Znanje i osviještenost opće populacije o kibernetičkoj sigurnosti

Končarević, Marta

Master's thesis / Diplomski rad

2023

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:430380

Sveučilište u Zagrebu
Ekonomski fakultet – Zagreb
Integrirani preddiplomski i diplomski sveučilišni studij
Poslovna ekonomija – smjer Menadžerska informatika

ZNANJE I OSVIJEŠTENOST OPĆE POPULACIJE O KIBERNETIČKOJ SIGURNOSTI

DIPLOMSKI RAD

Marta Končarević

Zagreb, lipanj 2023.

Sveučilište u Zagrebu

Sveučilište u Zagrebu
Ekonomski fakultet – Zagreb
Integrirani preddiplomski i diplomski sveučilišni studij
Poslovna ekonomija – smjer Menadžerska informatika

ZNANJE I OSVIJEŠTENOST OPĆE POPULACIJE O KIBERNETIČKOJ SIGURNOSTI

CYBERSECURITY AWARENESS AND PUBLIC KNOWLEDGE

DIPLOMSKI RAD

Student: Marta Končarević
JMBAG: 0083219660
Mentor: prof. dr. sc. Mario Spremić

Zagreb, lipanj 2023.

SAŽETAK

Brzi tehnološki napredak i intenzivnija primjena informacijskih i digitalnih tehnologija povećali su ranjivost na kibernetičke napade, čime je samo pitanje kibernetičke sigurnosti postalo sve važnije. Fokus diplomskog rada stavljen je na sam koncept kibernetičke sigurnosti, kibernetičke prijetnje i rizike s kojima se pojedinci suočavaju, te se stavlja naglasak na proaktivne i reaktivne mjere, kao i na važnost adekvatnog znanja i kontinuirano usavršavanje pojedinaca kao ključni elementi prilagodbe koje donosi moderno doba. Cilj ovog diplomskog rada je prikazati znanje i osviještenost opće populacije o kibernetičkoj sigurnosti. Anketnim upitnikom prikupljati će se kvalitetne informacije i analizirati rezultati, a na temelju dobivenih informacija, sastavljati će se preporuke i smjernice za buduće informiranje i podizanje svijesti o kibernetičkoj sigurnosti.

Ključne riječi: kibernetička sigurnost, kibernetički rizici, kibernetičke prijetnje, kibernetički napad proaktivne mjere, reaktivne mjere

SUMMARY

Rapid technological progress and the intensive use of information and digital technologies have increased vulnerability to cyberattacks, making the issue of cyber security increasingly important. This thesis focuses on the fundamental concept of cyber security, the cyber threats and risks individuals face, and emphasizes the significance of proactive and reactive measures, as well as the importance of adequate knowledge and continuous training for individuals to adapt to the challenges of the modern era. The objective of this thesis is to assess the knowledge and awareness of the general population regarding cyber security. Through a questionnaire, high-quality data will be collected then analyzed,. Based on the information obtained, recommendations and guidelines for future initiatives aimed at enhancing information and awareness about cyber security.

Keywords: cyber security, cyber risks, cyber threats, cyber attack, proactive measures, reactive measures

IZJAVA O AKADEMSKOJ ČESTITOSTI

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

_____

(vlastoručni potpis studenta)

_____

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.
I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.
I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

_____

(personal signature of the student)

_____

(place and date)

Sadržaj

1 UVOD

Brzi tehnološki napredak i prijelaz na digitalnu domenu doveo je svijet do novih modernih opasnosti. Unatoč tome što nam je svakodnevna uporaba tehnologije omogućila veću produktivnost i učinkovitost, olakšala brojne repetitivne poslove te pridonijela razvoju samog društva, svojim razvojem donosi i veliku odgovornost.

U današnje vrijeme sve veći broj stanovnika preferira obavljanje osobnih poslova online kao što je kupovina putem interneta ili plaćanje računa putem modernih aplikacija. Navedene, ali i mnoge druge radnje dovode do osobnog izlaganja potencijalnom hakerskom napadu.

Sve veću popularnost dobiva i rad na daljinu. Rad na daljinu ne samo da je proširio potencijalnu površinu napada, već ju je i premjestio izvan konvencionalnih perimetarskih obrana, poput vatrozida i sustava za otkrivanje upada, koje su organizacije tradicionalno gradile za sprječavanje napada *ransomwarea*, povreda podataka i drugih vrsta kibernetičkog kriminala. Dovoljna je jedna pogreška i klik na lažnu elektroničku adresu da se kompromitira sigurnost poslovanja, te se javlja pitanje: Koliko opća populacija uopće poznaje i razumije važnost kibernetičke sigurnosti?

1.1 Predmet i cilj rada

Predmet diplomskog rada je objasniti pojam kibernetičke sigurnosti, zašto nam je ona potrebna, koje su to sve prijetnje i rizici s kojima se možemo suočiti na dnevnoj bazi, te objasniti vrste kibernetičkog kriminala. Također, iznimno je važno objasniti koje su to proaktivne, a koje reaktivne mjere koje se mogu poduzeti s obzirom da pitanje više nije – hoćete li ćete biti hakirani, već kada i kojim intenzitetom.[1] Cilj istraživanja je ustanoviti kakvo je znanje i osviještenosti opće populacije o kibernetičkoj sigurnosti, sposobnost ispitanika prilikom prepoznavanja kibernetičkih napada, te analiza dobivenih rezultata. Istraživanje će se provoditi anketnim upitnikom.

1.2 Izvori podataka i metode prikupljanja

[1] Jalali, M.S.(2018.), Journal of Strategic Information Systems, Volume 28, Issue 1, Pages 66-82

Prilikom izrade diplomskog rada koristit će se primarni i sekundarni izvori podataka. Kao primarni izvor koristit će se kvantitativna metoda ispitivanja – anketa. Anketni upitnik bit će sastavljen od pitanja zatvorenog tipa i u potpunosti će se provoditi online putem. Hipoteze i istraživačka pitanja bit će postavljena prije provođenja samog ispitivanja, a kasnijom analizom rezultata utvrdit će se jesu li postavljene hipoteze potvrđene ili opovrgnute. Uz primarno istraživanje, dodatno će se koristiti i sekundarni izvori informacija poput znanstvenih i stručnih knjiga, internet članaka i stranica te znanstvenih publikacije i radova radi obrade teorijskog dijela diplomskog rada.

1.3 Sadržaj i struktura rada

Strukturu rada čini sedam poglavlja. U početnom dijelu, uvodu, apstraktno se opisuje tema, kao i predmet i cilj istraživanja. Pojam kibernetičke sigurnosti, njezin značaj, zatim prijetnje i rizici te metode zaštite opisane su u drugom poglavlju rada uz korištenje brojnih sekundarnih izvora podataka. Nakon teoretskog dijela diplomskog rada, slijedi provođenje anketnog upitnika i treće poglavlje „Ispitivanje znanja i osviještenosti opće populacije o kibernetičkoj sigurnosti“. U tom poglavlju objašnjena je svrha provedbe rada, te se navode istraživačka pitanja i hipoteze i detaljno se opisuje metoda metodologije koja je korištena pri istraživanju. Kako bi se utvrdilo realno stanje znanja opće populacije u razdoblju moderne tehnologije u poglavlju pod brojem četiri " Rezultati i analiza istraživanja" provest će se i detaljno analizirati dobiveni rezultati anketnog upitnika. Diplomski rad završava danim preporukama, zaključkom, literaturom i popisom slika.

2 Kibernetička sigurnosti

Brzi tehnološki napredak i prijelaz na digitalnu domenu sa sobom donosi nove, moderne opasnosti i rizike. Intenzivna primjena informacijskih i digitalnih tehnologija dovodi do povećanja ovisnost o tehnologiji, bilo da se radi o osobnoj ili poslovnoj primjeni iste, a samim time raste i ranjivost na kibernetičke napade. Korištenjem sve sofisticiranijih tehnika, napadači u opasnost dovode same pojedince, mala poduzeća te velike organizacije. Razumijevanje kibernetičke sigurnosti i podizanje svijesti o važnosti kibernetičke sigurnosti omogućit će adekvatno prepoznavanje prijetnji i rizika, ali i pravovremeno djelovanje kako bi se izbjegli sigurnosni incidenti.

2.1 Što je kibernetička sigurnost?

Postoje različite definicije pojma kibernetičke sigurnosti. Prema definiciji Središnjeg državnog ureda za razvoj digitalnog društva kibernetička sigurnost obuhvaća skup procesa, mjera i standarda koji osiguravaju određenu razinu pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru. Sustavna zaštita računala, računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od zlonamjernih napada doprinosi u tom području.[2] Prema navodima Udruge za reviziju i kontrolu informacijskih sustava ISACA (engl. *Information System Audit and Control Association*), kibernetička sigurnost se odnosi na zaštitu informacijske imovine putem rješavanja prijetnji koje nastaju u procesu obrade, pohrane i transporta putem umreženih informacijskih sustava.[3] Prema navodima Agencije Europske unije za kibernetičku sigurnost ENISA (engl. *European Union Agency for Cybersecurity*) kibernetička sigurnost odnosi se na sigurnost kibernetičkog prostora, pri čemu se sam kibernetički prostor odnosi na skup veza i odnosa između objekata koji su dostupni putem generalizirane telekomunikacijske mreže, i skupu samih objekata gdje predstavljaju sučelja koja omogućuju njihovo daljinsko upravljanje, daljinski pristup podacima ili njihovo sudjelovanje u kontrolnim radnjama unutar tog kibernetičkog prostora. (ENISA, 2016.) Iako postoje različite varijacije u definicijama kibernetičke sigurnosti, sama srž stručne, akademske

[2] Središnji državni ured za razvoj digitalnog društva, (n.d) Kibernetička sigurnost
[3] Udruga za reviziju i kontrolu informacijskih sustava ISACA, (2016.), *Cybersecurity Fundamentals Glossary,* preuzeto 14 travnja 2023 s https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/cybersecurity_fundamentals_glossary.pdf?la=en&hash=B74D338B90ED9CEA1B4E05AABF40139EF692C866

i državne literature, sadrži jednake ključne komponente koja označavaju zajednička stajališta o navedenom pojmu. Jedno od tih stajališta je da je ključni cilj kibernetičke sigurnosti uspostava mjera koje će spriječiti ili ublažiti pojavu prijetnji. (Perković, 2022.)

2.1.1 Pristupi upravljanja kibernetičkom sigurnosti

Postoje različiti pristupi upravljanja kibernetičkom sigurnosti. Inženjerskim pristupom moguće je dosegnuti maksimalnu sigurnost na internetu korištenjem robusnijeg softvera, kriptiranjem podataka, boljom provjerom cjelovitosti podataka, ali i boljim tehničkim standardima i inovacijama koji predstavljaju ključ ovog pristupa. Nacionalni pristup (engl. *Homeland security*) pomaže otkrivanju ilegalnih aktivnosti u zemlji i inozemstvu, otkriva napade na vitalne nacionalne interese, pojedince i poduzeća/institucije. Ključ ovoga pristupa su državne granice i intervencionizam.[4] Sljedeći pristup je ekonomsko-tržišni pristup koji stvara učinkovite i održive ekonomske i tržišne mehanizme koji će diktirati regulatorna, cjenovna i ostala tržišno usmjerena pravila kojih se svi moraju pridržavati. Primjeri tih mehanizama su: regulatorna pravila (objava informacija, odgovornosti), porezna politika (ulaganje u kibernetičku sigurnost), obveza dojave i analize sigurnosnih incidenata, pozitivne mrežne eksternalije, sveobuhvatni izvještaji o sigurnosti, kibernetičko osiguranje.[5]

2.2 Važnost kibernetičke sigurnosti

Iako je kibernetička sigurnost jedan od najvažnijih izazova s kojima se današnje vlade suočavaju, svijest javnosti o samoj važnosti kibernetičke sigurnosti ostaje ograničena.

Tehnološki napredak i uvođenje pametnih uređaja natjerali su i vladine i privatne organizacije na podizanje svijesti o kibernetičkim prijetnjama i rizicima. [6]

[4] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[5] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.

[6] De bruijn, H., Janssen M., (2017.), Building Cybersecurity Awareness: The need for evidence-based framing strategies, Government Information Quarterly, Volume 23, Issue 1, str. 1-7

Kako bi se razumjela važnost kibernetičke sigurnosti za pojedince i kompanije, te kako bi ih se zaštitilo od namjernih, sofisticiranih i ciljanih informatičkih napada, krađe podataka i incidenata[7], potreba za podizanjem svijesti i brušenju vještina o kibernetičkoj sigurnosti postaje sve hitnija zbog ovisnost o informacijskoj i komunikacijskoj tehnologiji (engl. *Information and Communications Technology*) u svim aspektima društva. [8]

Informacijska i komunikacijska tehnologija (engl. *Information and Communications Technology*) predstavlja skup tehnologija i alata, putem kojih se prenose sve vrste informacija. Svojim snažnim utjecajem na društvo i gospodarstvo, postaje temelj ekonomije 21. stoljeća. ICT tehnologija ključni je pokretač promjena u svim aspektima društva.[9] Brzi napredak informacijske tehnologije transformirao je način na koji Vlade, tvrtke, organizacije i pojedinci - koji svojim namjernim ili nenamjernim postupcima predstavljaju najveću prijetnju kibernetičkoj sigurnosti, moraju pristupiti pitanjima kibernetičke sigurnosti. Razvija se globalna kultura kibernetičke sigurnosti kao mjera za promicanje sigurnog ponašanja, a uključuje devet komplementarnih elemenata:[10][11]

a) *Svijest.* Sudionici trebaju biti svjesni potrebe za sigurnošću informacijskih sustava i mreža, te razumijevanje njihove uloge u povećanju razine sigurnosti;
b) *Odgovornost.* Sudionici su odgovorni za sigurnost informacijskih sustava i mreža na način koji je prilagođen njihovim individualnim ulogama. Oni bi trebali redovito analizirati svoje politike, prakse, mjere i postupke, te procijeniti prikladnost za okruženja;
c) *Odgovor.* Sudionici bi trebali pravovremeno i proaktivno djelovati kako bi spriječili, otkrili i odgovorili na sigurnosne incidente. Ukoliko je potrebno, sudionici trebaju dijeliti informacije o prijetnjama i ranjivostima, te primjenjivati procedure za brzu i učinkovitu suradnju kako bi se spriječilo, prepoznalo i reagiralo na iste;

[7]Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[8] European Union Agency for Cybersecurity, Arcus, R., Sarri, A. (2021.), *Raising awareness of cybersecurity : a key element of national cybersecurity strategies*, (R.Arcus, editor, A.Sarri, editor) Publications Office of the European Union. Preuzeto sa: **https://data.europa.eu/doi/10.2824/363629**
[9] Budin,L., Bajica,M., Carić, A., Čerić V., Glavinić V., Lovrek,I., Manger, R., Ursić, S., Hrvatska u 21. stoljeću, Informacijska i komunikacijska tehnologija, Ured za strategiju razvitka Republike Hrvatske, Zagreb, 2001 (ISBN 953-6430-23)
[10] Arbanas. K, Spremić M., Zajdela Hrustek, N., (2020.) Holistic framework foe evaluating and improving information security culture, *Aslib Journal of Information Management*, 73 (5), 699-719 doi:10.1108/ajim-02-2021-0037.
[11] UN, General Assembly (2003.), Creation of a global culture of cybersecurity : resolution / adopted by the General Assembly, preuzeto 14 travnja 2023 sa: https://digitallibrary.un.org/record/482184

d) *Etika*. Sudionici moraju svjesno poštivati legitimne interese drugih pojedinaca, prepoznajući da njihovo djelovanje ili nedjelovanje može negativno utjecati na druge;
e) *Demokracija.* Prilikom provođenja sigurnosnih mjera, potrebno ih je provoditi u skladu s vrijednostima priznatim u demokratskim društvima. To uključujuće slobodu izražavanja ideja i misli, slobodan protok informacija, zaštitu povjerljivost informacija i komunikacija, odgovarajuću zaštitu osobnih podataka, te otvorenost i transparentnost;
f) *Procjena rizika*. Svi sudionici trebaju redovito provoditi evaluacije rizika kojima se identificiraju prijetnje i ranjivosti. Evaluacije rizika trebaju biti sveobuhvatne i usmjerene kako bi obuhvatile ključne unutarnje i vanjske faktore, poput tehnologije, fizički i ljudski faktori, politike i treća strana pružanja usluga. Evaluacije rizika trebale bi omogućiti određivanje prihvatljivog nivoa rizika i pružati pomoći u odabiru odgovarajućih odnosno adekvatnih kontrola za upravljanje rizikom.;
g) *Sigurnosni dizajn i provedba*. Prilikom planiranja i dizajniranja, upravljanja i korištenja informacijskih sistema i mreža, sudionici trebaju inkorporirati sigurnost kao ključni element;
h) *Upravljanje sigurnošću*. Sudionici bi trebali usvojiti sveobuhvatan pristup upravljanju sigurnošću koji se temelji na procjeni rizika. Ovaj element obuhvaća sve razine aktivnosti sudionika i sve aspekte njihovog poslovanja;
i) *Ponovna procjena*. Redovitim pregledavanje i ponovnim procjenjivanjem sigurnost informacijskih sistema i mreža, te poduzimanjem odgovarajućih izmjena u sigurnosnim politikama, praksama, mjerama i postupcima koji uključuju adresiranje novih i promjenu postojećih prijetnji i ranjivosti, sudionici će stvoriti sigurnije globalno okruženje[12][13]

[12] United Nations General Assembly. (2002.), The role of the United Nations in the field of information and telecommunications in the context of international security.
[13] Hamidović, H. (2015.), Mjesto i uloga cyber sigurnosti u razvoju modernih društava. Sarajevski žurnal za društvena pitanja.

2.3 Prijetnje i rizici

Rizik se odnosi na mogućnost nastanka određenog izvora prijetnje, koji iskoristiti ranjivost odnosno slabost informacijskog sustava u određenim uvjetima i time nanijeti štetu imovini organizacije.[14] U ovom diplomskom radu, fokusirati ćemo se na kibernetičke rizike. Kibernetički rizici predstavljaju poslovne rizike koji proizlaze iz široke primjene informacijskih sustava i tehnologija.[15] Intenzivnom primjernom informacijskih sustava i tehnologija nastaju opasnosti i prijetnje koje mogu rezultirati nepoželjnim ili neočekivanim posljedicama, bilo da se radi o financijskim štetama ili drugim vrstama štete unutar organizacije i njezinoga neposrednog okruženja. Šteta može biti materijalna i financijska, te izravna ili neizravna.[16] Kibernetičke rizike često nazivamo i IT rizicima, koji promatrajući ih s nove perspektive upravljanja rizicima, predstavljaju vjerojatnost da prijetnje mogu iskoristit ranjivost i na taj način stvoriti negativne učinke na imovinu informacijskih sustava (u koje spadaju podatci, softver i hardver) i usluge, ali i na cijelo poduzeće.[17] Kako bi se uspješno upravljalo navedenom vrstom rizika, potrebno je kontinuirano ocjenjivati učinkovitost sigurnosnih kontrola. [18]

Kibernetički rizici proizlaze iz djelovanja prijetnji. Prijetnje se mogu kategorizirati prema njihovom mjestu nastanka, kao unutrašnje i vanjske prijetnje. Unutrašnje prijetnje uključuju internu prijevaru, neovlašteni pristup informacijama iznutra, krađe resursa informacijskoga sustava, greške u unosu podataka u aplikacije i nesvjesno otkrivanje povjerljivih informacija. Vanjske prijetnje uključuju hakerske napade, zlonamjerni računalni kod, društveni inženjering, epidemije bolesti i elementarne nepogode.[19]

Iz navedenih primjera možemo zaključiti da se u današnje vrijeme glavne prijetnje na internetu odnose na:

a) Kibernetički kriminal (engl. *Cybercrime*) također zvan računalni kriminal, koristi računala ili računalne uređaje kao što su pametni telefoni, tableti, osobni digitalni pomoćnici (PDA) itd.,

[14] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[15] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[16] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[17] Spremić, M.,(2012.), Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks , Ekonomski fakultet, Zagreb.
[18] Spremić, M., Šimunić A., (2018.), *Cyber Security Challenges in Digital Economy* In *World Congress on Engineering WCE*. Vol. vol. I. London, UK,
[19] Spremić, M. (2017.): Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.

kao instrumente za počinjenje daljnjih nezakonitih ciljeva, kao što je počinjenje prijevare, trgovina dječjom pornografijom i intelektualnim vlasništvom, krađa identiteta ili kršenje privatnosti. [20][21]

Takvu vrstu kriminala provode pojedinci ili organizacije, koji mogu izvršavati unutarnje ili vanjske napade na druge pojedince ili organizacije, te na temelju navedene činjenice možemo kibernetički kriminal kategorizirati u dvije vrste:[22]

1. Insajderski napad predstavlja napad na mrežu ili računalni sustav od strane osobe s ovlaštenim pristupom sustavu. Općenito ga izvode nezadovoljni ili nesretni zaposlenici ili izvođači zaposleni unutar organizacije koji prodaju pristup drugim napadačima. Motiv takvog napad može biti osveta ili pohlepa. Kibernetičkom kriminalcu relativno je lako izvesti napad jer je dobro svjestan politika, procesa, IT arhitekture i dobrobit sigurnosnog sustava, te sam napadač ima pristup mreži, pomoću koje mu je relativno lako doći do osjetljivih informacija, odnosno srušiti mrežu. Ovakva vrsta napada može se spriječiti planiranjem i instaliranjem internih sustava za otkrivanje upada (IDS) u organizaciji.
2. Vanjski napad zahtjeva angažiranje vanjskog ili unutarnjeg entiteta za izvršenje napada. Organizacija koja je žrtva kibernetičkog napada suočava se sa financijskim gubitkom, ali i gubitkom ugleda s obzirom da je napadač pristupio mreži organizacije, unatoč uspostavljenim mjerama kontrole.

Kibernetičke napade možemo klasificirati kao strukturirane i nestrukturirane napade na temelju stupnja zrelosti napadača. Neki od autora klasificiraju ove napade kao oblik vanjskih napada, ali postoji velik broj slučajeva kada je strukturirani napad bio obavljan od strane internog zaposlenika:

1. Nestrukturirane napade provode amateri koji nemaju unaprijed definirane motive za izvođenje kibernetičkog kriminala.
2. Strukturirane napade izvode vješti i iskusni hakeri koji imaju pristup sofisticiranim alatima i tehnologijama pomoću kojih mogu pristupiti drugim mrežama, te njihov upad u sustave neće primijetiti ni sustavi za otkrivanje upada (IDS).[23]

[20] Encyclopedia Britannica, Cybercrime, preuzeto 15.travnja 2023. s https://www.britannica.com/topic/cybercrime
[21] Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University
[22] Pande, J. (2017), Introduction to Cyber Security, Uttarakhand Open University
[23] Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University

b) Kibernetička špijunaža predstavlja vrstu kibernetičke prijetnje koja se koristi za krađu i otkrivanje povjerljivih informacija, te uključuje neovlašteno odavanje tajni bez pristanka nositelja informacija (bilo da se radi o osobnim, osjetljivim, vlasničkim ili tajnim informacijama) od pojedinca, konkurenata, vlade.[24] Provodi se s ciljem postizanja ekonomske, političke ili vojne prednosti koristeći se ilegalnim metodama na internetu, mreži ili pojedinačnim računalima. Napad može biti izvršen od strane pojedinaca ili kriminalnih skupina, a ponekad i državnih agencija.[25] Razvojem Interneta i digitalnih tehnologija riješen je najveći problem kibernetičke špijunaže: ograničenost informacija. Internet je omogućio golemu količinu informacija koje su toliko obilne da je njihovo analiziranje i potvrđivanje postalo izazovno, a samim time vlade i privatni subjekti počeli su dobrovoljno širiti informacije koje ranije nisu bile dostupne. Rast društvenih medija mogao bi se smatrati dobrovoljnim širenjem informacija, gdje pojedinci dobrovoljno dijele podatke o sebi na društvenoj mreži, misleći da su zaštićeni. [26]

Primjer ovakve vrste napada je napad zvan *Night Dragon*. *Night Dragon* bila je kampanja cyber špijunaže izvršena od strane vlade koja je ciljala naftne, energetske i petrokemijske tvrtke, zajedno s pojedincima i rukovoditeljima u Kazahstanu, Tajvanu, Grčkoj i Sjedinjenim Državama. Neidentificirani akteri tražili su informacije vezane uz proizvodne sustave naftnih i plinskih polja, financijske informacije te su prikupljali i podatke iz SCADA sustava (eng. *Supervisory Control And Data Acquisition*). Na temelju opaženih tehnika, alata i mrežnih aktivnosti, sigurnosni istraživači procijenili su da je kampanja uključivala skupinu aktera sa sjedištem u Kini.[27]

c) Kibernetičko ratovanje definirano je kao akcija jedne države koja želi prodrijeti u nacionalnu mrežu ili računala druge države, vlade ili vojne mreže sa svrhom nanošenja štete ili disrupcija. Osim akcija od strane države napade mogu izvršavati terorističke skupine, političke ili ideološke tvrtke, ekstremističke skupine, haktivisti i transnacionalne kriminalne organizacije.[28]

---

[24] Hercigonja, M. (2019.), *Kibernetska sigurnost : Stručni završni rad* (Završni rad). Zaprešić: Veleučilište s pravom javnosti Baltazar Zaprešić
[25] Hercigonja, M. (2019.), *Kibernetska sigurnost : Stručni završni rad* (Završni rad). Zaprešić: Veleučilište s pravom javnosti Baltazar Zaprešić
[26] Kallberg, Jan. (2018.), Cyberespionage, SAGE Publications, Inc
[27] Gulen, K., (2022.), Cyber espionage remains a real threat to both governments and business, Data Conomy, preuzetno 18. travnja 2023 s https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/?utm_content=cmp-true
[28] Hrůza, P., Cerny, J., (2017.), Cyberwarfare. International conference KNOWLEDGE-BASED ORGANIZATION. 23. 10.1515/kbo-2017-0024

[29] Iz tog su razloga oružane snage, obavještajne službe i službe za provođenje zakona mnogih zemalja postavili računalnu sigurnost kao glavni prioritet za financijska ulaganja i zapošljavanje. Međutim razvoj modernih tehnologija s ofenzivnim sposobnostima, dovodi pojedine zemlje u nelagodan položaj, jer se takve tehnologije pojavljuju brže nego su pojedine zemlje sposobne razviti potrebnu obranu protiv njih. Takve tehnologije također nadmašuju sposobnost međunarodnih zajednica za pronalaženje rješenja za reguliranje kibernetičkih sukoba. Moguće rješenje mogu biti bilateralni i multilateralni sporazumi između različitih država. Ovi sporazumi mogu definirati norme, standarde i principe miroljubivog ponašanja; uspostaviti pravila i postupke u slučajevima teških kibernetičkih incidenata; olakšati suradnju i stvaranje zajedničkih kapaciteta za otkrivanje kibernetičkih napada i identifikaciju napadača.[30]

Primjer ovakve vrste napada predstavlja *Stuxnet*, revolucionarno kibernetičko oružje. Dizajniran od strane obavještajne agencije Sjedinjenih Američkih Država i Izraela s ciljem uništenja i sprječavanja razvoja nuklearnog oružja s primarnim fokusom na uništenje centrifuga koje je Iran koristio za obogaćivanje urana kao dio nuklearnog programa. Za prijenos *Stuxnet* iskorišten je *USB stick,* a nakon ulaska u sustav maliciozni kod manipulirao je programibilnim logičkim kontrolerima (engl. PLC) te promijenio njihov rad izdavanjem zlonamjernih naredbi. Takve naredbe uzrokovale su nekontroliranu brzinu centrifuga i njihovo neočekivano isključivanje. Stuxnet je uspješno sabotirao proces obogaćivanja uranija, a samim time spriječio razvoj nuklearnog programa Irana. Predstavlja međunarodni kibernetički napad, koji je poslužio kao poziv na oprez Vladama, organizacijama i pridonio važnosti kibernetičke sigurnosti u vezi s utjecanjem i posljedicama kibernetičkog ratovanja.[31]

2.3.1 Vrste kibernetičkih napada

Kibernetički napad predstavlja bilo koji nedozvoljeni pokušaj pristupa računalu, računalnom sustavu i računalnoj mreži s namjerom uzorkovanja štete, krađe, razotkrivanja ili uništavanja

[29] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[30] Klopfer,F., Rizmal, I., Sekuloski, M., Hatzl, T., Mladenovic, D., (2019.) Introduction to Cybersecurity Governance – A tool for Members of Parliament, Geneva Center for Security Sector Governance preuzeto s https://cybilportal.org/stage73uere8/publications/introduction-to-cybersecurity-governance-a-tool-for-members-of-parliament/
[31] CSO,(2022.), Stuxnet explained: The first known cyberweapon, preuzeto s https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html

informacija putem neovlaštenog pristupa. Glavni cilj je zaštititi IT infrastrukturu i podatke razvojem i implementacijom odgovarajućih mjera zaštite, a kako bi mogli izabrati iste, potrebno je raspoznati različite vrste kibernetičkih napada:

a) Zlonamjerni računalni programi (eng. *Malware*) dizajnirani za dobivanje pristupa računalu ili su instalirani u računalo bez pristanka s namjerom ometanja ili nanošenja određene štete. Svrha malwarea je ugroziti integritet, povjerljivost ili dostupnosti podataka, aplikacija, operativnog sustava ili drugih dijelova računalnoga ili informacijskoga sustava[3233]. Tijekom 2022. svjetski broj napada zlonamjernim softverom dosegnuo je 5,5 milijardi, što predstavlja povećanje od dva posto u usporedbi s prethodnom godinu i time postaju jedni od najčešćih vrsta kibernetičkih napada.[34] Isto tako važno je razlikovati tipove zlonamjernih softvera, a to su:
   - Računalni crvi (engl. *Worms*) sastavljeni su od samo-kopirajućega koda koji omogućava razmnožavanje i širenje svoga malicioznog sadržaja putem računalne mreže;[35]
   - Virusi su napisani s ciljem da naštete računalu brisanjem ili dodavanjem datoteka, zauzimanjem memorije i usporavanjem performansi računala. Virus se može nalaziti u računalu, ali ne može se aktivirati bez ljudske intervencije;
   - Zlonamjerni oglašivački softver (engl. *Adware*) koristi se za prisilno oglašavanje i promociju proizvoda ili događaja;
   - Špijunski softver (engl. *Spyware*) dizajniran je za krađu osjetljivih podataka bez znanja korisnika;
   - Ucjenjivački softver (eng. *Ransomware*) predstavlja vrstu računalne ucjene kojom se nakon neovlaštenog upada, podaci šifriraju te kibernetički kriminalci traže odštetu za njihovo dešifriranje;[3637]

[32] Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University
[33] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb
[34] Statista (2023.), Annual number of malware attacks worldwide from 2015 to 2022 preuzeto 6. svibnja 2023 s https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
[35] Spremić, M. (20217.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb
[36] Pande, J. (2017.), Introduction to Cyber Security., Uttarakhand Open University
[37] Spremić, M. (20217.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb

b) *Phishing* napad predstavlja vrstu računalne prijevare koji za cilj ima krađu identiteta. Ovaj oblik napada provode prevaranti i računalni kriminalci. Žrtve *Phishing* napada dobivaj lažne elektroničke poruke, koje izgledaju kao da su poslane od strane legitimne organizacije. Cilj je otkrivanje povjerljivih korisničkih podataka žrtve. Slična vrsta takve prijevare, gdje se dobivaju lažni pozivi umjesto elektroničke pošte naziva se *Vishing* napad;[38]

c) *Man-in-the-Middle* napadi predstavljaju vrstu napada prisluškivanjem. U ovom obliku napada, napadač se nalazi na kanalu komunikacije između izvora i odredišta podataka, te na taj način iskorištava ranjivosti mreže kako bi zaobišao komunikacijske protokole. Samim time, napadaču je mu omogućeno pohranjivati datoteke, nadgledati sadržaj komunikacije, ali ga i mijenjati.

d) Napadi uskraćivanjem usluge (eng. *Denial-of-Service*) predstavljaju vrstu računalnih napada koji nedopuštenim aktivnostima sprječavaju ili onemogućavaju ovlaštene uporabu računalne mreže, sustava ili programa iskorištavajući njihove resurse;

e) Raspodijeljeni napad uskraćivanjem usluge (eng. *Distributed Denial-of-Service*) predstavlja vrstu koordiniranog napad prilikom kojeg se upotrjebljuje više računala, ponekad i botneta s ciljem onemogućavanja rada sustava;
Botnets se odnose na mrežu velikog broja povezanih uređaja koji su pod kontrolom napadača, ali bez znanja korisnika. *Botnets* se koriste kao alat za zlouporabu određenih računalnih resursa, kao što su slanje neželjenih poruka elektroničke pošte - spam poruka, zlouporaba online oglašivanja, izvođenje napada uskraćivanjem usluge, podrška *phishing* napadima itd.;[39]

f) Socijalni inženjering predstavlja vrstu napada kojom se iskorištava ljudska pogreška, te se navodi pojedinca na otvaranje zlonamjernih dokumenata, datoteka ili elektroničke pošte kako bi se dobio pristup osobnim podacima ili sustavu. Prema istraživanju koje provodi ENISA (engl. *European Union Agency for Cybersecurity*) 60% izvršenih

[38] Spremić, M. (20217.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb
[39] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb

napada u Europi, Bliskom istoku i Africi uključuje socijalni inženjering kao sastavni dio napada[40][41];

g) Dezinformiranje predstavlja širenje lažnih i netočnih informacija i podataka s ciljem stvaranja straha i neizvjesnosti. Povećanom uporabom društvenih mreža i online medija dovela je do porasta lažno plasiranih informacija. Korištenjem *Deepfake* tehnologije moguće je stvarati lažne audio i video uratke te fotografije koje su gotovo nemoguće razlikovati od stvarnih.;

U istraživanju koje provodi ISACA, navodi se da bi 97% kibernetičkih napada bilo spriječeno ako bi se provodile učinkovite metode zaštite, koje se koriste za otkrivanje ili sprečavanje nepoželjnih događaja ili problema iz vanjskih izvora informacijskog okruženja.[42]

2.4 Proaktivne i reaktivne metode zaštite

U posljednjih 15 godina pojavili brojni problemi koji uvelike utječu na sigurnost informacijskih sustava kao što su to: povrede podatka, unutarnje i vanjske prijetnje te zlonamjerni napadi.[43] Postoje dvije vrsta strategija kibernetičke sigurnosti koje se koriste pri zaštiti od rizika i prijetnji te je vrlo je važno razumjeti razliku između proaktivnih i reaktivnih metoda zaštite, s toga se u prvom dijelu ovog poglavlja fokus stavlja na proaktivnu metodu.

2.4.1 Proaktivna metoda zaštite

Proaktivna kibernetička sigurnost uključuje proces otkrivanja, prepoznavanja i rješavanja zlonamjernih aktivnosti u sustavu putem internih alata za praćenje ili uz pomoć vanjske usluge koji objavljuju informacije o otkrivenim incidentima, prije nego dođe do napada, odnosno prije nego pogođeni sustavni dijelovi postanu svjesni problema.[44] Možemo zaključiti da su ove sigurnosne mjere prvenstveno usmjerene na sprječavanje napada, te da je fokus na svim

[40] European Parliament. (2023.), Cybersecurity: main and emerging threats.
[41] European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I. (2022.), *ENISA threat landscape 2022 – July 2021 to July 2022*,
[42] Spremić, M., Šimunić A., (2018.), Cyber Security Challenges in Digital Economy In *World Congress on Engineering WCE*. Vol. vol. I. London, UK,
[43] Spremić M., (2013.), Holistic Approach for Governing in Information System security, Lecture Notes in Engineering and Computer Science. 2. 1242-1247.
[44] Białczak, P., Pawliński P., Rydz, K., Mattioli, R., (2020.), Proactive Detection – Survey Results, European Union Agency for Cybersecurity

procesima, metodama i aktivnostima koje bi se trebale redovito provoditi unutar organizacije kako bi se spriječili rizici na način da se lociraju i isprave ranjivosti sustava prije nego iste te ranjivosti mogu iskoristit kriminalci.
Vrste metoda i aktivnosti koje se mogu provoditi kako bi se proaktivno reagiralo kibernetičke rizike i prijetnje su:

1) *Lov na prijetnje:* Cilj ove proaktivne metode je identificirati nepoznate prijetnje koje vrebaju unutar sustava organizacije. Ova metoda omogućuje shvaćanje razmišljanja kibernetičkih kriminalaca. Sigurnosni stručnjaci pretvaraju se da su probili obrambeni sustav tvrtke, a na temelju toga pokušavaju predvidjeti plan potencijalnog kibernetičkog kriminalca sa te ulazne točke. Ovom metodom analiziraju se najslabije točke sustava, a nakon identifikacije prijetnji, mogu se implementirati obrambeni koraci kako bi zlonamjernim kriminalcima otežali ili čak onemogućili izvođenje takvih napada u budućnosti.[45]

2) *Penetracijsko testiranje/etičko hakiranje:* Etični hakeri (engl. *ethical hacker, white hat*) su stručnjaci računarstva i računalnih mreža te se bave ispitivanjem sigurnosti računalnih sustava, izvodeći stvarne napade umjesto da pokušavaju oponašati način razmišljanja kibernetičkog kriminalca, što ovu metodu razlikuje od metode lova na prijetnje. Etički hakeri, prema uputama vlasnika ciljanog sustava, nastoje iskoristiti slabosti sustava s ciljem identifikacije ranjivosti i sprečavanja djelovanja zlonamjernih hakera. Rad etičnog hakera često se još naziva i penetracijskim testiranjem (engl. *penetration testing*).[4647] Penetracijsko testiranje je metodologija koja se koristi pri procijeni sigurnosti računalnog sustava ili mreže putem simuliranja stvarnog napada. Prilikom provođenja testiranja, ovlašteni ispitivač simulira različite vrste napada koristeći se tehnikama koje bi koristio i stvarni napadač. Svrha je uočiti bilo kakvu ranjivost koje bi mogle biti iskorištene za ostvarivanje neovlaštenog pristupa.[48]

[45] Thompson, E., (2020.), Threat Hunting, HIPPA, Compliant Security Operation Centar
[46] CARNet CERT–a i LS&S–a,. (2008.), Metodologija penetracijskog testiranja. 3-4., Hrvatska akademska i istraživačka mreža
[47] Mukherjee, A. (2023). *Proactive Cybersecurity - What Is It, and Why You Need It*. Threat Intelligence, dostupno na: https://www.threatintelligence.com/blog/proactive-cybersecurity (pristupljeno: 4.5.2023)
[48] CARNet CERT–a i LS&S–a,. (2008.), Metodologija penetracijskog testiranja. 3-4, Hrvatska akademska i istraživačka mreža

3) *Proaktivno praćenje mreže i krajnje točke:* Kako bi doista bili proaktivni u kibernetičkoj sigurnosti, nužno je nadzirati vlastitu mrežu na dnevnoj bazi, te vršiti nadzor krajnje točke. Učinkovita strategija nadzora krajnjih točaka obično uključuje niz sigurnosnih alata, obavljanje zadataka kao što je praćenje dnevnika povezanih s poslovanjem, osiguravanje ažuriranja zakrpa i otkrivanje skrivenih prijetnji poput zlonamjernog softvera otpornog na memoriju. Cilj automatiziranih programa koji provjeravaju nepravilnosti u sustavu jest slanje obavijesti o potencijalnim poteškoćama koji bi se mogli uzrokovati štetu, ako se na vrijeme ne zaustave.[49] Primjeri programa koji koriste nadzor mreže kao dio zaštite kibernetičke sigurnosti su:

   a) Nmap – Network Mapper je besplatni uslužni program otvorenog koda za skeniranje mreže i neovisni alat za reviziju sigurnosti. Razvijen od strane Gordona Lyon-a. Nmap se definira kao alat koji može otkriti ili dijagnosticirati otvorene portove u sustavu povezanom s internetom te prepoznavati potencijalne sigurnosne propuste.[50]
   b) Wireshark je vodeći svjetski analizator otvorenog koda mrežnih protokola i predstavlja standard u mnogim industrijama. Dizajnirao ga je Gerald Combs. Glavni cilj programa je analizirati promet, presijecati informacije o paketima podatkovne mreže u stvarnom vremenu i pohranjivati ih tako da korisnik može vidjeti navedene pakete podatkovne mreže u jednostavnom korisničkom sučelju, te se može koristit za otkrivanje zlonamjernog prometa i hakiranja mreže.[51] [52]

4) *Edukacija zaposlenika*: Iznenadna pojava globalne pandemije Covid-19 naglo mijenja način poslovanja. Prelazak sa radnih mjesta u uredu na rad od kuće (poznatijeg kao *work form home, telework*) donosi nove rizike povezane sa informacijskom, a samim time i kibernetičkom sigurnošću. Ljudske pogreške su slučajne radnje pod utjecajem stavova, znanja i ponašanja zaposlenika. Radi vlastitog neznanja, neuki zaposlenici razotkrivaju vrijedne i poslovne informacije, te otvaraju neovlašteni pristup oportunističkim kriminalcima. Iz svega navedenog jasno je da kibernetička i informacijska sigurnost uvelike ovise o ponašanju zaposlenika koji može ojačati ili

[49] Kwon, J., Johnson, M. E. (2011, June). An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security. In *WEIS*.
[50] Liao, S, Zhou, C., Zhao, Y., Zhang, Z., Zhang, C., Gao, Y., Zhong, G., (2020). A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments, Huazhong University of Science and Technology, China
[51] Vanparia, P., Ghodasara, Y., Donga, H., (2015.), Network Protocol Analyzer with Wireshark, Developeriq.in.
[52] Adams, M., (2013.), Wire Shark What is it & What is its purpose?, Illinois Institute of Technology

oslabiti sigurnost IS. Stoga je vrlo važno ozbiljno shvatiti značaj ljudskih čimbenika u kibernetičkoj sigurnosti, razvijati globalnu kibernetičku kulturu i odgovornost[53] te poduzeti potrebne mjere za minimiziranje rizika. Edukacijom zaposlenika o kreiranju snažnih lozinka, prijavljivanjem i brisanjem sumnjivih poruka elektroničke poste, korištenjem VPN za pristup podacima tvrtke na osobnom telefonu stvoriti će sigurnije okruženje kako u uredu, tako i prilikom rada od kuće.[54]

Prema istraživanju tržišta Data Bridge-a ulaganje u proaktivna sigurnosna rješenja kao što su lov na prijetnje, edukacija zaposlenika, penetracijsko testiranje, omogućilo je poduzećima bolju procjenu rizika i ranjivosti, napredniju zaštitu od zlonamjernih softvera, a samim time i pravovremeno sprječavanje opasnosti.[55] U svojim analizama tržišta Data Bridge očekuje da će tržište proaktivne sigurnosti narasti s 32,55 milijardi USD u 2022. na 108,57 milijardi USD do 2030., uprosječenu godišnju stopu rasta (engl. CARG, *Compound Annual Growth Rate*) od 16,25% tijekom predviđenog razdoblja. Zaključno, očekuje se rast ulaganja u proaktivne mjere sigurnosti, uz prepoznavanje važnosti proaktivnih mjera, od strane pojedinaca i poduzeća, u zaštiti od kibernetičkih prijetnji i zaštite od sve složenijih napada.[56]

2.4.2 Reaktivna metoda zaštite

Uspješan pristup suočavanja sa kibernetičkim kriminalcima uključuje višestruke slojeve zaštite. Brzim tehnološkim napretkom širi se površina napada, gdje samouvjereni, tehnički potkovani kriminalci, iskorištavaju ranjivosti poduzeća i izvršavaju napade koristeći se unaprijeđenim tehnikama, alatima i metodama. Upravo iz tog razloga reaktivna metoda zaštite, iako sadrži nedostatke, je važna i ne treba je zanemariti.

Reaktivna kibernetička sigurnost predstavlja potpunu suprotnost od proaktivne kibernetičke sigurnosti. Reaktivne strategije usmjerene su na rješavanje tradicionalnijih napada. Sastoje se od čekanja vidljivih znakova upada i indikatora ugroženosti, a kada se napad dogodi pokreću

[53] Arbanas. K, Spremić M., Zajdela Hrustek, N., (2020.) Holistic framework foe evaluating and improving information security culture, *Aslib Journal of Information Management*, 73 (5), 699-719 doi:10.1108/ajim-02-2021-0037.

[54] Ncubukezi, T. (2022.), Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security. (395-403.)

[55] Data Bridge Market Research. (2021.). Global Proactive Security Market Report. Dostupno na: https://www.databridgemarketresearch.com/reports/global-proactive-security-market

[56] Data Bridge Market Research. (2021.). Global Proactive Security Market Report. Dostupno na: https://www.databridgemarketresearch.com/reports/global-proactive-security-market

plan za sustavno rješavanje njegovih posljedica. Većina poduzeća ima postavljane strategije kibernetičke sigurnosti, te se često oslanjaju samo na njih, a u stvarnosti bi reaktivni sigurnosni pristup trebao biti samo jedan dio veće obrambene slagalice.[57]

Reaktivne metode kibernetičke sigurnosti mogu uključivati:

1) Vatrozid (engl. *Firewall*) predstavlja vrstu sigurnosne mjere koja se koristi za zaštitu računalne mreže, bilo u obliku softvera ili hardvera. Primarni cilj vatrozida je kontrola dolaznoga i odlaznoga prometa u mreži. Vatrozid analizira dolazne podatkovne pakete i primjenjuje prethodno definirana sigurnosna pravilima. Na taj način odlučuje se hoće li se dozvoliti ili blokirati ulazak paketa u zaštićeni dio mreže. Vatrozid propušta samo sigurnosno ispravan sadržaj u branjeni dio mreže. Unutarnji ili zaštićeni dio računalne mreže najčešće se naziva i demilitarizirana zona (DMZ). Demilitarizirana zona predstavlja sigurne, branjene i pouzdane dijelove računalne mreže namijenjene pohrani najvažnijih dijelova informacijskoga sustava.[58] Možemo zaključiti da su vatrozidi bitna komponenta mreže organizacije, koji štite organizaciju protiv virusa i drugog zlonamjernog koda, ali i sprječavaju hakere da iskoriste korisnikovu mrežnu infrastrukturu za pokretanje DOS napada.[59]

2) Antivirusni softver dizajniran je za detekciju i zaštitu sustava od malicioznog koda, virusa, crva, trojanskih konja itd. koji se šire putem interneta kako bi ugrozili sigurnost računala ili uništili podatke pohranjene u računalu, ili kako bi stekli financijsku korist krađom lozinki. Antivirusni program redovito ažurira svoje baze podataka i osigurava imunitet sustava protiv ovih novonastalih prijetnji i rizika.[60] Poznati antivirusni softveri su McAFee, Sophos Home, Norton AntiVirus, AVAST, TOTAL AV itd.[61]

3) Upravljanje i zaštita lozinkom ključan je segment sigurnosti informacijskih sustava. Lozinke povijesno predstavljaju prvu liniju obrane protiv neovlaštenog pristupa

[57] Kwon, J., Johnson, M. E. (2011, June). An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security. In *WEIS*.
[58] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[59] Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University
[60] Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University
[61] Spremić, M. (2017.),Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb

računalu i osobnim podacima, štite korisnikovu privatnost i osiguravaju povjerljivost podataka koje dijeli putem interneta. Što je lozinka jača, snažnija, to je korisničko računalo ili uređaj sigurnije. Međutim, postavljanje snažne lozinke, zna biti izazovno. [62]Kako bi se korisnicima/zaposlenicima omogućilo lakše postavljanje što kvalitetnije lozinke, u nastavku su zapisane određene preporuke:

- lozinka treba biti što dulja, a minimalno osam znakova
- lozinka treba biti kombinacija velikih i malih slova, brojeva, simbola
- prilikom kreiranja lozinke važno je izbjegavati korištenje osobnih podataka
- potrebno je izbjegavati da lozinka bude riječ iz rječnika. [63]

Prilikom obrade rezultata istraživanja „ Znanje i osviještenosti opće populacije o kibernetičkoj sigurnosti“ dodatno ćemo se osvrnuti na važnost postavljanja snažnih lozinka.

4) Plan oporavka i upravljanje kontinuitetom poslovanja predstavljaju skup aktivnosti, postupaka i pravila koji se primjenjuju kako bi se preventivnim mjerama spriječili nepoželjni štetni događaji, te kako bi se reaktivnim mjera prema kojima se reagiralo u slučaju njihova nastanka.[64] Svrha i cilj procesa ovog procesa je osigurati neometan nastavak poslovanja u slučaju bilo kakvoga štetnog događaja, prekida ili problema u informacijskom sustavu. Također, ciljevi procesa upravljanja kontinuitetom poslovanja uključuju osiguravanje oporavka i ponovnu uspostavu poslovanja nakon štetnih događaja.[65] Primjeri takvih događaja su raspodijeljeni napadi uskraćivanjem usluge – DDos napadi (engl. *Distributed Denial of Service*) i povreda podataka koja rezultira povredom povjerljivosti, dostupnosti ili cjelovitosti istih.

Korištenjem proaktivnih i reaktivnih metoda zaštite, poduzeća i pojedinci mogu pratiti brz i neprestan razvoj tehnologije, mogu održati povjerljivost, integritet i dostupnost podataka. Također, prepoznavanjem ranjivosti u ranoj fazi i pripremanjem na razne scenarije, moguće je brzo i učinkovito djelovati tijekom kibernetičkih incidenata.

[62] Pande, J. (2017.). Introduction to Cyber Security, Uttarakhand Open University
[63] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb
[64] Spremić, M (2007.), METODE PROVEDBE REVIZIJE INFORMACIJSKIH SUSTAVA, Zbornik Ekonomskog fakulteta u Zagrebu,
[65] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb

3 Ispitivanje znanja i osviještenosti opće populacije o kibernetičkoj sigurnosti

Kako bi se provelo kvalitetno ispitivanje znanja i osviještenosti populacije, potrebno je definirati cilj i svrhu istraživanja te postaviti hipoteze. Hipoteze predstavljaju teorijske odgovore na pitanja o problemu koji će biti empirijski provjeren u istraživanju.[66] Važno je i definirati istraživačka pitanja te navesti moguća ograničenja prilikom provođenja anketnog upitnika. U nastavku, detaljno su opisani, svi navedeni elementi.

3.1 Ciljevi i svrha istraživanja

Kao što je navedeno u prethodnim poglavljima cilj i svrha istraživanja jeste ustanoviti kolika je količina znanja populacije o važnosti kibernetičke sigurnosti, uzimajući u obzir rastuću uporabu interneta u svakodnevnom životu, ali i izlaganju istog opasnostima koje prijete. Fokusirajući se na rastući trend kibernetičkih opasnosti od početka pandemije te sve veću medijsku pokrivenost[67] postavlja se pitanje koliku značajnosti modernoj opasnosti pridaju ispitanici.

3.2 Hipoteze istraživanja

U okviru istraživanja definirane su sljedeće hipoteze:

H1: Razina svijesti i znanja o rizicima kibernetičke sigurnosti pozitivno je korelirana s ostvarenom razinom obrazovanja ispitanika.

H2: Razina svijesti i znanja o rizicima kibernetičke sigurnosti adekvatnija je kod mlađih ispitanika.

H3: Ispitanici pokazuju obrasce ponašanja za koje znaju da su rizični.

---

[66] Vujević, Miroslav (2002.), Uvođenje u znanstveni rad u području društvenih znanosti. Zagreb: Školska knjiga (str. 20- 55).

[67] *The International Criminal Police Organization*, INTERPOL : U.S. National Central Bureau, Washington, D.C. : point of contact for international law enforcement. (2002.). [Washington, D.C.] :U.S. Dept. of Justice : U.S. Dept. of the Treasury,(2020) INTERPOLreport shows alarming rate of cyberattacks during COVID; dostupno na: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (pristupljeno 14.4.2023)

3.3 Istraživačka pitanja

U okviru istraživanja postavljena su sljedeća pitanja istraživačke prirode:

1. Smatraju li ispitanici kibernetičku sigurnost važnim elementom zaštite vlastite privatnosti?

2. Je li razina svijesti i znanja o kibernetičkoj sigurnosti adekvatnija u IT sektoru?

3. Koliki broj ispitanika se smatra potencijalnim kandidatom za kibernetički napad?

3.4 Metodologija

Za potrebe diplomskog rada i provođenja istraživanja korišten je kvantitativni pristup – anketni upitnik. Kvantitativni pristup u istraživanju temelji se na primjeni metoda koje omogućuju kvantifikaciju pojava, tj. njihovo izražavanje brojkama, te generaliziranje zaključaka na cjelokupnu populaciju. Ovaj pristup je koristan za testiranje teorija, proučavanje odnosa, identifikaciju obrazaca u podacima i čak uspostavljanje uzročno-posljedičnih veza među pojavama[68] te je upravo iz navedenih razloga izabran kao najbolji način prikupljanja podataka. Anketni upitnik fokusiran je na ispitivanje pojave na individualnoj razini, što omogućuje izravnu analizu i tumačenje rezultata u odnosu na relevantne demografske, obrazovne i druge karakteristike obuhvaćenih društvenih skupina [69] Anketni upitnik, ispitanicima je proslijeđen putem e-maila, te je u potpunosti anoniman. Ispitivanje je provedeno u razdoblju od 14.4.2023 do 1.5.2023. Postavljena su 3 seta pitanja, prvi set pitanja ispituje opće znanje i osviještenosti populacije o kibernetičkoj sigurnosti, drugi set odnosi se na lozinke koje predstavljaju jedan od ključnih slojeva zaštite[70], dok se zadnji set pitanja odnosi na E- poštu (tkz. Email) - jedan od najvažnijih kanala komunikacije u svakodnevnom poslovanju, ali i jedan od najvećih ulaza za kibernetičke napade. U anketi je sudjelovalo 143 sudionika, a svi ispunjeni upitnici bili su valjani. Uvjeti za sudjelovanje u anketi bili su svakodnevno korištenje interneta i posjedovanje

[68] Mejovšek, M. (2013). Metode znanstvenog istraživanja u društvenim i humanističkim znanostima. Jastrebarsko: Naknada Slap
[69] Rotim, A. (2017). *Društvene mreže i slobodno vrijeme: ovisnost ili stil života?*, Diplomski rad, Fakultet političkih znanosti, Zagreb
[70] VISHNEVETSKY, G.,(2022), *Passwords Are Key to Cyber Security,* dostupno na: https://www.stewart.com/en/insights/2022/passwords-are-key-to-cyber-security.html (pristupljeno 14.4.2023)

pametnog telefona. Ispitanicima je prije same ispune anketa objašnjeno da će se dobiveni rezultati koristit u svrhu izrade diplomskog rada s ciljem otkrivanja znanja opće populacije o kibernetičkoj sigurnosti

3.4.1 Moguća ograničenja prilikom provođenja anketnog upitnika

Zbog složenosti provođenja anketnog upitnika, mogu se pojaviti prepreke i problemi, a oni s kojima smo se susreli prilikom provođenja anketnog upitnika su:

1) Svaki ispitanik može posjedovati više različitih adresa elektroničke pošte, što postavlja pitanje s kojom anketom se ispitanik koristi i otvara se mogućnost višestrukog sudjelovanja u istraživanju
2) Kada se govori o vjerodostojnosti odgovora ispitanika, potrebno je uzeti i u obzir mogućnost takozvanog brzanja (engl. *speeding*) što znači da ispitanik ne posvećuje dovoljno vremena pitanju, te mu odgovor nije nužno vjerodostojan.
3) Ispitanik se može suočiti s tehničkim problemima koji se javljaju nakon što je pristupio ispitivanju. Jedna od takvih poteškoća bila je nemogućnost davanja odgovora na obavezno pitanje koja se javila prilikom ispune pitanja u prvom dijelu anketnog upitnika.[71]

Bez obzira na navedene prepreke i poteškoće, anketni upitnik o znanju i osviještenosti opće populacije na temu kibernetičke sigurnosti, uspješno je proveden.

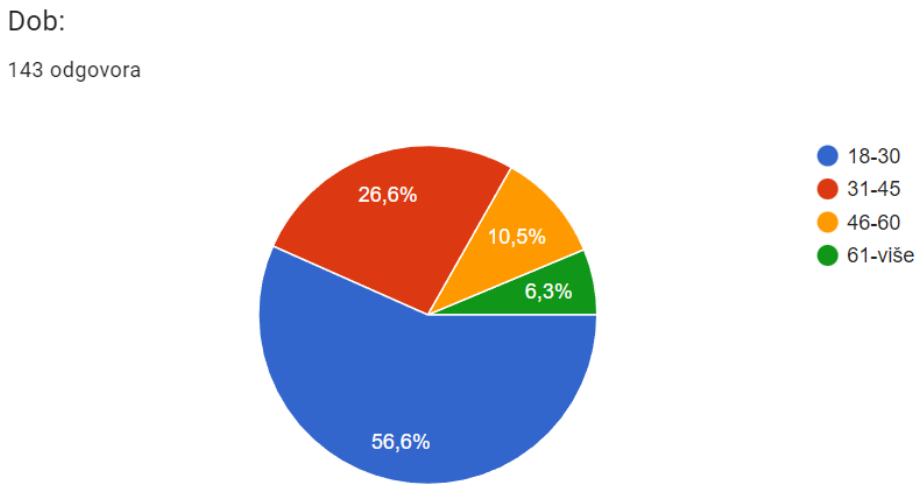
[71] Žmuk, B. (2019.), Najčešći problemi i izazovi u provođenju poslovnih web anketa, Ekonomski fakultet Sveučilište u Zagrebu.

4 Rezultati i analiza istraživanja

Anketa provedena u potpunosti online putem sastavljena je od 3 seta pitanja. Prvi set sadrži 26 pitanja općeg karaktera ispituje opće znanje i osviještenosti populacije o kibernetičkoj sigurnosti, drugi set odnosi se na lozinke i sadrži 14 pitanja, dok se zadnji set odnosi na pitanja vezana za elektroničku poštu te sadrži 7 pitanja.

Pitanja pod rednim brojem od 1. do 4. odnose se na identifikacijske informacije samih ispitanika. Analiza anketnih odgovora pokazala je da od ukupno 143 ispitanika, 85 ispitanika čine osobe ženskog spola (59,4%), a 58 ispitanika čine osobe muškog spola (40,6%). Najniža dobna granica činila je 18 godina, te se u skupini od 18-30 nalazi najveći broj ispitanika, 81(56,6%). U skupini od 31-45 nalazi se 38 ispitanika (26,6%), dok se u skupini od 46-60 nalazi 15 ispitanika (10,5%). Najstariju dobnu skupinu čine ispitanici od 61-više, u kojoj se nalazi 9 ispitanika (6,3%).

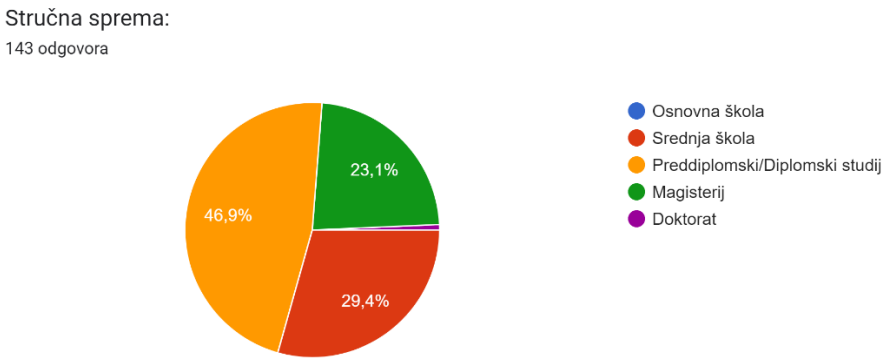
Slika 1 Dobna skupina ispitanika



Izvor: Samostalna izrada autorice rada

Od ukupno 143 ispitanika, njih 101 (70,6%) ima završen barem jedan akademski stupanj obrazovanja, dok preostalih 42 (29,4%) ima završenu srednju školu. Ovaj uzorak je prikladan za donošenje općih zaključaka o utjecaju obrazovanja na znanje o kibernetičkoj sigurnosti.

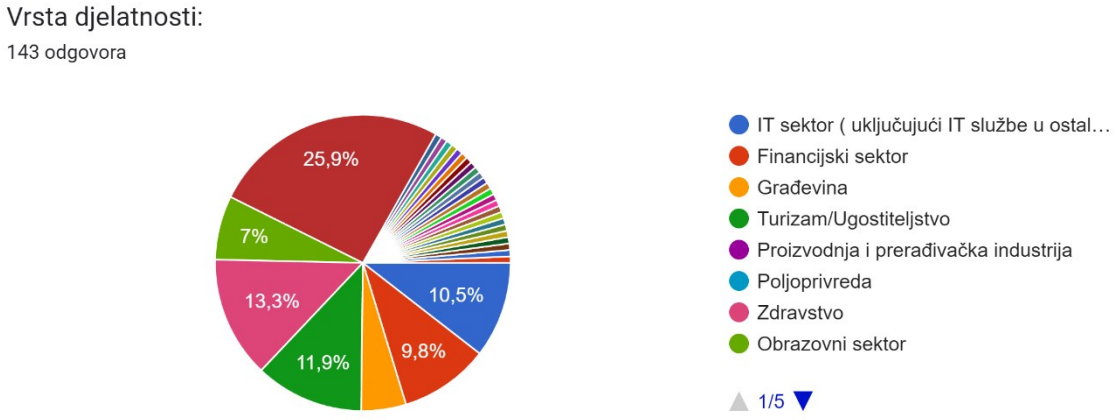
Slika 2 Stručna sprema ispitanika



Izvor: Samostalna izrada autorice rada

Najveći broj ispitanika radi u stručnim, znanstvenim i tehničkim djelatnostima (25,9%), zdravstvu(13,3%), turizmu i ugostiteljstvu (11,9%) i IT sektoru-uključujući i IT službe u ostalim sektorima (10,5%).

Slika 3 Vrsta djelatnosti



Izvor: Samostalna izrada autorice rada

U nastavku diplomskog rada prikazani su rezultati općeg znanja i osviještenosti ispitanika o kibernetičkoj sigurnosti, uz pomoć grafikona popraćeni tekstualnim objašnjenjima i kratkim zaključcima.

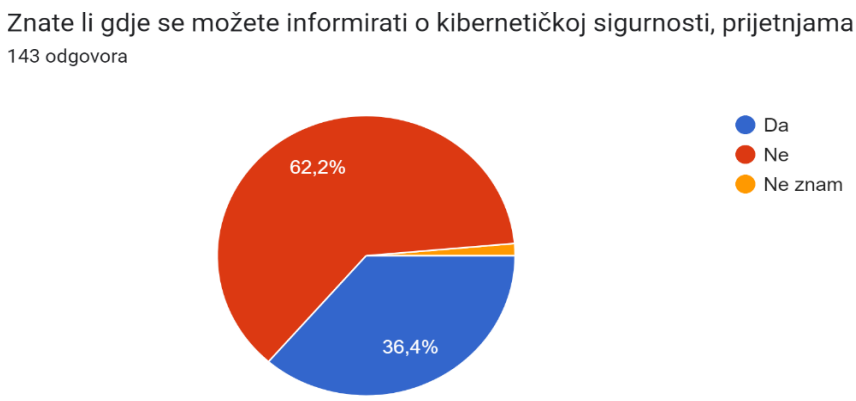
Na pitanje „Smatrate li da je kibernetička sigurnost važna za zaštitu Vaše privatnosti?“ 137 ispitanika odgovorilo je „Da“, a preostalih 6 dalo je negativan odgovor. Iako su dali pozitivan odgovor na prethodno pitanje, 98 ispitanika smatra da nije dovoljno informiranima o kibernetičkoj sigurnosti, prijetnjama i rizicima.

Slika 4 Važnost kibernetičke sigurnosti za zaštitu privatnosti

Izvor: Samostalna izrada autorice rada

Ne dovoljna informiranost o kibernetičkoj sigurnosti, prijetnjama i rizicima rezultat je manjka znanja o mogućim izvorima informacija vezanih za navedenu temu, a to nam pokazuju sljedeći rezultati. Od 143 ispitanika, njih 91 (62,2%) odgovorilo je „Ne“, dok je njih 52 (36,4%) dalo potvrdan odgovor.

Slika 5 Mogućnost informiranja o kibernetičkoj sigurnosti, prijetnjama i rizicima



Izvor: Samostalna izrada autorice rada

Na pitanje „Smatrate li se potencijalnim kandidatom za kibernetički napad?“ odgovorilo je 138 ispitanika, manji broj ispitanika nego na prethodnim pitanjima, ali i dalje reprezentativan uzorak. Razlog k tomu su navedena moguća ograničenja prilikom provođenja anketnog upitnika. Od 138 ispitanika, 98 ispitanika (71%) se ne smatra potencijalnim kandidatom za kibernetički napad, dok se 40 ispitanika (29%) ipak smatra takvim kandidatom. Više od polovine potvrdnih odgovora dale su osobe koje su mlađe od 30 godina, koje imaju završen barem jedan akademski stupanj obrazovanja. Kako bi se promijenio ovakav način razmišljanja, bitno je pridonositi edukaciji o kibernetičkoj sigurnosti, te objasniti općoj populaciji da nije pitanje hoće li biti hakirani, već kada i kolikim intenzitetom.[72]

Slika 6 Potencijalni kandidati za kibernetički napad

Izvor: Samostalna izrada autorice rada

[72] Jalali, M.S.(2018.) Journal of Strategic Information Systems, Volume 28, Issue 1, Pages 66-82

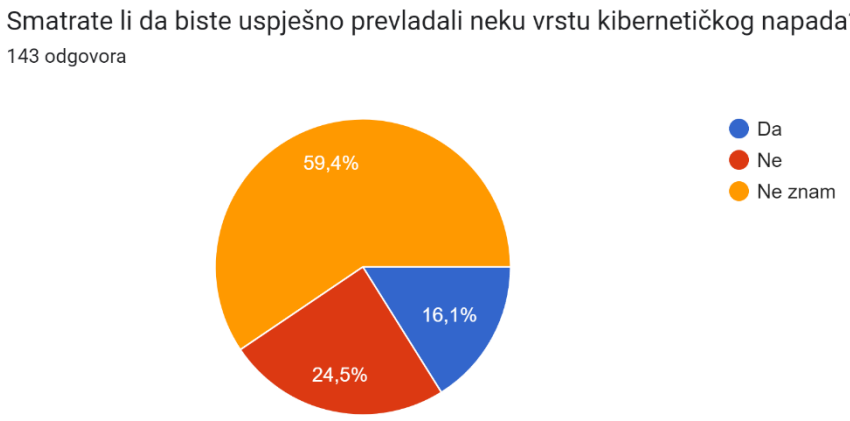
Od ukupno 143 ispitanika, 110 ispitanika (76,9%) nije doživjelo kibernetički napad, a 33 ispitanika (23,1%) susrelo se sa nekom vrstom kibernetičkog napada. Najveći broj ispitanika koji je doživio kibernetički napad nalazi se u dobnoj skupini od 18-30 godine. Pretpostavka je da intenzivnija uporaba internetske mreže od strane žrtava kibernetičkog napada. Na pitanje „Poznate li nekoga tko je doživio kibernetički napad?“ raste broj potvrdnih odgovora na čak 74 (51,7%), dok 69 ispitanika (48,3%) daje negativan odgovor.

Slika 7 Žrtve kibernetičkog napada

Izvor: Samostalna izrada autorice rada

Sljedeće pitanje anketnog upitnika glasilo je „Smatrate li da biste uspješno prevladali neku vrstu kibernetičkog napada?“. Na pitanje je odgovorilo 143 ispitanika, od kojih je 85 (59,4%) odgovorilo sa „Ne znam“, 35 (24,5%) odgovorilo sa „Ne“, a 23 (16,1%) smatra da bi uspješno prevladalo neku vrstu kibernetičkog napada. Daljnjom analizom prikupljenih odgovora, dolazimo do zaključka da su najveći broj potvrdnih odgovora dali zaposlenici zaposleni u IT sektorima, a zatim u stručnim, znanstvenim i tehničkim djelatnostima, što daje odgovor na istraživačko pitanje, koje je glasilo da je razina svijesti i znanja o kibernetičkoj sigurnosti adekvatnija u IT sektoru.

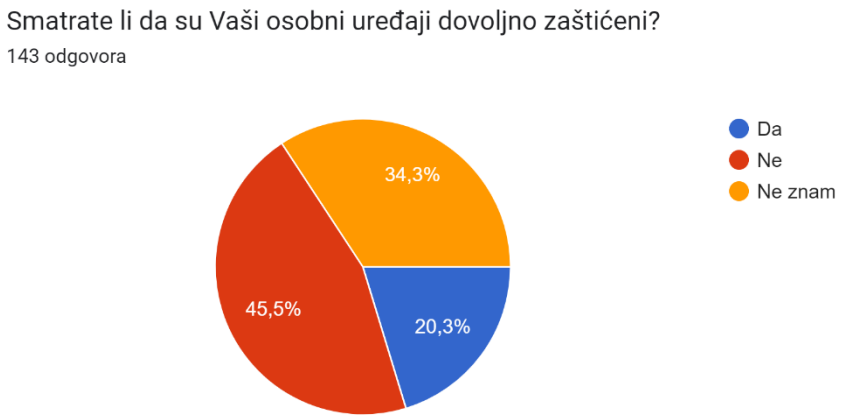
Slika 8 Procjena znanja o prevladavanju kibernetičkog napada



Izvor: Samostalna izrada autorice rada

Većina stanovništva danas koristi pametne uređaje, no postavlja se pitanje „Smatrate li da su Vaši osobni uređaji dovoljno zaštićeni?“. Od 143 ispitanika, 65 (45,5%) ispitanika ne smatra da im je uređaj dovoljno zaštićen, ,49 (34,3%) ispitanika ne zna je li im uređaj dovoljno zaštićen – te se javlja pitanje postoji li manjak znanja ispitanika koji su dali neodlučan odgovor ili problem stvara dobna skupina s obzirom da većina ispitanika koja je dala neodlučan odgovor spada u stariju dobnu skupinu. Preostalih 29 (20,3%) ispitanika smatra svoje osobne uređaje dovoljno zaštićenima, od kojih 21 ispitanik pripada najmlađoj dobnoj skupini.

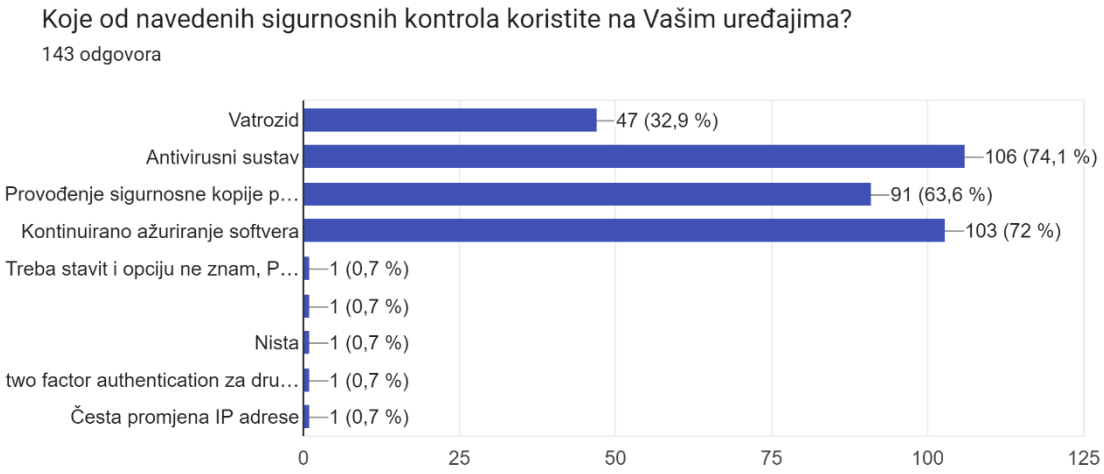
Slika 9 Zaštita osobnih uređaja



Izvor: Samostalna izrada autorice rada

Kako bi uvidjeli kojim sigurnosnim kontrolama na osobnim uređajima se koriste ispitanici postavljeno je sljedeće anketno pitanje „Koje od navedenih sigurnosnih kontrola koristite na Vašim uređajima?“. Na pitanje je bilo moguće ponuditi više odgovora. Također postojala je i dodatna opcija u kojoj se moglo samostalno napisati dodatnu sigurnosnu kontrolu, van onih koje su bile inicijalno postavljenje unutar pitanja. Najveći broj ispitanika provodi kontinuirano ažuriranje sustava (72%) te se koristi nekom vrstom antivirusnog sustava (74,1%). Nešto manji broj ispitanika provodi sigurnosne kopije podataka (63,6%), dok vatrozid kao sigurnosnu metodu koristi najmanji broj ispitanika (32,9%). U samostalno dodanim sigurnosnim kontrolama ispitanici su dodali korištenje dvo-faktorske autentifikacije za društvene mreže, te čestu promjenu IP adrese, dok je jedan ispitanik napisao da ne koristi ni jednu navedeni sigurnosnu kontrolu na svojim uređajima. Svaka osoba zaposlena u IT sektoru provodi minimalno tri sigurnosne kontrole na vlastitim uređajima, što ukazuje na razumijevanje i važnost primjene istih.

Slika 10 Korištenje sigurnosnih kontrola na vlastitim uređajima



Izvor: Samostalna izrada autorice rada

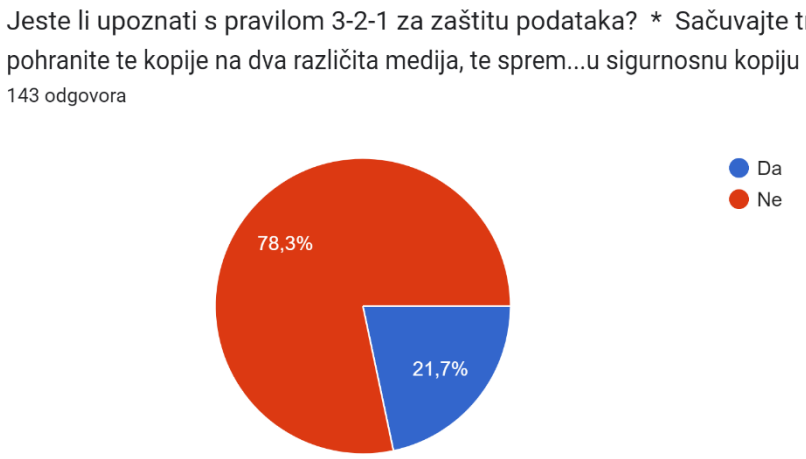
Na pitanje o provođenju sigurnosne kopije podataka, rezultati su sljedeći: Jednom dnevno sigurnosnu kopiju podataka provodi 11 ispitanika (9%), a jednom tjedno sigurnosnu kopiju provodi 22 ispitanika (18%). Na mjesečnoj bazi, sigurnosno kopiranje podataka, provodi 31 ispitanik (25,4%), a svakih par mjeseci 32 ispitanika (26,2%). Iznimno zabrinjavajući podaci prikazuju da sigurnosno kopiranje podataka čak 26 ispitanika (21,3%) provodi sigurnosnu kopiju jednom godišnje ili rjeđe od toga. O samoj važnosti provođenja sigurnosne kopije podataka govorit ćemo u poglavlju „ Preporuke i smjernice namijenjene općem stanovništvu“.

Slika 11 Provođenje sigurnosne kopije podataka

Izvor: Samostalna izrada autorice rada

Primjer jedne vrste sigurnosne strategije je 3-2-1 strategija za zaštitu podataka. Pravilo zahtjeva da korisnik sačuva tri primjerka važne datoteke, pohrani te kopije na dva različita medija, te spremi barem jednu sigurnosnu kopiju na udaljenoj lokaciji ili oblaku. Od 143 ispitanika, 112 ispitanika (78,3%) nije upoznato s navedenim pravilom, dok 31 ispitanik (21,7%) poznaje navedena pravila. Detaljnom analizom rezultata utvrđeno je da svaki ispitanik zaposlen u IT sektoru upoznat je sa ovom vrstom sigurnosne strategije.

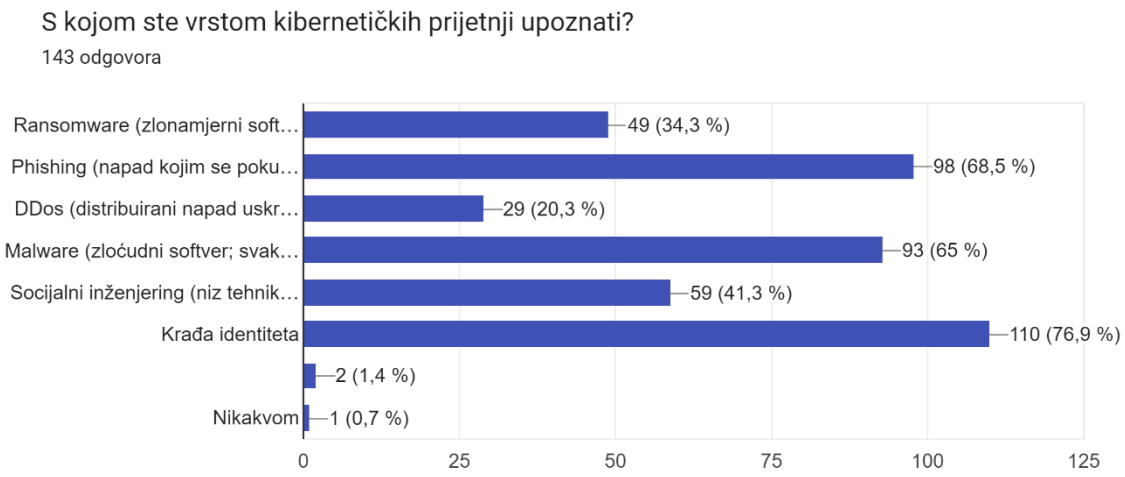
Slika 12. 3-2-1 strategija za zaštitu podataka



Izvor: Samostalna izrada autorice rada

Ispitanicima je bilo ponuđen izbor pet različitih vrsta najčešćih kibernetičkih napada, uz dana objašnjenja istih, te ih se tražilo da izaberu jednu ili više vrsta kibernetičkih napada s kojima su upoznati. Također ispitanicima je ostavljena mogućnost dodatnog odgovora, unutar kojeg su sami mogli dopisati vrstu napada koja nije ponuđena. Od 143 ispitanika, najveći broj ispitanika, 110 (76,9%) upoznato je s krađom identiteta, zatim 98 ispitanika (68,5%) upoznato je s phishing napadima, 93 ispitanika (65%) označava malware, dok je 49 ispitanika (34,4%) i 29 (20,3%) upoznato s ransomwarom i DDos napadima. Jedan ispitanik nije upoznati sa ni jednim od navedenih kibernetičkih prijetnji, a dva odgovora nailaze na tehničke poteškoće priliko davanja obaveznog odgovora na postavljeno pitanje.

Slika 13 Vrste kibernetičkih prijetnji



Izvor: Samostalna izrada autorice rada

Od 133 dana odgovora, 80 ispitanika (60,2%) nema mogućnost rada od kuće, što nam pokazuje da se organizacije nisu u potpunosti prihvatile hibridni način rada, dok ostatak koji čine 53 ispitanika (39,8%) ima tu mogućnost.

Slika 14 Hibridni način rada

Izvor: Samostalna izrada autorice rada

Rad na daljinu širi potencijalnu površinu napada, a ne pružanjem edukacija vezanih za kibernetičku sigurnost organizacije pridonese tom riziku. Od 95 ispitanika, 71 (74,7%) nije imalo organizirane edukacije o kibernetičkoj sigurnosti pružene od strane poduzeća unutar kojeg su zaposleni. S druge strane, samo 24 ispitanika (25,3%) prošlo je kroz takvu vrstu edukacije.

Slika 15 Pružene edukacije o kibernetičkoj sigurnosti

Izvor: Samostalna izrada autorice rada

Na pitanje koriste li ispitanici privatne uređaje u poslovne svrhe, 88 ispitanika (64,2%) odgovorilo je „Da“, dok je 49 ispitanika odgovorilo „Ne“ Korištenje privatnih uređaja u poslovne svrhe 102 ispitanika (73,4%) ne smatra sigurnim, dok se s tvrdnjom ne slaže 37 (26,6%) ispitanika. Ovim pitanjem se potvrđuje jedna od zadanih hipoteza „ Ispitanici pokazuju obrasce ponašanja za koje znaju da su rizični.“ Unatoč razumijevanju opasnosti korištenja privatnih uređaja prilikom obavljanja poslovnih obaveza, ispitanici ne mijenjaju svoj obrazac ponašanja. Pretpostavka je da će se taj obrazac ponašanja promijeniti u trenutku kada se pretrpi neka vrsta kibernetičkog napada koja će rezultirati štetom ili za pojedinca ili za organizaciju unutar koje je pojedinac zaposlen.

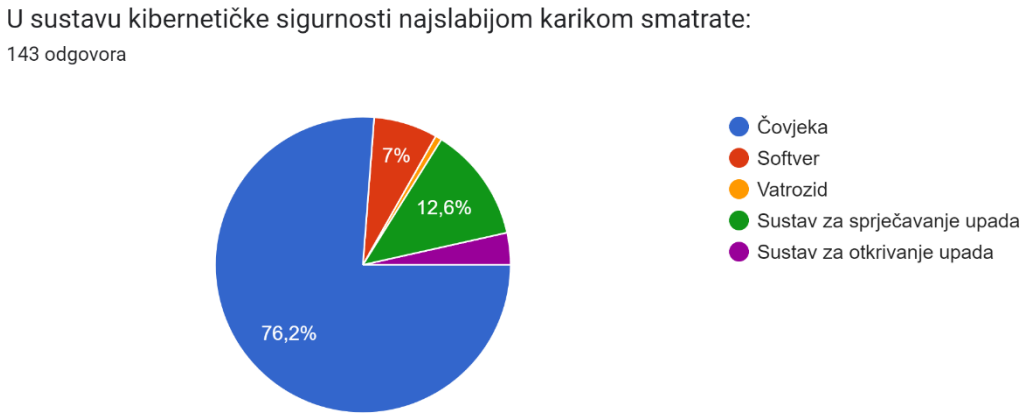
Slika 16 Sigurnost korištenja privatnih uređaja u poslovne svrhe

Izvor: Samostalna izrada autorice rada

Kako bi uvidjeli razumijevanje i razmišljanje ispitanika o kibernetičkoj sigurnosti postavljena su pitanja općeg znanja:

„ U sustavu kibernetičke sigurnosti najslabijom karikom smatrate:“ 109 ispitanika (76,2%) uspješno je raspoznalo čovjeka kao najslabiju kariku u kibernetičkoj sigurnosti, dok je ostatak ispitanika smatrao da je to ipak sustav za sprječavanje upada, sustav za otkrivanje upada, softver ili pak vatrozid.

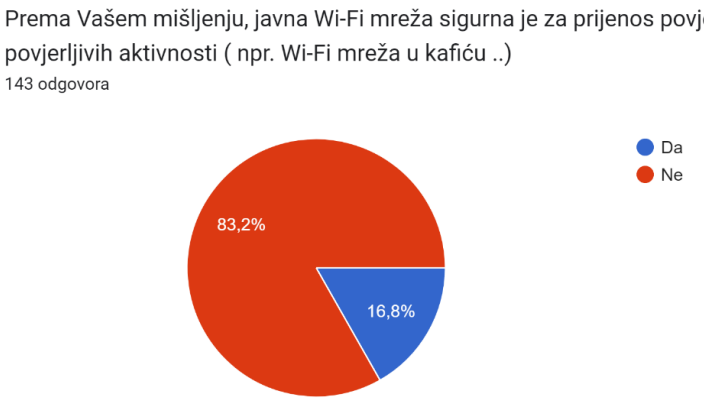
Slika 17 Najslabija karika u sustavu kibernetičke sigurnosti



Izvor: Samostalna izrada autorice rada

„Prema Vašem mišljenju, javna Wi-Fi mreža sigurna je za prijenos povjerljivih podataka i obavljanje povjerljivih aktivnosti (npr. Wi-Fi mreža u kafiću ..)“ 119 ispitanika (83,2%) raspoznaje da javna Wi-Fi mreža nije sigurna za prijenos povjerljivih podataka, dok 24 ispitanika (16,8%) ipak misli da je će biti zaštićeni prilikom obavljanja povjerljivih aktivnosti putem javne mreže. Daljnjom analizom utvrdilo se da svaki ispitanik, koji je dao potvrdan odgovor na navedeno pitanje, spada u stariju dobnu skupinu.

Slika 18 Sigurnost javne Wi-Fi mreže za prijenos povjerljivih podataka i obavljanje povjerljivih aktivnosti



Izvor: Samostalna izrada autorice rada

„Smatrate li da širenje dezinformacija, odnosno stvaranja ili dijeljenja lažnih i pogrešnih informacija, predstavlja vrstu kibernetičke prijetnje“ pozitivan odgovor na navedeno anketno pitanje dalo je 117 ispitanika (84,2%), dok ovu vrstu kibernetičke prijetnje nije prepoznalo 22 ispitanika (15,8%).

Slika 19 Širenje dezinformacija kao vrsta kibernetičke prijetnje

Izvor: Samostalna izrada autorice rada

Na pitanje „Jeste li primijetili povećanje broja napada u posljednjih 3. godine (od početka Covid pandemije)?“ od 143 ispitanika, 77 ispitanika (53,8%) primijetilo je povećanje broja napada u posljednje 3. godine, do 66 ispitanika (46,2%) takvu nema takvu opservaciju.

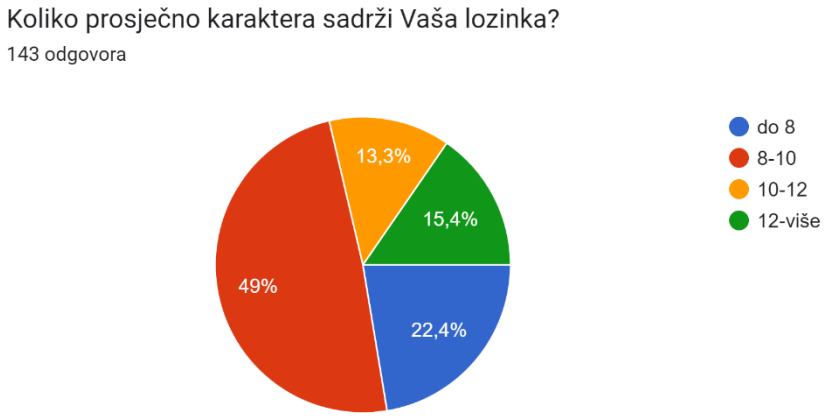
Slika 20 Povećanje broja kibernetičkih napada u posljednje 3. godine

Izvor: Samostalna izrada autorice rada

U drugom djelu anketnog upitnika fokusirali smo se na pitanja posvećena lozinkama. Lozinke su još uvijek su najpopularniji mehanizam provjere autentičnosti na Internetu i vjerojatno će biti i u bliskoj budućnosti.[73]

Na pitanje „Koliko prosječno karaktera sadrži Vaša lozinka?“ 32 ispitanika (22,4%) odgovorilo je „do 8“, 70 ispitanika (49%) odgovorilo je „8-10“, 19 ispitanika (13,3%) odgovorilo je „10-12“, a „12-više“ odgovorilo je 22 ispitanika (15,4%).

Slika 21 Broj karaktera korištenih prilikom kreiranja lozinke



Izvor: Samostalna izrada autorice rada

[73] M., Yıldırım, I., Mackie,(2019.), Encouraging users to improve password security and memorability, International Journal of Information Security

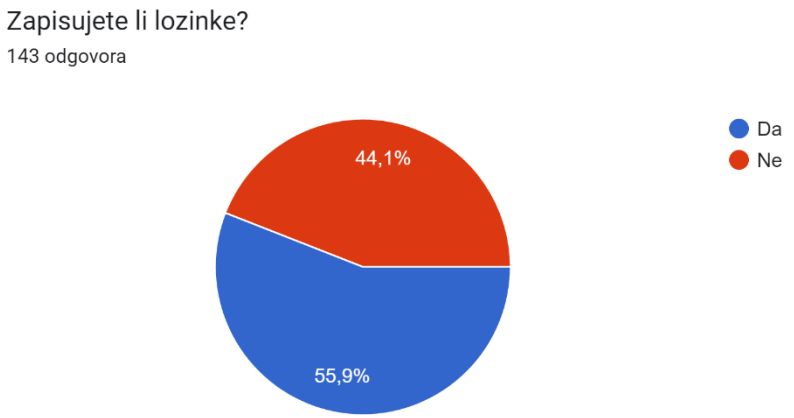
Analiza pitanja o korištenju osobnih podataka prilikom kreiranja lozinke dalo je pozitivne rezultate. Od 143 ispitanika, 89 ispitanika (62,2%) ne koristi osobne podatke kao što su ime, prezime, datum rođenja itd. prilikom kreiranja lozinke, dok ostatak ispitanih (37,8%) ipak koristi dio osobnih podataka u svojim lozinkama.

Slika 22 Korištenje osobnih podataka prilikom kreiranja lozinke

Izvor: Samostalna izrada autorice rada

Na pitanje „Zapisujete li lozinke?“ od 143 ispitanika, 80 (55,9%) ih daje pozitivan odgovor, dok 63 ispitanika (44,1%) ne provodi takvu praksu.

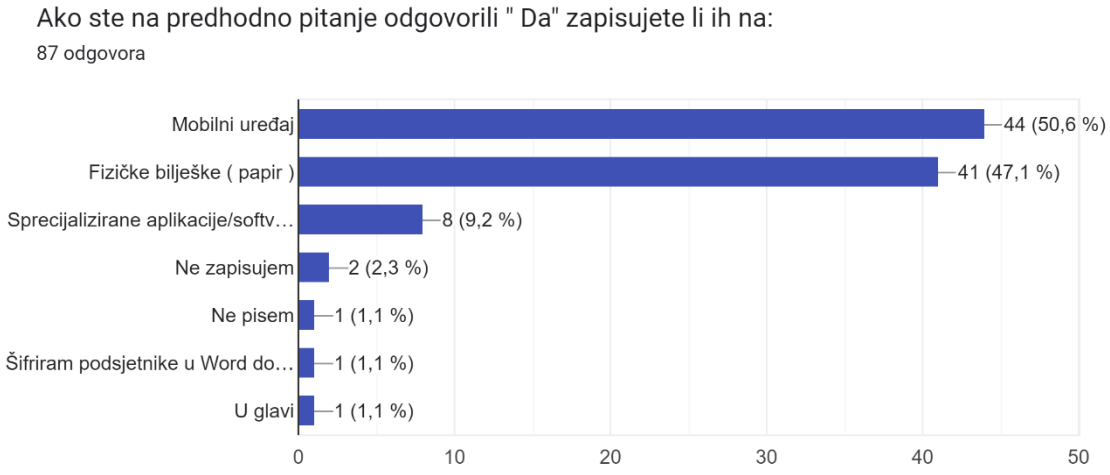
Slika 23 Zapisivanje lozinki



Izvor: Samostalna izrada autorice rada

Ispitanici koji su na prethodno pitanje dali potvrdan odgovor, zamoljeni su da označe na koji gdje zapisuju iste. Odgovori su sljedeći: 44 ispitanika (50,6%) svoje lozinke zapisuje na svojim mobilnim uređajima, 41 ispitanik (47,1%) zapisuje lozinke na fizičke bilješke poput papira, 8 ispitanika (9,2%) za pohranu lozinke koristi specijalizirane aplikacije/softverska rješenja. Ispitanicima je ponovno dana mogućnost dodatnog odgovora među kojima je jedan ispitanik objasnio svoj sistem zapisivanja lozinke – šifriranje podsjetnika u Word dokumentima sa samo prva dva znaka lozinke uz zapisivanje aplikacije na koju se ta lozinka odnosi. Ispitanik predstavlja pravi primjer opreznog korisnika.

Slika 24 Zapisivanje lozinki 2.



Izvor: Samostalna izrada autorice rada

Na pitanje „Jeste li ikada ponovili istu lozinku za različite račune?“ odgovor je dalo 143 ispitanika, od kojih je 128 (89,5%) ponovilo istu lozinku za različite račune. Preostalih 15 ispitanika (10,5%) ne ponavlja svoje lozinke, shvaćajući rizik koji može rezultirati takvom akcijom.

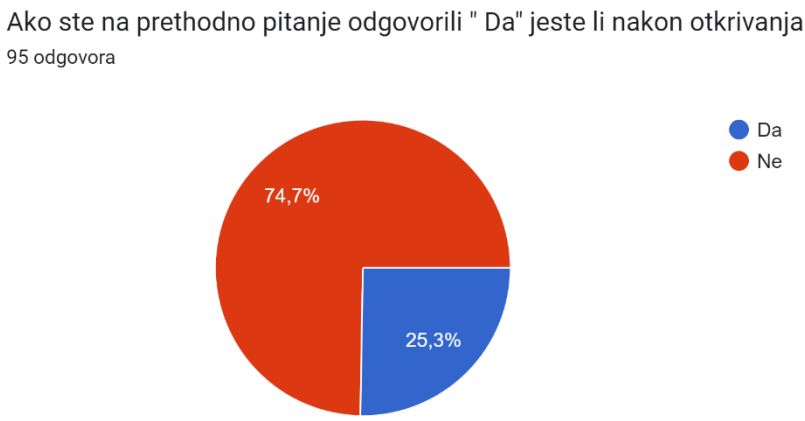
Slika 25 Ponavljanje lozinki

Izvor: Samostalna izrada autorice rada

Kako bi utvrdili razinu neopreznosti ispitanika, postavljena su sljedeća pitanja:

Sljedeće anketno pitanje bilo je „Jeste li ikada slučajno (ili namjerno) otkrili svoju lozinku drugoj osobi?“ na koje je od 143 ispitanika, pozitivan odgovor dalo 88 (61,5%), a negativan 55 (38,5%). Međutim na pitanje „Ako ste na prethodno pitanje odgovorili " Da" jeste li nakon otkrivanja lozinke istu promijenili?“ 71 ispitanik nakon slučajnog (ili namjernog) otkrivanja lozinke istu nije promijenio, što prikazuje još jedan rizičan obrazac ponašanja. Potvrdan odgovor na pitanje dalo je samo 24 ispitanika (25,3%).

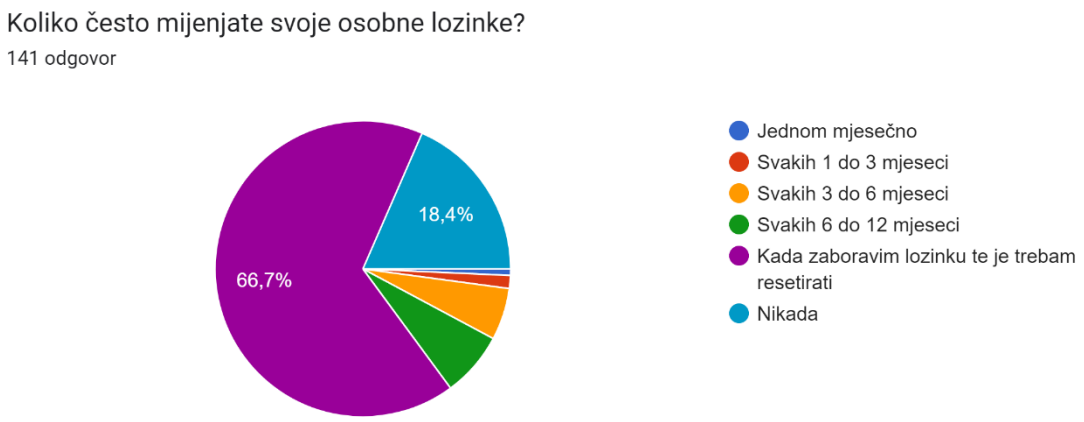
Slika 26 Slučajno ili namjerno otkrivanje lozinki 2



Izvor: Samostalna izrada autorice rada

Proučavanjem grafikona vidljivo je da 94 ispitanika (66,7%) svoju lozinku resetira isključivo u trenucima kada istu zaboravi, te je resetiranje potrebno. Svoju lozinku, 26 ispitanika (18,4%), nije promijenilo od trenutka prve kreacija. Nekoliko puta godišnje svoju lozinku mijena svega nekolicina ispitanika, dok jednom mjesečno promjenu lozinke vrši samo 1 ispitanik.

Slika 27 Promjena osobnih lozinki



Izvor: Samostalna izrada autorice rada

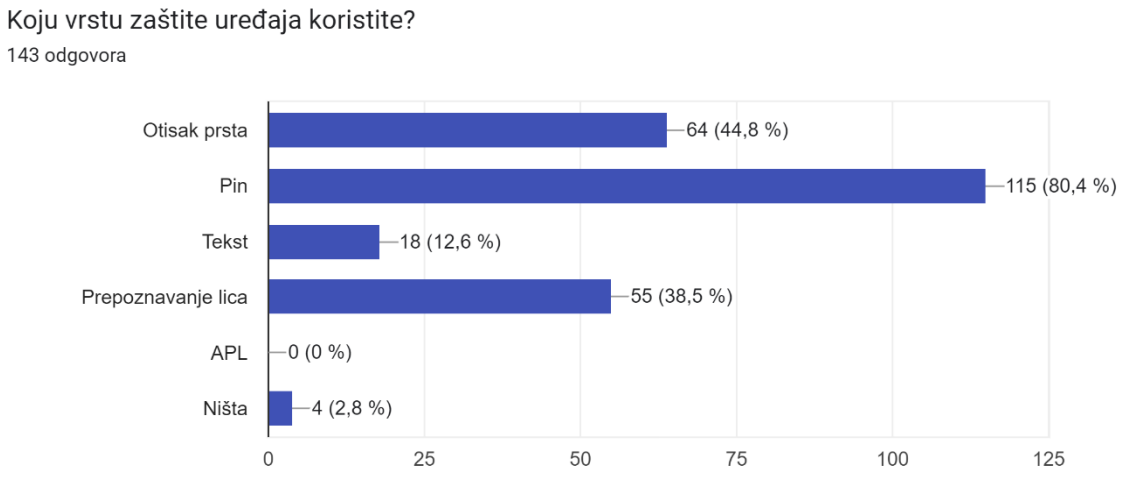
Neku vrstu zaštite na osobnim uređajima koristi 136 ispitanika (95,1%), dok preostalih 7 nije zaštitilo svoje uređaje.

Slika 28 Zaštita uređaja

Izvor: Samostalna izrada autorice rada

Najčešće korištena zaštita uređaja je zaštita PIN-om, tu vrstu zaštite koristi 115 ispitanika (80,4%). Otisak prsta kao način zaštite koristi 64 ispitanika (44,8%), dok prepoznavanje lica koristi 55 ispitanika (38,5%). Najslabije korištene metode zaštite su zaštita tekstom (12,6%) i APL (0,0%). Nezaštićen uređaj posjeduje 4 ispitanika (2,8%).

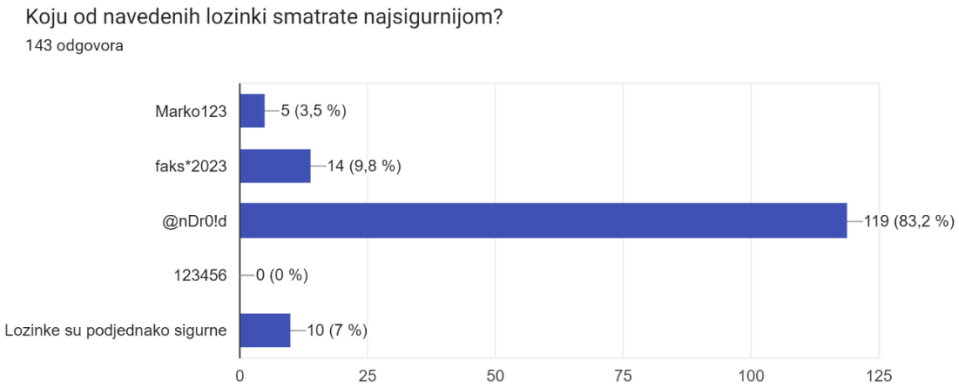
Slika 29 Zaštita uređaja



Izvor: Samostalna izrada autorice rada

Od 143 ispitanika, 119 (83,2%) uspješno je prepoznalo najsigurniju lozinku među ponuđenima, 19 ispitanika (13,3%) izabralo je pogrešnu lozinku, dok 10 ispitanika (7%) smatra da su lozinke podjednako sigurne.

Slika 30 Prepoznavanje najsigurnije lozinke



Izvor: Samostalna izrada autorice rada

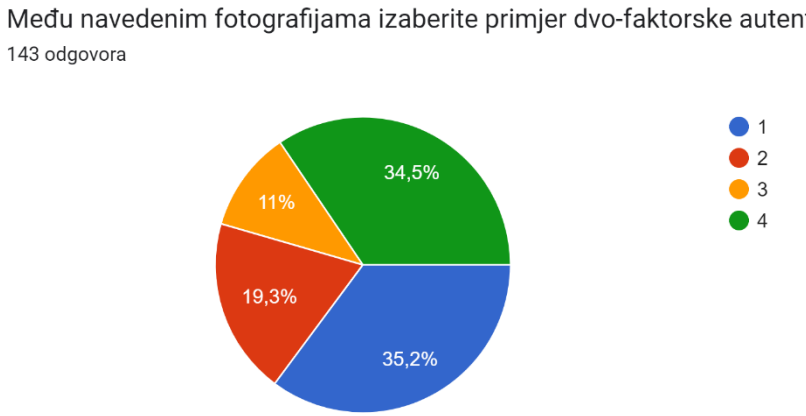
Sa pojmom više faktorske autentifikacije upoznato je 68 ispitanika (47,6%), a 75 ispitanika (52,4%) nije se susrelo sa navedenim pojmom. Od 143 ispitanika, 93 ispitanika (65%) ne koristi se metodom više faktorske autentifikacije ili barem ne zna da se koristi istom, dok 50 ispitanika (35%) koristi navedenu metodu.

Slika 31 Korištenje više faktorskom autentifikacijom

Izvor: Samostalna izrada autorice rada

Na sljedećem pitanju, ispitanici su trebali prepoznati i označiti primjer dvo-faktorske autentifikacije. Zadatak je uspješno obavljen od strane 50 ispitanika (35,2%). Preostalih 83 ispitanika (64,8%) među navedenim fotografijama pogrešno je izabralo primjer dvo-faktorske autentifikacije.

Slika 32 Prepoznavanje najsigurnije lozinke

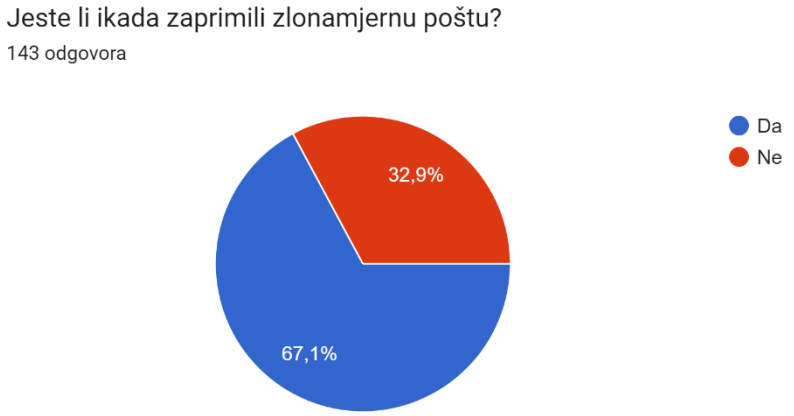


Izvor: Samostalna izrada autorice rada

U trećem, ujedno i posljednjem djelu anketnog upitnika fokusirali smo se na pitanja posvećena elektroničkoj pošti. Elektronička pošta smatra se najpopularnijim sustavom za razmjenu informacija putem Interneta (ili bilo koje druge računalne mreže). Nakon web poslužitelja, poslužitelji e-pošte su hostovi unutar mreže organizacije, koji su najčešće na meti napadača. Upravo iz tog razloga, odgovorno i osviješteno ponašanje korisnika, potrebno je kako bi se poboljšala sigurnost razmjene informacija.[74]

Od 143 ispitanika, na pitanje „Jeste li ikada zaprimili zlonamjernu poštu?“ 96 ispitanika (67,1%) je odgovorilo „Da“, dok je 47 ispitanika (32,9%) odgovorilo „Ne“.

Slika 33 Zlonamjerna pošta

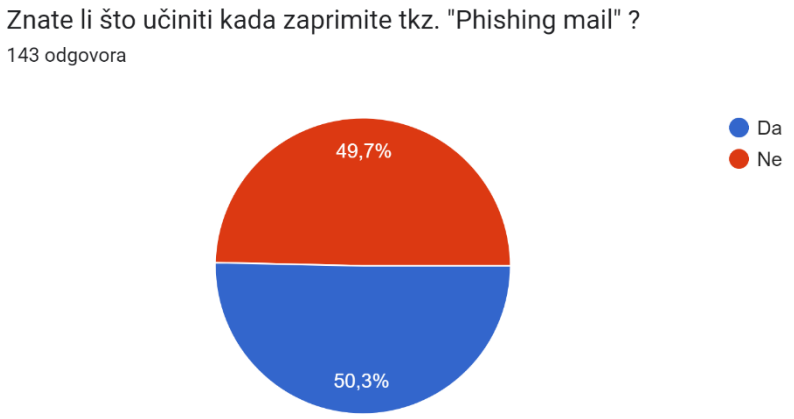


Izvor: Samostalna izrada autorice rada

[74] Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (2007.) Guidelines on Electronic Mail Security, National Institute of Standards and Technology

Sljedeće anketno pitanje „Jeste li upoznati s pojmom Phishing mail?“ pokazuje da je od 143 ispitanika, njih 87 (60,8%) upoznato s pojmom Phishing mail, dok se 56 ispitanih (39,2%) nije susretalo s navedenim pojmom, a na pitanje „Jeste li upoznati sa pojmom „Spam mail?“ 128 ispitanika (90,8%) dalo je potvrdan odgovor, a anketa pokazuje da se 12 ispitanika (9,2%) nije susrelo sa navedenim pojmom. Međutim, nešto manje od polovice ispitanih (49,7%) ne zna koja je procedura kada se zaprimi mail zlonamjernog sadržaja, dok ostatak (50,3%) smatra da bi uspješno prevladao navedenu opasnost.

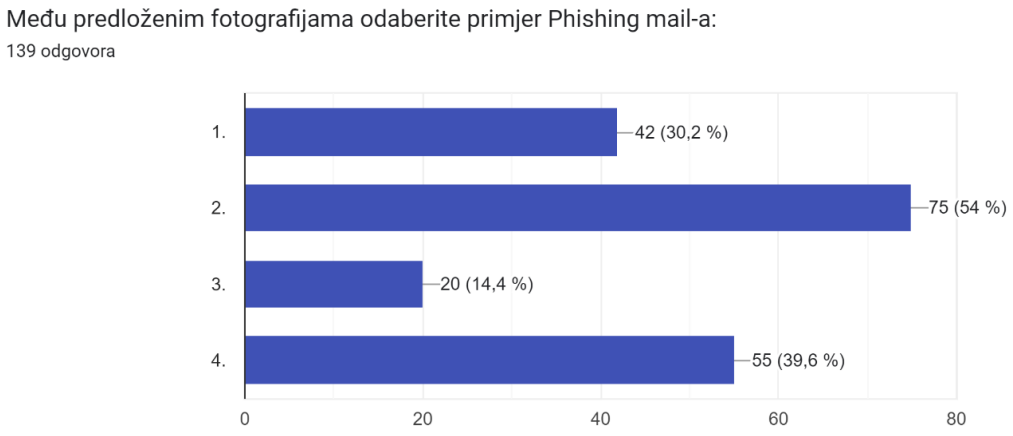
Slika 34 Phishing mail



Izvor: Samostalna izrada autorice rada

Među predloženim fotografijama, ispitanici su zamoljeni da prema svome znanju i razumijevanju Phishing maila, isti i označe. Zadatak je uspješno izvršilo 75 ispitanika (54%) odabirom druge fotografije, te 42 ispitanika (30,2%) odabirom fotografije koja se nalazila na prvom mjestu. Ostatak ispitanika nije uspješno prepoznao primjer Phishing mail-a.

Slika 35 Prepoznavanje Phishing mail-a



Izvor: Samostalna izrada autorice rada

Anketni upitnik pokazuje da 126 ispitanika (88,1%) smatra da je odjava odnosno otkazivanje newslettera poželjna praksa, dok se 17 ispitanika (11,9%) s tim ne slaže.

Slika 36 Odjava/otkazivanje newslettera

Izvor: Samostalna izrada autorice rada

5 Smjernice i preporuke namijenjene općem stanovništvu

U današnje vrijeme, opće stanovništvo se sve više oslanja na Internet i preferira obavljanje osobnih poslova online putem. Iako je internet uvelike olakšao obavljanje svakodnevnih zadataka kao što su komunikacija, plaćanje računa putem modernih aplikacija, online kupovina, te učenje i rad na daljinu, tim napretkom dolaze novi izazovi i rizici vezani uz kibernetičku sigurnost, koji često ostaju neprepoznati od strane općeg stanovništva.

Kako bi dali odgovor na pitanje: „Koliko opća populacija uopće poznaje i razumije važnost kibernetičke sigurnosti?“ proveden je anketni upitnik, a povratni rezultati su zabrinjavajući. Prilikom razgovora sa nekolicinom ispitanika, nakon provedene ankete, većina ih kibernetičku sigurnost povezuje sa sofisticiranim hakerima, te smatraju da kibernetička sigurnost zahtijeva dubinsko znanje informacijske tehnologije i računarstva. Međutim, kibernetički napadi dolaze u različitim oblicima, a najštetnije povrede podataka rezultat su jednostavne ljudske pogreške. [75]

U nastavku, navede su smjernice i preporuke namijenjene općem stanovništvu, sa svrhom edukacije i podizanja svijesti o važnosti kibernetičke sigurnosti, kako bi se umanjile ljudske pogreške te kako bi se pružio temelj za izgradnju sigurnijeg digitalnog okruženja za populaciju:

1) Informiranje o kibernetičkoj sigurnosti

Istraživanje je pokazalo da veliki broj ispitanika kibernetičku sigurnost smatra važnim aspektom pri zaštiti svoje privatnosti, međutim ne znaju gdje se mogu informirati o navedenoj temi. Kako bi omogućili ispitanicima produbljivanje svoga znanja, u nastavku su navedene preporuke stranica koje sadrže sve potrebne informacije o kibernetičkoj sigurnosti.

Vlade različitih republika prepoznale su važnost kibernetičke sigurnosti, te razvijaju i posvećuju portale i odjele koji pružaju ažurirane informacije o najboljim praksama i potrebnim smjernicama koje ukazuju na važnost kibernetike. Iznimno je važno za svakog građana Republike Hrvatske poznavanje zakona i institucija koje se bave jednim od najosjetljivijih pitanja današnjice – kibernetičkom sigurnosti.

[75] The National Association of County & City Health Officials, (2015.), Cybersecurity: Risks and Recommendations for Increasingly Connected Local Health Departments preuzeto 5 svibnja 2023 s https://www.naccho.org/uploads/downloadable-resources/Issue-brief-on-Cybersecurity-NA639PDF.pdf

Vlada Republike Hrvatske, 2016. godine donosi zakon o osnivanju Nacionalnog vijeća za kibernetičku sigurnosti, čija je obaveza pregledavati i organizirati nacionalne vježbe iz područja kibernetičke sigurnosti, izrađivati preporuke, mišljenja, izvješća i smjernice vezane uz provedbu strategija i akcijskog plana.[76] Uspostavom Nacionalnog vijeća za kibernetičku sigurnost uspostavljen je mehanizam za razmjenu informacija i usklađivanja aktivnosti državne uprave na stručnoj, političkoj i upravnoj razini. Svake godine, od osnivanja Nacionalnog vijeća, vijeće za kibernetičku sigurnost formira izvješće o radu, u kojem se bavi najbitnijim pitanjima od velike važnosti za državu i globalno okruženje. [77]

Osim institucije, informiranje je moguće i pomoću portala, a pravi primjer takvog portala je Hrvatski institut za kibernetičku sigurnost. Hrvatski institut za kibernetičku sigurnost osnovan je od strane stručnjaka iz područja kibernetičke sigurnosti, koji djeluju kroz različite stručne i promotivne aktivnosti, te kroz održavanje kongresa iz područja kibernetike. Osnovni cilj i vizija Hrvatskog instituta je unapređenje informacijske sigurnosti u Republici Hrvatskoj kroz razmjenu znanja, edukaciju i profesionalni rast.[78]

Europska unija 2004. godine, razvija Agenciju Europske unije za kibernetičku sigurnost (ENISA) agencija je koja je u potpunosti posvećena postizanju zajedničke razine kibernetičke sigurnosti diljem Europe. ENISA ima ulogu u jačanju kibernetičke politike Europske Unije, kroz implementaciju shema certificiranja kibernetičke sigurnosti. Agencija surađuje s državama članicama i tijelima EU-a i pomaže Europi u suočavanju s izazovima vezanima za kibernetičku sigurnost u budućnosti. ENISA izdaje smjernice i preporuke o upravljanju rizikom, zaštiti kritične infrastrukture, zaštiti osobnih podataka, analize sigurnosnih prijetnji, prikazuje primjere dobre prakse ili daje procjene sigurnosti određenih tehnologija. Međutim izrazito je važno napomenuti da su dokumenti koje ENISA pruža skloni promjenama, radi razvoja i napretka kibernetičke sigurnosti.[79]

Važno je napomenuti i Nacionalni centar za kibernetičku sigurnost (NCSC) koji je osnovan 2011. godine s ciljem savjetovanja i informiranja vladinih pružatelja IT-a i kritične nacionalne

[76] Zakon o nacionalnoj strategiji kibernetičke sigurnosti, Narodne novine, br. 108/15 (2016.)
[77] Ured Vijeća za nacionalnu sigurnost Republike Hrvatske, dostupno na: https://www.uvns.hr/hr/informacijska-sigurnost/kiberneticka-sigurnost
[78] Hrvatski institut za kibernetičku sigurnost, dostupno na: https://hiks.hr/
[79] European Union Agency for Cybersecurity, dostupno na: https://www.enisa .europa.eu/about-enisa/about/hr

infrastrukture o prijetnjama i slabostima. Glavne uloge NCSC-a su upravljanje velikim incidentima kibernetičke sigurnosti u vladi, davanje smjernica i savjeta građanima i tvrtkama o velikim incidentima kibernetičke sigurnosti i razvijanje snažnih međunarodnih odnosa u globalnoj zajednici radi dijeljenja informacija o kibernetičkoj sigurnosti. [80]

Međutim, uzimajući u obzir okupiranost svakodnevnim obavezama te razumijevanjem da ispitanici nemaju dovoljno slobodnog vremena, predlaže se pristupačniji i brži način informiranja putem sljedećih publikacija, blogova, portala i knjiga:
- IT Security Guru: IT Security daje dnevni pregled najnovijih vijesti u industriji IT sigurnosti. Sadrži brojne članke, studije slučaja, analize te imaju posvećen odjeljak najnovijim prijevarama u području kibernetičke sigurnosti.
- The Cyber Security Hub: iznimno zanimljiv svjetski portal o kibernetičkoj sigurnosti koji ažurno objavljuje najnovije vijesti o kibernetičkim napadima, prijetnjama i rizicima, trendovima, analizama tržišta, sigurnosnim incidentima.
- Nick Espinosa: Stručnjak za kibernetičku sigurnost i mrežnu infrastrukturu, koji dizajnira, izgrađuje i implementira multinacionalne mreže, sustave šifriranja i višeslojne infrastrukture. Naglašava važnost proaktivnih metoda zaštite, zaštite podataka, te važnost sigurnost Interneta stvar (IoT). Sudjelovao je na TED Talku u kojem, u samo par minuta, na zanimljiv način objašnjava 5 zakona kibernetičke sigurnosti, koji mogu poboljšati stanje kibernetičke sigurnosti pojedinaca i organizacija. [81]
- *The Art of Invisibility*: knjiga napisana od strane hakera i stručnjaka za kibernetičku sigurnost Kevina Mitnika u kojoj objašnjava tehnike i strategije za očuvanje privatnosti, sigurnosti i anonimnosti u digitalnom svijetu. [82]

2) Generiranje sigurne lozinke

Lozinka predstavlja niz znakova, brojeva, posebnih simbola ili pak riječi, koje korisnik kreira kako bi zatražio pristup određenim uređajima, aplikacijama ili web stranicama. Lozinka predstavlja temeljnu metodu autentifikacije korisnika, pomoću koje se korisnik predstavlja sustavu, a računalo uspoređuje upisne podatke s podacima u bazama korisnika.[83] Iznimno su

[80] National Cyber Security Centre (n.d.) Dostupno na; https://www.ncsc.gov.ie/
[81] Espinosa, N. (Speaker). (7 rujna 2018) The five laws of cybersecurity [Video]. TED Dostupno na: https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity
[82] Mitnick, K. (2017). The Art of Invisibility, Brown and Company
[83] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.

važan faktor pri zaštiti podataka i sigurnosti korisnika, te sprječavaju neovlašten pristup osobnim računima, uređajima i podacima.

Prilikom analiziranja anketnog upitnika, jasno je da većina ispitanika svjesna važnosti odabira snažnih lozinki, međutim radi nedostatka smjernica i savjeta prilikom kreiranja istih, ispitanici gube motivaciju i sastavljaju slabe lozinke. U nastavku nalaze se navedene preporuke i smjernice za generiranje sigurne lozinke:

Postoje različite politike kreiranja lozinki koje prihvaća sustav za provjeru autentičnosti. Takva pravila koriste administratori sustava kako bi poboljšali sigurnost računala usmjeravanjem korisnika za stvaranje sigurnije lozinke. [84]

Istraživanje je pokazalo da većina ispitanika prilikom kreiranja svoje lozinke koristi do maksimalno 12 karaktera, te da istu lozinku koristi za različite račune. Prema izvješću objavljenom od strane ENISE slabe ili ponovljene lozinke (56%) te otključani uređaji (44%) predstavljaju dvije najveće slabosti unutar organizacije.[85] Koliko je jednostavno razotkrivanje slabih lozinki, opisuje sljedeća tablica.

Tablica pokazuje koliko je vremenski potrebno kako bi se „razotkrile“ različite vrste lozinaka. O brzini, koja je potrebna da se razotkrije šifra, utječu različiti faktori poput broja karaktera, sadrži li lozinka samo brojeve, samo slova ili njihovu kombinaciju jesu li upotrjebljena velika i mala slova te jesu li upotrjebljeni posebni znakovi. Iz navedenog proizlazi zaključak – što je lozinka dulja i složenija, lozinka je sigurnija.

Slika 37 Vrijeme potrebno za razotkrivanje lozinke

[84] Yıldırım, M., Mackie, I. (2019.), Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* **18**, 741–759

[85] European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I. (2022.), *ENISA threat landscape 2022 – July 2021 to July 2022*,

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Izvor: https://thesecurityfactory.be/password-cracking-speed/ (preuzeto 30. svibnja 2023)

Smjernice i preporuke za generiranje dobre lozinke su:[86]

1) Lozinka treba imati što više znakova – Kevin Mitnik u svojoj knjizi The Art of Invisibility preporučuje čak 25 znakova;

2) Lozinka treba sadržavati nasumičnu kombinaciju znakova, brojeva, malih i velikih slova, simbola i interpunkcijskih znakova;

3) Lozinka ne smije biti riječ iz rječnika, bilo da se radi o hrvatskom ili stranom rječniku

4) Lozinka ne smije sadržavati osobne podatke;

5) Ne smije se koristiti ista lozinka, dva puta;

Ispitanici pokazuju obrasce ponašanja za koje znaju da su rizični. Lozinke su tajna, ne smiju se otkrivati ili priopćavati drugim korisnicima, ne smiju se zapisivati na mjesta na kojima su dostupna drugim korisnicima, te se trebaju mijenjati.[87] Naime, istraživanje je pokazalo da je velik broj ispitanika podijelio svoju lozinku sa drugim osobama, nakon čega istu nije

[86] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
[87] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.

promijenio. Također, većina ispitanika mijenja svoju lozinku ne mijenja nikada ili provodi promjenu u onome trenu kada istu zaboravi, te je lozinku potrebno resetirati.

Prema kibernetičkim stručnjacima, promjena lozinke mora se vršiti svaka tri mjeseca. Učestala promjena lozinke može smanjiti rizik od kompromitiranja, ali razumljivo je da su sigurnosni problemi u tekstualnoj provjeri autentičnosti lozinke rijetko uzrokovani tehničkim problemima, već ograničenjima ljudske memorije, zato se preporuča korištenje upraviteljem lozinki. Upravitelj lozinki softversko je rješenje koje se koristi za pohranjivanje i upravljanje lozinkama koje se spremaju u šifriranom obliku, te im se pristupa uz pomoć glavne lozinke. Nude i mogućnost automatskog generiranja nasumičnih lozinki, tako stvarajući dodatan sloj sigurnosti.[88]

Jedna vrsta rizičnog ponašanje je zapisivanje lozinki bilo da se radi o fizičkim bilješkama ili zapisivanju lozinki na pametne uređaje. Takav pristup može rezultirati stjecanjem neovlaštenog pristupa korisničkim računima, krađom podataka ili zlouporabom računa. Kako bi se spriječila moguća šteta preporučuje se korištenje višefaktorske autentifikacije. Dodatni korak izvan unosa lozinke kako bi se potvrdilo da osoba koja pokušava pristupiti računu je doista ona kojom se predstavlja. Može se provoditi slanjem tekstualne poruke na broj mobitela vlasnika računa, koristeći se aplikaciju koja podržava autentifikaciju ili korištenjem tokena.[89]

3) Izrada sigurnosne kopije (engl. Backup)

Sigurnosno kopiranje podataka odnosi se na kopiranje fizičkih ili virtualnih datoteka ili baza podataka na sekundarnu lokaciju radi očuvanja u slučaju kvara opreme ili katastrofe.[90] Odličan primjer takve metode je 3-2-1 strategija za zaštitu podataka. Pravilo zahtjeva da korisnik sačuva tri primjerka važne datoteke, pohrani te kopije na dva različita medija, te spremi barem jednu sigurnosnu kopiju na udaljenoj lokaciji ili oblaku.[91] Postoje različita mjesta pohrane sigurnosne kopije:

- USB ili Flash pohrana predstavljaju oblik pohrane unutar kojeg se podaci lako mogu brisati ili mijenjati, te se ova vrsta pohrane treba koristiti ako je potreba jeftina, prijenosa i fizička

[88] Yıldırım, M., Mackie, I. (2019.), Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* **18**, 741–759
[89] European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I. (2022). *ENISA threat landscape 2022 – July 2021 to July 2022*, **https://data.europa.eu/doi/10.2824/764318**
[90] Gotseva, D., Gancheva, V., Georgiev, I., (2011). DATABASE BACKUP STRATEGIES AND RECOVERY MODELS, Technical University of Sofia, Faculty of Computer Systems and Control, Sofia, Bulgaria
[91] European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I. (2022.), *ENISA threat landscape 2022 – July 2021 to July 2022*, **https://data.europa.eu/doi/10.2824/764318**

pohrana
- CD/DVD je jednostavan i jeftin način sigurnosnog kopiranja podataka, ali je ograničen veličinom, odnosno megabajtima;
- Tvrdi disk fizički je odvojen od samog računala, prenosiv je i može pohraniti veću količinu podataka od samog CD-a, DVD-a i flash diskova;
- Pohrana podataka u oblaku predstavlja model usluge koji omogućuje jednostavno pohranjivanje datoteka na mreži, s mogućnošću pristupa putem Interneta. Podaci se čuvaju na vanjskom poslužitelju;

Ažurno provođenje sigurnosne kopije omogućuje korisnicima dodatan sloj zaštite u slučaju neželjenog događaja, kvara ili pretrpljenog napada, a kako bi se osigurala učinkovita sigurnosna kopija podataka, preporučuje se uspostaviti redovite rasporede sigurnosne kopije.[92]

4) Zaštita osobnih uređaja

Kako bi zaštitili svoje osobne uređaje, preporučene su sljedeće smjernice:
- Zaštita uređaja korištenjem lozinke bilo da se radi o zaštiti PIN-om, prepoznavanjem lica, tekstualnoj lozinki ili APL-om;
- Onemogućite skidanje aplikacije na mobilne uređaje bez unosa lozinke, na takav način spriječit ćete instaliranje neovlaštenih aplikacija na uređaj;
- Bluetooth ostavite isključenim kada se ne koristi. Bluetooth tehnologija djeluje tako da uređaji otkrivaju jedni druge, pomoću odašiljanja signala, kada su u neposrednoj blizini. Iz tog razloga uređaji su ranjivi i mogu pretrpjeti zlonamjerni napad ako je haker u blizini, bilo da se haker uspije povezati s uređajem bez dopuštenja korisnika ili slanjem niza zahtjeva za povezivanje koji ostavljaju telefon privremeno neupotrebljivim;[93]
- Antimalware/Antivirusna rješenja dizajnirana su za otkrivanje i uklanjanje virusa i drugih vrsta zlonamjernog softvera sa računala ili laptopa;
- Ažurno provođenje sigurnosne kopije podataka radi dodatnog sloja zaštite;
- Izbjegavanje korištenja javne Wi-Fi mreže za prijenos povjerljivih podataka kako bi se smanjio rizik od izlaganja različitim vrstama kibernetičkih napada;
- Korištenje VPN-a (engl. Virtual Private Network) pridonosi stvaranju sigurnosti i anonimnosti prilikom pregledavanja web stranica preko javnog Wi-Fi-ja, na način da sakriva

[92] Baylor Unyversity (2013.), Back Up Data https://www.baylor.edu/content/services/document.php/192120.pdf
[93] Padgette, J., Scarfone, K., Chen, L., (2012.), Guide to Bluetooth Security, National Institute of Standards and Technology

pravu IP adresu, a korištenjem VPN tunela omogućuje slanje i primanje informacija između korisničkog računala i udaljenog poslužitelja;[94]

- Ukoliko se koriste osobni mobilni uređaji prilikom obavljanja zadataka vezanih uz posao (praksa poznatija pod imenom engl. *Bring Your Own Device*) potrebno je postrožiti način pregledavanja uređaja, s obzirom da isti mogu imati različite operativne sustave, aplikacije s ugrađenim malwareom koje mogu ostaviti negativan utjecaj na informacijsku sigurnost poduzeća, a samim time povećati sigurnosne rizike;[95]

5) Rad od kuće

Koncept rada od kuće, rada na daljinu odnosno telework-a dobiva na popularnosti posljednje 3. godine početkom Covid pandemije. Istraživanja Help Net Security-ja pokazala su da je prelazak na rad od kuće povećao produktivnost zaposlenika te povećao stopu zadržavanja zaposlenika na radnome mjestu[96]. Unatoč navedenom rad na daljinu ne samo da je proširio potencijalnu površinu napada, već ju je i premjestio izvan konvencionalnih perimetarskih obrana, poput vatrozida i sustava za otkrivanje upada, koje su organizacije tradicionalno gradile za sprječavanje napada ransomwarea, povreda podataka i drugih vrsta kibernetičkog kriminala. Kako bi se spriječile ljudske pogreške koji predstavljaju primarnu prijetnju sigurnosnim podacima organizacije[97], navedene su smjernice i proaktivne mjere zaštite za stvaranje sigurnog okruženja:

- Zaštitite Wi-Fi mrežu snažnom i jedinstvenom lozinkom slijedeći smjernice koje su detaljno opisane u prethodnom dijelu uz obavezno korištenje VPN organizacije kako bi kriptirali vezu, te šifrirali podatke. Kao dodatan sloj zaštite preporučuje se korištenje više-faktorske autentifikacija
- Provođenje sigurnosne kopije podataka na sekundarnu lokaciju radi očuvanja u slučaju kvara opreme ili katastrofe.[98]
- Omogućavanjem kontrole pristupa, zaposlenici jamče svoj identitet prilikom pristupa aplikacijama i bazama podataka organizacije, a sustav ih automatski identificira, autentificira, te autorizira pristup.

[94] A. Alsayed, Nemah. (2015). Virtual Private Networks (VPN), Dar Al-Hekma University
[95] Hajdarevic, H., Allen, P., Spremić M., (2016.) Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments 1-4. 10.1109/TELFOR.2016.7818717
[96] Borkovich, D., Skovira, R., (2020.), Working From Home: Cybersecurity in the Age of Covid-19. Information Systems. 234-236.
[97] Borkovich, D., Skovira, R., (2020.), Working From Home: Cybersecurity in the Age of Covid-19. Information Systems. 234-236.
[98] Gotseva, D., Gancheva, V., Georgiev, I., (2011). DATABASE BACKUP STRATEGIES AND RECOVERY MODELS, Technical University of Sofia, Faculty of Computer Systems and Control, Sofia, Bulgaria

- Dodatna opreznosti pri korištenju elektroničke pošte i privicima koji su pridruženi samom sadržaju elektroničke pošte, potrebna je kako bi se zaštitili od zlonamjernih napada poput phishing mailova. Preporučuje se otvaranje poveznica koje su povezane s poslom kojeg se obavlja ili onih koji dolaze iz pouzdanih izvora.
- Ne dijelite osjetljive podatke putem elektroničke pošte osim ako isti nisu kriptirani ili sigurni.
- Uređaje zaštitite lozinkom ili softverom za zaključavanje zaslona koji koristi Bluetooth za provjeru jeste li unutar dometa uređaja, u protivnom zaslon se automatski zaključava[99]
- Pohađajte edukacije vezane za kibernetičku sigurnost omogućenih od strane organizacije, te se informirajte o najnovijim prijetnjama i trendovima dostupnima na gore navedenim publikacijama, portalima, te blogovima.[100]

[99] Mitnick, K. (2017.), The Art of Invisibility, Brown and Company
[100] Cyber Security Education (n.d.) CYBER CRIME IS ON THE RISE. WILL YOU ACCEPT THE CHALLENGE? Preuzeto 28. svibnja 2023 s https://www.cybersecurityeducation.org/

6 Zaključak

Kibernetička sigurnost predstavlja jedan od najvažnijih izazova suvremenog doba, a svijest o samoj važnosti kibernetičke sigurnosti ostaje ograničena.[101] Brzi tehnološki napredak i intenzivnija primjena informacijskih i digitalnih tehnologija povećali su ranjivost na kibernetičke napade, a samim time raste i potreba o podizanju svijesti i brušenju vještina o kibernetičkoj sigurnosti.[102] Kako bi pojedinci mogli implementirati određene mjere zaštite, potrebno je poznavati materiju same kibernetičke sigurnosti, kibernetičkih napada, prijetnji i rizika. Postoje različite definicije pojma kibernetičke sigurnosti, ali u suštini svaka od njih definira kibernetičku sigurnost kao zaštitu računala, računalnih mreža i informacijske imovine te uspostavu mjera kojima će se spriječiti ili ublažiti pojava prijetnji.[103][104][105] Kibernetički rizici proizlaze iz učestale uporabe informacijskih sustava i tehnologija, dok prijetnje uključuju interne prijevare, neovlaštene pristupe informacijama, hakerske napade, društvene inženjeringe itd.[106] Kibernetički napad predstavlja bilo koji nedozvoljeni pokušaj pristupa računalu, računalnom sustavu i računalnoj mreži s namjerom uzorkovanja štete, krađe, razotkrivanja ili uništavanja informacija putem neovlaštenog pristupa. Postoje dvije metode zaštite koje pojedinci mogu koristit pri zaštiti od rizika, prijetnji i kibernetičkih napada, a to su proaktivna i reaktivna metoda zaštite. Kao što samo ime govori proaktivna metoda uključuje proces prepoznavanja i rješavanja zlonamjernih aktivnosti, prije nego dođe do samog napada, dok je reaktivna metoda usmjerena na rješavanje tradicionalnijih napada, nakon što se napad izvršio.

Razumno je da je internet uvelike olakšao obavljanje svakodnevnih zadataka kao što su komunikacija, plaćanje računa putem modernih aplikacija, online kupovina, te učenje i rad na daljinu, te da s tim napretkom dolaze novi izazovi i rizici vezani uz kibernetičku sigurnost, koji

[101] De bruijn, H., Janssen M., (2017.), Building Cybersecurity Awareness: The need for evidence-based framing strategies, Government Information Quarterly, Volume 23, Issue 1, str. 1-7

[102] European Union Agency for Cybersecurity, Arcus, R., Sarri, A. (2021.), *Raising awareness of cybersecurity : a key element of national cybersecurity strategies*, (R.Arcus, editor, A.Sarri, editor) Publications Office of the European Union.

[103] European Union Agency for Cybersecurity,(2016.), Rannenberg, K., Gerber, B., Shamah, J. (2016). *Definition of cybersecurity : gaps and overlaps in standardisation*, European Network and Information Security Agency.

[104] Perković, P. (2022.), *Utjecaj Covid-19 pandemije na kibernetičku sigurnost* , Diplomski rad, Sveučilište u Zagrebu, Ekonomski fakultet

[105] Udruga za reviziju i kontrolu informacijskih sustava ISACA, (2016.), *Cybersecurity Fundamentals Glossary,* preuzeto 14 travnja 2023 s https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/cybersecurity_fundamentals_glossary.pdf?la=en&hash=B74D338B90ED9CEA1B4E05AABF40139EF692C866

[106] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.

često ostaju neprepoznati od strane općeg stanovništva. Sukladno s navedenim provodi se anketni upitnik, s ciljem utvrđivanja znanja i stanja svijesti stanovništva. Istraživački dio diplomskog rada donio je kvalitetne informacije koje su ukazale na izrazitu potrebu educiranja općeg stanovništva i podizanju svijesti o kibernetičkoj sigurnosti, te se zaključno navode smjernice i preporuke općem stanovištu kako bi se umanjile ljudske pogreške i pružio temelj za izgradnju sigurnijeg okruženja za opće stanovništvo.

Popis literature:

1. A. Alsayed, Nemah. (2015). Virtual Private Networks (VPN), Dar Al-Hekma University
2. Adams, M., (2013.), Wire Shark What is it & What is its purpose?, Illinois Institute of Technology
3. Arbanas. K, Spremić M., Zajdela Hrustek, N., (2020.) Holistic framework foe evaluating and improving information security culture, *Aslib Journal of Information Management*, 73 (5), 699-719 doi:10.1108/ajim-02-2021-0037.
4. Baylor Unyversity (2013.), Back Up Data https://www.baylor.edu/content/services/document.php/192120.pdf
5. Borkovich, D., Skovira, R., (2020.), Working From Home: Cybersecurity in the Age of Covid-19. Information Systems. 234-236.
6. Budin,L., Bajica,M., Carić, A., Čerić V., Glavinić V., Lovrek,I., Manger, R., Ursić, S., Hrvatska u 21. stoljeću, Informacijska i komunikacijska tehnologija, Ured za strategiju razvitka Republike Hrvatske, Zagreb, 2001 (ISBN 953-6430-23)
7. CARNet CERT–a i LS&S–a,. (2008.), Metodologija penetracijskog testiranja. 3-4. Hrvatska akademska i istraživačka mreža
8. Data Bridge Market Research. (2021.). Global Proactive Security Market Report. Preuzeto 7. svibnja 2023 s https://www.databridgemarketresearch.com/reports/global-proactive-security-market
9. De bruijn, H., Janssen M., (2017.), Building Cybersecurity Awareness: The need for evidence-based framing strategies, Government Information Quarterly, Volume 23, Issue 1, str. 1-7
10. Espinosa, N. (Speaker). (7 rujna 2018) The five laws of cybersecurity [Video]. TED Dostupno na: https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity
11. European Union Agency for Cybersecurity, preuzeto 15. travnja 2023 s https://www.enisa.europa.eu/about-enisa/about/hr
12. European Union Agency for Cybersecurity,(2016.), Rannenberg, K., Gerber, B., Shamah, J. (2016). *Definition of cybersecurity : gaps and overlaps in standardisation*, European Network and Information Security Agency.

13. European Union Agency for Cybersecurity, Arcus, R., Sarri, A. (2021.), *Raising awareness of cybersecurity : a key element of national cybersecurity strategies*, (R.Arcus, editor, A.Sarri, editor) Publications Office of the European Union.
14. European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I. (2022.), *ENISA threat landscape 2022 – July 2021 to July 2022*,
15. Gibson, C. (2021.). Cybersecurity Awareness: Tips to Protect Your Data. Spanning. https://spanning.com/blog/cybersecurity-awareness/https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436
16. glaGotseva, D., Gancheva, V., Georgiev, I., (2011). DATABASE BACKUP STRATEGIES AND RECOVERY MODELS, Technical University of Sofia, Faculty of Computer Systems and Control, Bulgaria
17. Gulen, K., (2022). Cyber espionage remains a real threat to both governments and business, Dana Economy, dostupno na: https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/?utm_content=cmp-true
18. Hajdarevic, H., Allen, P., Spremić M., (2016.) Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments 1-4. 10.1109/TELFOR.2016.7818717
19. Hercigonja, M. (2019). *Kibernetska sigurnost : Stručni završni rad* (Završni rad). Zaprešić: Veleučilište s pravom javnosti Baltazar Zaprešić
20. Hrůza, P., Cerny, J., (2017.), Cyberwarfare. International conference KNOWLEDGE-BASED ORGANIZATION. 23. 10.1515/kbo-2017-0024
21. Hrvatski institut za kibernetičku sigurnost, preuzeto 5. svibnja 2023 s https://hiks.hr/
22. Jalali, M.S.(2018.) Journal of Strategic Information Systems, Volume 28, Issue 1, Pages 66-82
23. Kallberg, Jan. (2018). Cyberespionage, SAGE Publications, Inc
24. Klopfer,F., Rizmal, I., Sekuloski, M., Hatzl, T., Mladenovic, D., (2019.) Introduction to Cybersecurity Governance – A tool for Members of Parliament
25. Kwon, J., Johnson, M. E. (2011, June). An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security. In *WEIS*.
26. Liao, S, Zhou, C., Zhao, Y., Zhang, Z., Zhang, C., Gao, Y., Zhong, G., (2020). A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments, Huazhong University of Science and Technology, China

27. McCarty, B., (2021), Email Security: Turn Your Weakest Link Into Your Strongest Line Of Defense preuzeto 5. svibnja 2023 s https://www.forbes.com/sites/forbestechcouncil/2021/06/22/email-security-turn-your-weakest-link-into-your-strongest-line-of-defense/?sh=32feaa933ce2
28. Mejovšek, M. (2013). Metode znanstvenog istraživanja u društvenim i humanističkim znanostima. Jastrebarsko: Naknada Slap
29. Mitnick, K. (2017.), The Art of Invisibility, Brown and Company
30. National Cyber Security Centre (n.d.) Dostupno na; https://www.ncsc.gov.ie/
31. Ncubukezi, T. (2022.), Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security. (395-403.)
32. Padgette, J., Scarfone, K., Chen, L., (2012.), Guide to Bluetooth Security, National Institute of Standards and Technol
33. Pande, J. (2017.), Introduction to Cyber Security, Uttarakhand Open University
34. Rotim, A. (2017). *Društvene mreže i slobodno vrijeme: ovisnost ili stil života?* Diplomski rad, Fakultet političkih znanosti, Zagreb
35. Spremić, M.,(2012.), Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks , Ekonomski fakultet, Zagreb.
36. Spremić M., (2013.), Holistic Approach for Governing in Information System security, Lecture Notes in Engineering and Computer Science. 2. 1242-1247.
37. Spremić, M (2007.), Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta u Zagrebu,
38. Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet, Zagreb.
39. Spremić, M., Šimunić A., (2018.), *Cyber Security Challenges in Digital Economy* In *World Congress on Engineering WCE*. Vol. vol. I. London, UK,
40. Statista (2023.), Annual number of malware attacks worldwide from 2015 to 2022 preuzeto 6. svibnja 2023 s https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
41. *The International Criminal Police Organization*, INTERPOL : U.S. National Central Bureau, Washington, D.C. : point of contact for international law enforcement. (2002.). [Washington, D.C.] :U.S. Dept. of Justice : U.S. Dept. of the Treasury,(2020) INTERPOLreport shows alarming rate of cyberattacks during COVID; preuzeto 14.

travnja 2023. s https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

42. Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (2007.) Guidelines on Electronic Mail Security, National Institute of Standards and Technology
43. Thompson, E., (2020.), Threat Hunting, HIPPA, Compliant Security Operation Centar
44. Udruga za reviziju i kontrolu informacijskih sustava ISACA, (2016.), *Cybersecurity Fundamentals Glossary,* preuzeto 7. svibnja 2023 s https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/cybersecurity_fundamentals_glossary.pdf?la=en&hash=B74D338B90ED9CEA1B4E05AABF40139EF692C866
45. United Nations General Assembly. (2002), The role of the United Nations in the field of information and telecommunications in the context of international security.
46. Ured Vijeća za nacionalnu sigurnost Republike Hrvatske, preuzeto 15. svibnja 2023 s https://www.uvns.hr/hr/informacijska-sigurnost/kiberneticka-sigurnost
47. Vanparia, P., Ghodasara, Y., Donga, H., (2015.), Network Protocol Analyzer with Wireshark. Developeriq.in
48. VISHNEVETSKY, G.,(2022), *Passwords Are Key to Cyber Security,* preuzeto 14. travnja 2023 https://www.stewart.com/en/insights/2022/passwords-are-key-to-cyber-security.html
49. Vujević, M., (2002.), Uvođenje u znanstveni rad u području društvenih znanosti. Zagreb: Školska knjiga (str. 20- 55).
50. Yıldırım, M., Mackie, I. (2019.), Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* **18**, 741–759
51. Zakon o nacionalnoj strategiji kibernetičke sigurnosti, Narodne novine, br. 108/15 (2016.)
52. Žmuk, B. (2019.), Najčešći problemi i izazovi u provođenju poslovnih web anketa, Ekonomski fakultet Sveučilište u Zagrebu.

Popis ilustracija

ŽIVOTOPIS

europass

Marta Končarević

Državljanstvo: hrvatsko **Datum rođenja:** 19 ruj 1997 **Spol:** Žensko

Telefonski broj: (+385) 995141917 **E-adresa:** mkoncarev@net.efzg.hr

Kućna: obala kneza Branimira 10, 23000 Zadar (Hrvatska)

RADNO ISKUSTVO

Prodavačica odjeće, obuće i galanterije
Topaz d.o.o [15 lip 2022 – 1 ruj 2022]

Mjesto: Zadar
Zemlja: Hrvatska

– Rad na blagajni
– Rad s kupcima
– Prodaja robe
– Dnevni obračun blagajne
– Inventura

Prodavačica
Sfinga d.o.o [1 srp 2021 – 15 ruj 2021]

Mjesto: Zadar
Zemlja: Hrvatska

– Rad na blagajni
– Rad s kupcima
– Prodaja suvenira, nakita i torbi
– Dnevni obračun blagajne
– Inventura

Rad u turizmu
Apartman Nata [1 svi 2017 – 1 lis 2020]

Adresa: (Hrvatska)
Zemlja: Hrvatska
Poduzeće ili sektor: Usluge Smještaja I Gastronomija

– Sezonski posao
– Priprema apartmana
– Rad s turistima
– Prijava i odjava turista

OBRAZOVANJE I OSPOSOBLJAVANJE

UiPath
Faculty of Economics & Business Zagreb [svi 2022]

Adresa: (Hrvatska)

Process Mining - Fundamentals for Students Training
Celonis [stu 2021]

Elements of AI
University of Helsinki [sij 2021]

Course EU Data sources
Faculty of Economics & Business Zagreb [ožu 2018]

Organize Your Talk - competition in presentation skills in English
Faculty of Economics & Business Zagreb [11 svi 2018]

JEZIČNE VJEŠTINE

Materinski jezik/jezici: **Hrvatski**

Drugi jezici:

Engleski	**talijanski**
SLUŠANJE C1 **ČITANJE** C1 **PISANJE** C1	**SLUŠANJE** A2 **ČITANJE** A2 **PISANJE** A2
GOVORNA PRODUKCIJA C1	**GOVORNA PRODUKCIJA** A2
GOVORNA INTERAKCIJA C1	**GOVORNA INTERAKCIJA** A2

DIGITALNE VJEŠTINE

Canva / Poznavanje rada u Microsoft Office programima (Word PowerPoint Excel) / Poznavanje MS Office-a (Excel, Word, Powerpoint..) / SQL bazama podataka (SQLyog) / UML, BPMN