljima" da vide vaš profil ili objave ili da vam šalju poruke.
- Ne prihvatajte pozive za prijatelje od onih koje ne poznajete.
- Uključite dostupne sigurnosne funkcije, kao što su SSL enkripcija i upozorenja o prijavi.

Zabranjene aktivnosti uključuju:

- Pravljenje, instaliranje ili dijeljenje ilegalnih ili piratskih kopija softvera.
- Pokušaj pristupa sigurnim podacima ili resursima bez autorizacije.

Očistite svoj stol

- Dok ste daleko od svog stola, provjerite jesu li svi papiri, prenosivi mediji i drugi predmeti koji sadrže osjetljive informacije uklonjeni sa vašeg stola i zaključani.
- Odjavite se ili zaključajte svoj računar kako biste osigurali da mu niko ne može pristupiti dok ste odsutni.
- Čuvar ekrana zaštićen lozinkom može se koristiti za automatsko zaključavanje vašeg računara nakon određenog perioda neaktivnosti.

Zajednička područja za sastanke

Zajedničke prostore za sastanke također treba držati bez osjetljivih informacija. Kada napustite prostor za sastanke, obavezno obrišite sve table, ponesite sve dokumente sa sobom i pazite što bacate u smeće.

Skladištenje podataka koje pružaju javni pružaoci usluga u oblaku

Pohranjivanje osjetljivih podataka s radnog mjesta na javnim servisima za pohranu u oblaku (npr. iCloud ili Google Drive) predstavlja ozbiljnu sigurnosnu prijetnju jer informacije stavlja izvan kontrole naše organizacije. A ako je usluga pohrane u oblaku hakirana, što nije neuobičajeno, osjetljive informacije mogle bi biti izložene. To bi moglo prekršiti politiku, ugovorne obveze i zakon. Za optimalnu sigurnost koristite samo odobrene sigurne usluge pohrane u oblaku.

Zaštita mobilnih podataka i uređaja

Svi mobilni uređaji za prenos podataka

- Postavite poslovne informacije sa radnog mjesta na mobilni uređaj samo ako je to apsolutno neophodno i uređaj ih može zaštititi.
- Uklonite poslovne informacije kada više nisu potrebne.
- Ako morate pohraniti poslovne informacije na mobilnom uređaju, šifrirajte podatke.
- Koristite jaku lozinku na svim mobilnim uređajima.

Dokumenti koji postoje u obliku materijala, poput otisnutih papira, fascikli ili mapa.

Pravilno odložite sve osjetljive ili povjerljive informacije u štampanom formatu koje uklonite sa radnog mjesta na osnovu naše sigurnosne politike.

Pametni telefoni i tableti

- Provjerite je li vaš mobilni operativni sistem ažuriran s najnovijim ažuriranjima softvera.
- Odmah prijavite izgubljeni uređaj koji sadrži ili može pristupiti informacijama s radnog mjesta. Neke informacije na radnom mjestu, kao što je e-mail, mogu se onemogućiti, a podaci na uređaju također se mogu obrisati na daljinu.
- Koristite samo provjerene, regulisane trgovine aplikacija.
- Nikada nemojte raditi "*jail-break*" iPhone ili "*root*" Android telefona, jer to isključuje sigurnosne postavke. Ukoliko niste upoznati sa ovim terminima, onda ignorišite preporuku.

Najbolje prakse: Rad na javnim mjestima

Rad na javnim mjestima može vam pomoći da budete efikasniji, ali i izlaže vas dodatnim rizicima. Pridržavajte se ovih najboljih praksi kada radite na javnim mjestima:

- Nikada ne razgovarajte o povjerljivim informacijama na javnim mjestima. Nikad ne znate ko bi mogao da prisluškuje.

- Budite oprezni kada prikazujete poslovne informacije na ekranu na javnim mjestima. Neko bi to mogao čitati preko vašeg ramena.
- Koristite samo šifrirane Wi-Fi internetske veze. Imajte na umu da će cyber kriminalci često oponašati legitimnu bežičnu mrežu, poput hotela ili aerodroma s onom koja izgleda vrlo slično. Provjerite je li naziv tačan ako trebate pristupiti nekoj od ovih mreža.
- Nikada ne ostavljajte mobilne uređaje za prijenos podataka na vidiku gdje bi mogli namamiti lopove.

Najbolji primjeri iz prakse: Pristup sa udaljene lokacije

Pristup sa udaljene lokacije se odnosi na mogućnost pristupa računarskim resursima ili podacima izvan fizičke lokacije gdje su ti resursi ili podaci smješteni. Ovo je posebno važno u današnje vrijeme kada sve više ljudi radi izvan tradicionalnih kancelarijskih prostora i koristi udaljeni pristup kako bi obavljali poslovne zadatke. Rad na daljinu, na primjer od kuće zahtijeva posebne mjere opreza. Imajte na umu da iste sigurnosne politike i standardi vrijede za rad na daljinu kao i na radnom mjestu.

„Za ponijeti“

- Osiguravanje naših informacijskih resursa je od vitalnog značaja za naš uspjeh i ne može se postići bez vaše pomoći.
- Računamo na vas da ćete najbolje prakse navedene u ovom kursu odmah koristiti kako biste osigurali naše informacije i osigurali privatnost.
- Također zavisimo od vas da prijavite sve sigurnosne incidente za koje ste svjesni kako bismo mogli poboljšati ukupnu sigurnost, performanse i pouzdanost mreže.
- Incident sigurnosti informacija je kršenje ili neposredna prijetnja kršenjem sigurnosnih politika, politika prihvatljivog korištenja ili standardnih sigurnosnih praksi. Molimo vas da odmah prijavite sve sigurnosne incidente.

Modul 4.

Naziv modula	KVIZ – provjera znanja

Način izvođenja obuke	Uživo i/ili online	
Broj sati vođene edukacije	Min. 10 min.	Max. 20 min.
Cilj modula		
Provjera stečenih zanja		
Opis modula		

Pitanje 1 od 10

Što je od sljedećeg primjer PII?

1. Vaš broj bankovnog računa.
2. Uredska financijska evidencija.
3. Strategije, planovi i interni procesi.
4. Šifrirane datoteke.

Tačno pod 1. Vaš broj bankovnog računa se može koristiti za vašu ličnu identifikaciju.

Pitanje 2 od 10

Šta mislite s kim biste trebali podijeliti svoju lozinku?

1. Samo sa onima kojima vjerujete
2. Nikom

Tačno pod 2: Ne biste trebali dijeliti svoju lozinku ni s kim.

Pitanje 3 od 10

Koji je najbolji odgovor o tome ko bi trebao biti odgovoran za cyber sigurnost u poslovanju?

1. Vlasnici preduzeća. Oni vode posao, stoga bi trebali poznavati osnove kibernetičke sigurnosti i primjenjivati ih kako bi smanjili rizik od cyber napada.
2. IT stručnjaci, jer su oni u najboljoj poziciji da znaju i promovišu cyber sigurnost u okviru poslovanja.

3. Menadžeri, jer su odgovorni za osiguravanje da članovi osoblja slijede ispravne prakse u cyber sigurnosti.
4. Svi zaposlenici trebaju znati osnove cyber sigurnosti kako bi smanjili rizik od cyber napada.

Tačno pod 4: Svi zaposlenici trebaju biti svjesni osnovnih principa cyber sigurnosti kako bi pomogli u zaštiti organizacijskih resursa i podataka.

Pitanje 4 od 10

Kada pretražujete na mreži, pojavljuje se novi prozor u kojem se navodi da je virus pronađen na vašem računaru. U prozoru se nalazi dugme za klik na ponudu da biste riješili problem.

Vaš najbolji način djelovanja je da:

1. Kliknite na dugme da uklonite virus.
2. Postavite kursor preko dugmeta i provjerite adresu web stranice (URL) veze. Ako adresa izgleda legitimno, kliknite na nju. Ako izgleda kao veza za prevaru, zatvorite prozor.
3. Zatvorite i originalni prozor pretraživača i novi "skočni" prozor. Ne vraćajte se na tu stranicu.
4. Pritisnite dugme za povratak i pogledajte da li nestaje.

Tačno pod 3: Ovo je preporučeni postupak jer takvi prozori često predstavljaju pokušaj prevare korisnika. Zatvaranje prozora i ne vraćanje na tu stranicu najsigurniji je način da se zaštiti vaš računar od potencijalnih prijetnji.

Pitanje 5 od 10

Povjerljivi podaci moraju biti šifrirani dok se pohranjuju ili prenose i uvijek zaštićeni lozinkom.

1. Da, moraju
2. Ne, ne moraju

Tačno pod 1: Povjerljivi podaci moraju biti zaštićeni ovim naprednim mjerama sigurnosti.

Pitanje 6 od 10

Preuzimate aplikaciju na svoj tablet koja vam daje pristup mnogim besplatnim aplikacijama. Trebate li preuzeti i instalirati ove aplikacije?

1. Da
2. Ne

Točno pod 2: Neslužbene trgovine aplikacija koje nude besplatne verzije popularnih aplikacija po cijeni obično su pune "prepakiranih aplikacija" koje su verzije aplikacija koje su hakirane da sadrže zlonamjerni softver. Trebali biste koristiti samo provjerene trgovine aplikacijama, kao što su Google Play ili Appleov App Store.

Pitanje 7 od 10

Koja vrsta prijetnje pokušava ucijeniti korisnika da izvrši plaćanje hakeru?

1. Malware
2. Ransomware
3. Kompromitovanje poslovne e-pošte (BEC)

Točno pod 2: Ransomware pokušava ucijeniti korisnika da izvrši plaćanje hakeru.

Pitanje 8 od 10

Koja tehnika društvenog inženjeringa koristi e-mail da pokuša prevariti korisnike da daju osobne podatke?

1. Cryptojacking
2. Phishing
3. Firewall

Točno pod 2: Phishing koristi e-mail kako bi pokušao prevariti korisnike da daju osobne podatke.

Pitanje 9 od 10

Koja je od ovih najjača lozinka?

1. CS3sTb1t^s1z#
2. CS3sTb1Zapamti
3. CSTbZapamtiLozinku

Tačno pod 1: CS3sTb1t^s1z# je najjača lozinka. Sadrži velika i mala slova, brojeve i simbole.

Pitanje 10 od 10

Šta je Surfanje preko ramena (Shoulder surfing)?

1. Surfanje preko ramena je čin sticanja informacija direktnim posmatranjem nekoga
2. Surfanje preko ramena je čin korištenja softvera bez zakrpa za pristup mreži
3. Surfanje preko ramena je čin korištenja zlonamjernog USB uređaja za dobivanje informacija

Tačno pod 1: Surfanje preko ramena je čin sticanja informacija direktnim posmatranjem nekoga.

ZAKLJUČAK

Uz sve veći porast prijetnji u digitalnom okruženju, važno je razvijati i provoditi strategije za unapređenje informacijske sigurnosti u organizacijama.

Sveobuhvatan pristup informacijskoj pismenosti prema modelu Christine Bruce "The Seven Faces of Information Literacy" omogućava dublje razumijevanje informacijskih potreba i sposobnosti pojedinaca u različitim kontekstima. Integracija sedam lica informacijske pismenosti u obrazovne programe, organizacijske procese i društvene prakse ključna je za razvoj informacijski pismenih građana i uspješnih organizacija u savremenom digitalnom dobu. Informacijska pismenost i cjeloživotno učenje su ključni za uspjeh u savremenom informacijskom dobu. Kako ističe Vajzović (2021) „*Informacijska pismenost, kao kompetencija cjeloživotnog učenja, predstavlja sposobnost da se prepozna informacijska potreba, pronađe relevantna i pouzdana informacija, te potom evaluira, upravlja, sintetizira odnosno efikasno i etično koristi da bi se odgovorilo na informacijsku potrebu. Sve to zahtijeva poznavanje alata korištenih u procesu zbog čega su neophodni informacijski izvori istraživački alati da bise pronašle kvalitetne informacije što istovremeno uključuje vještine njihovog kritičkog tumačenja i vrednovanja, kao i evaluacije cjelokupnog istraživačkog procesa. Kritičko mišljenje podrazumijeva analiziranje, komparaciju, usporedbe, generalizacije, ispitivanje, eksperimentiranje, kreiranje, konceptualizaciju, sintetiziranje i evaluaciju informacija da bi se riješio problem, planirao smjer djelovanja, odnosno efikasno obavio istraživački zadatak. Informacijska pismenost je kao takva pretpostavka participacije u istraživačkim zajednicama, preduvjet stvaranja informacijski pismenog građanstva i djelatnog civilnog društva. Riječ je o preduvjetu za donošenje informiranih odluka, stvaranju novog znanja, osobni razvoj...“*[76]

Povezivanjem ovih koncepata, pojedinci i organizacije mogu bolje upravljati informacijama, prilagoditi se promjenama i suočiti se s izazovima u stalno mijenjajućem okruženju. Kroz kontinuirano obrazovanje i razvijanje informacijske pismenosti, moguće je stvoriti temelje za inovativne, sigurne i učinkovite prakse koje će osigurati dugoročni uspjeh.

[76] Vajzović, E., Hibert, M., Turčilo, L., Vučetić, V., & Silajdžić, L. (2021). Medijska i informacijska pismenost: dizajn učenja za digitalno doba (Vol. 2, p. 327). Fakultet političkih nauka Univerziteta. https://fpn.unsa.ba/b/wp-content/uploads/2021/04/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-DIZAJN-UCENJA-ZA-DIGITALNO-DOBA_e-izdanje-1.pdf.

Kontinuiranim usavršavanjem i primjenom informacijskih vještina u svakodnevnom životu, pojedinci postaju sposobni kritički razmišljati, efikasno koristiti tehnologiju, surađivati s drugima i donositi informirane odluke. Istovremeno, organizacije koje promovišu informacijsku pismenost među svojim zaposlenicima stvaraju produktivno i inovativno radno okruženje te pridonose svojoj konkurentnosti i uspjehu na tržištu. Zato je važno je nastaviti podržavati razvoj informacijske pismenosti na svim razinama društva kako bismo ostvarili pozitivne promjene i napredak u digitalnoj eri.

Na temelju provedenog istraživanja u okviru magistarskog rada, potvrđena je hipoteza da nedostatak adekvatne edukacije zaposlenih o informacijskoj sigurnosti značajno doprinosi povećanju rizika od cyber napada i zloupotreba unutar korporativnih okruženja, što implicira da sveobuhvatni pristup informacijskoj sigurnosti mora podjednako uključivati razvoj tehničkih sistema i unapređenje ljudskih kapaciteta. Ovo istraživanje je uspješno potvrdilo da postoji pozitivna veza između nivoa informacijske pismenosti zaposlenika i njihove sposobnosti doprinosa informacijskoj sigurnosti u organizacijama. Zaposlenici koji su bolje informacijski pismeni pokazali su veću svijest o sigurnosnim prijetnjama, bolju sposobnost prepoznavanja phishing napada i pravilno reagiranje u slučaju sigurnosnih incidenata.

Ovi rezultati su od izuzetne važnosti za organizacije koje žele da budu otpornije na sigurnosne prijetnje i da efikasnije odgovore na sve izazove u digitalnom okruženju. Uvođenje programa obuke i edukacije o informacijskoj sigurnosti za zaposlenike, posebno fokusiranih na razvoj informacijske pismenosti, može značajno doprinijeti smanjenju rizika od sigurnosnih incidenata i poboljšanju cjelokupne informacijske sigurnosti u organizacijama.

Ovaj rad naglašava važnost edukacije i treninga za sve zaposlenike kako bi se podigla razina svijesti o sigurnosnim prijetnjama i smanjio rizik od uspješnih napada. Implementacija redovnih simulacija phishing napada, zajedno s obukama i edukativnim inicijativama, može značajno doprinijeti jačanju informacijske sigurnosti unutar organizacija i smanjenju sigurnosnih propusta.

U konačnici, ovaj rad pruža korisne smjernice i preporuke za organizacije kako bi se osiguralo unapređenje informacijske sigurnosti putem podizanja svijesti, edukacije zaposlenika i implementacije najboljih praksi u ovoj važnoj oblasti.

Literatura

1. ACRL Framework for Information Literacy Advisory Board. (2017). The ACRL Framework for Information Literacy Toolkit [Website]. Retrieved from https://acrl.libguides.com/framework/toolkit
2. Alsmadi, I., et al. (2018). Practical information security: A competency-based education course (1st ed.). Springer International Publishing.
3. Andress, J. (2011). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (Online-ausg.). Syngress. Accessed May 6, 2024. http://site.ebrary.com/id/10477252
4. Bundy, A. (Ed.). (2004). Australian and New Zealand Information Literacy Framework: Principles, Standards and Practice (2nd ed.). Adelaide: Australian and New Zealand Institute for Information Literacy. Pristupljeno12.9.2023. https://www.library.qut.edu.au/about/policies/information-literacy-amework/documents/anz-info-lit-policy.pdf
5. Beridan, I. (2007). Politika i sigurnost - sadržaj i obilježja pojmova. Fakultet političkih nauka – Godišnjak 2007 (str. 99-121).
6. Bruce, C. (1997). The seven faces of information literacy. Auslib Press.
7. Bruce, Christine Susan (1999) Workplace experiences of information literacy. International Journal of Information Management, 19 (1). 33 - 47.
8. Cisco Meraki. (n.d.). Retrieved from https://meraki.cisco.com/ Pristupljeno 12.9.2023.
9. Cisco. (n.d.). Cisco Secure Email Advanced Email Protection Data Sheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html, Pristupljeno 12.9.2023.
10. Cisco Systems, Inc. (2017) Cryptojacking: Hijacking your computer resources. Retrived from https://blogs.cisco.com/security/cryptojacking-hijacking-your-computer-resources, Pristupljeno 12.5.2024.

11. Christmann, E. P., Badgett, J. L. (2009). Interpreting Assessment Data: Statistical Techniques You Can Use. Washington, DC, NSTA Press.

12. Claycomb, W. R., & Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. In 2012 IEEE 36th Annual Computer Software and Applications Conference (pp. 387-394). Izmir, Turkey. doi:10.1109/COMPSAC.2012.113

13. Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. Computer Security, 28(3-4), 189-198.

14. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Članak 32 Sigurnost obrade. Official Journal of the European Union, L 119, (2016, May 4). Retrieved from https://gdprinfo.eu/hr/hr-article-32

15. Fruhlinger, J. (2020, February 10). The CIA triad: Definition, components and examples. CSO Online. Pristupljeno 11.06.2023. https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

16. HCL Software. (n.d.). BigFix. Pristupljeno 12.9.2023. Retrieved from https://www.hcl-software.com/bigfix

17. Leksikografski zavod Miroslav Krleža. (2013-2024). *Hrvatska enciklopedija, mrežno izdanje*. Retrieved April 25, 2024, from https://www.enciklopedija.hr/clanak/haker

18. Leksikografski zavod Miroslav Krleža. (2013-2023). Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. <https://www.enciklopedija.hr/clanak/korporacija>.

19. Leksikografski zavod Miroslav Krleža. (2013-2023). Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. <https://www.enciklopedija.hr/clanak/organizacija>.

20. Leksikografski zavod Miroslav Krleža. (2013-2023). Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2023. Pristupljeno 10.5.2023. https://www.enciklopedija.hr/clanak/edukacija.

21. Hylender, D. (2022). Verizon 2022 data breach investigations report. Verizon. Pristupljeno

10.5.2023 Retrieved from https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report

22. IBM Security. (2023). Cost of a data breach report 2023. Pristupljeno 10.5.2023. Retrieved from https://www.ibm.com/downloads/cas/E3G5JMBP

23. International Organization for Standardization (2023). ISO/IEC 27032:2023 - Cybersecurity - Guidelines for Internet security. Retrieved from https://www.iso.org/standard/76070.html

24. International Organization for Standardization. (2018). ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

25. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems—Requirements. Pristupljeno 10.06.2023. Retrieved from https://www.iso.org/standard/27001

26. International Organization for Standardization. (n.d.). ISO/IEC 27000 family: Information security management. Pristupljeno 10.06.2023. Retrieved from https://www.iso.org/standard/iso-iec-27000-family

27. Izoologic. (n.d.). Retrieved from https://izoologic.com/ Pristupljeno 12.9.2023.

28. KnowBe4. (n.d.). Retrieved from https://www.knowbe4.com/ Pristupljeno 12.9.2023.

29. KnowBe4. (2023). 2023 Phishing By Industry Benchmarking [Report]. Pristupljeno 17.03.2024. https://info.knowbe4.com/en-us/phishing-by-industry-benchmarking-report

30. Merkow, M. S., & Breithaupt, J. (2014). Information security: Principles and practices (2nd ed.). Pearson IT Certification.

31. Möller, D. P. F. (2023). Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices. Springer Nature Switzerland.

32. Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209.

33. National Institute of Standards and Technology (2009). NIST IR 7609, Cryptographic key

management workshop summary June 8-9, 2009. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7609.pdf Pristupljeno 01.10.2023.

34. National Institute of Standards and Technology. (n.d.). NIST SP 1800-10B under information security from FIPS 199, 44 U.S.C., Sec. 3542 of NIST. Američki Nacionalni Institut za Standarde i Tehnologiju.

35. National Institute of Standards and Technology. (n.d.). Malware. Glossary of Key Information Security Terms. Retrieved from https://csrc.nist.gov/glossary/term/malware Pristupljeno 12.3.2024.

36. National Institute of Standards and Technology. (n.d.). Social engineering. Glossary of Key Information Security Terms. Retrieved from https://csrc.nist.gov/glossary/term/social_engineering Pristupljeno 12.3.2024.

37. OSCE. (2019). Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini. Sarajevo. Retrieved from https://www.osce.org/files/f/documents/4/8/438386.pdf Pristupljeno 12.11.2022.

38. Salahdine, F.; Kaabouch, N. (2019) Social Engineering Attacks: A Survey. Future Internet 2019, 11, 89 Pristupljeno: 12.03.2024. https://doi.org/10.3390/fi11040089

39. SCONUL Working Group on Information Literacy. (April 2011). The SCONUL Seven Pillars of Information Literacy Core Model for Higher Education. Retrieved from https://access.sconul.ac.uk/sites/default/files/documents/coremodel.pdf Pistupljeno 01.04.2023.

40. SentinelOne. (n.d.). Retrieved from https://www.sentinelone.com/ Pristupljeno 12.3.2024.

41. Shinde, A. (2021). Introduction to cyber security: Guide to the world of cyber security. Notion Press.

42. Steinerova, J., & Šušol, J. (2005). Library users in human information behaviour. Online Information Review, 29(2), 139-156.

43. United States Senate, Committee on Governmental Affairs. (2000). Cyber attack: Is the government safe?: Hearing before the Committee on Governmental Affairs, United States

Senate, One Hundred Sixth Congress, Second Session, March 2, 2000. U.S. Government Printing Office.

44. Vajzović, E., Hibert, M., Turčilo, L., Vučetić, V., & Silajdžić, L. (2021). Medijska i informacijska pismenost: dizajn učenja za digitalno doba (Vol. 2, p. 327). Fakultet političkih nauka Univerziteta. Pristupljeno 10.5.2023. https://fpn.unsa.ba/b/wp-content/uploads/2021/04/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-DIZAJN-UCENJA-ZA-DIGITALNO-DOBA_e-izdanje-1.pdf.

45. Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti = Media and information literacy in cyber security system. Kriminalističke Teme, (5), 529-543. Pristupljeno 10.5.2023 http://krimteme.fkn.unsa.ba/index.php/kt/article/view/240

46. von Solms, S.H. (2010). The 5 Waves of Information Security – From Kristian Beckman to the Present. In: Rannenberg, K., Varadharajan, V., Weber, C. (eds) Security and Privacy – Silver Linings in the Cloud. SEC 2010. IFIP Advances in Information and Communication Technology, vol 330. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15257-3_1

47. von Solms R., van Niekerk J. (2013) From information security to cyber security, Computers & Security, Volume 38, Pages 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

48. Webber, S., & Johnston, B. (2000). Conceptions of information literacy: New perspectives and implications. Journal of Information Science, 26(6), 381-397.

49. Zscaler. (n.d.). Retrieved from https://www.zscaler.com/ Pristupljeno 12.3.2024.

50. Zurkowski, P. G. (1974). The information service environment: Relationships and priorities. National Commission on Libraries and Information Science.

Naziv odsjeka i/ili katedre:	SIMS
Predmet:	Magistarski rad

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime:	Mersudin Šuman
Naslov rada:	INFORMACIJSKA PISMENOST U SEKTORU INFORMACIJSKE SIGURNOSTI: PRIJEDLOG MODELA U STRATEGIJI KORPORATIVNOG PRISTUPA
Vrsta rada:	Završni magistarski rad
Broj stranica:	80

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum **Potpis**

_____ _____