Utjecaj Covid-19 pandemije na kibernetičku sigurnost

Perković, Petra

Master's thesis / Diplomski rad

2022

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:148:978023

Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

UTJECAJ COVID-19 PANDEMIJE NA KIBERNETIČKU SIGURNOST

Diplomski rad

Petra Perković

Zagreb, rujan, 2022.

Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

UTJECAJ COVID-19 PANDEMIJE NA KIBERNETIČKU SIGURNOST

IMPACT OF COVID-19 PANDEMIC ON CYBER SECURITY

Diplomski rad

Petra Perković, 0067567525

Mentor: Prof. dr. sc., Mario Spremić

Zagreb, rujan, 2022.

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)

Sažetak i ključne riječi

Područje kibernetičke sigurnosti iznimno je važno područje, a pojavom pandemije korona virusa navedeno područje dobiva na važnosti i primjeni. Adekvatno upravljanje kibernetičkom sigurnosti temelj je svake uspješne organizacije. Ipak, mnoge organizacije te njihovi zaposlenici, prije pojave pandemije korona virusa, nisu imale uspostavljene potrebne kontrole upravljanja kibernetičkom sigurnosti niti mogućim rizicima. Zbog pojave COVID-a 19 i neefikasnih kontrola i mjera mnoge su organizacije bile mete kibernetičkih napada. Izostala je edukacija i pravovremeno informiranje zaposlenika. U ovom radu osvrće se na probleme koji su bili ključni okidači pojave novih kibernetskih prijetnji, kao što su nedovoljna informiranost, manjak resursa i vremena, nove metode i pristupi poslovanja kao što je rad od kuće. Kako bi se dokazalo da se u pandemijskome razdoblju povećao broj kibernetičkih napada, da mnogi zaposlenici i dalje rade od kuće te da se programi podizanja svijesti o kibernetičkoj sigurnosti ne provode dovoljno često, provedeno je istraživanje na zaposlenicima odjela IT-a i odjela informacijske sigurnosti. Kako bi kibernetička sigurnost postala prioritet organizacijama u ovim nesigurnim vremenima, potrebno je promijeniti perspektivu menadžera i zaposlenika te se u ovom radu pokušava osvijestiti potreba za širim gledanjem na područje kibernetičke sigurnosti, izvan okvira. Kibernetički kriminalci, hakeri i ostali napadači iskorištavaju i najmanju ranjivost informacijskog sustava, a njihove metode postaju sve sofisticiranije. Kibernetički svijet i okruženje se svakodnevno mijenja stoga je nužno da se promjene i pristupi prema kibernetičkoj sigurnosti.

Ključne riječi: kibernetička sigurnost, kibernetički napadi, pandemija, COVID-19

Summary and key words

Cyber security is crucial, and with the events of the coronavirus pandemic, the said area is gaining in importance and application. Adequate cyber security management is the foundation of any successful organization. However, many organizations and their employees, before the onset of the coronavirus pandemic, did not have the necessary controls in place to manage cyber security or possible risks. Many organizations were the targets of cyberattacks as a result of the emergence of COVID-19 and ineffective controls and measures. There was a lack of education and timely information for employees. This paper looks at the problems that were the key triggers for the emergence of new cyber threats, such as insufficient information, lack of resources and time, and new business methods and approaches, such as working from home. A survey was conducted on employees of the IT department and the information security department to prove that the number of cyberattacks increased during the pandemic period, with many employees still working from home, and that cyber security awareness programs are not conducted often enough. For cyber security to become a priority for organizations in these uncertain times, it is necessary to change the perspective of managers and employees, and this paper tries to raise awareness of the need for a broader view of the field of cyber security, outside the box. Cybercriminals, hackers, and other attackers exploit even the smallest vulnerabilities in the information system, and their methods are becoming more and more sophisticated. The cyber world and its environment are changing every day, so it is necessary to change approaches to cyber security.

Keywords: cyber security, cybersecurity, cyberattacks, pandemic, COVID-19

Sadržaj

1. Uvod

Od početka pandemije korona virusa započeo je trend masovnog rada na daljinu, tj. „rada od kuće“. Vijest o pojavi virusa, kao i sam virus, zahvatio je sve dijelova svijeta, sve grane djelatnosti, razna područja pa tako i područje kibernetičke sigurnosti. Povećanjem broja zaposlenika koji su tijekom pandemije započeli rad na daljinu, tj. „rad od kuće“, povećao se i broj kibernetičkih napada. Budući da se utjecaj ove i dalje nove pandemije ne smanjuje, dolazi do pojave novih rizika u svakodnevnom poslovanju. Mnoge tvrtke bile su prisiljene prijeći na nove načine rada u što kraćem roku. Unutar tog razdoblja izostavila se izrazito nužna edukacija zaposlenika kao i ulaganja u informacijsku sigurnost i što sigurniji rad od kuće. Hakeri su iskoristili, i dalje iskorištavaju, ranjivosti koje su im pružile mogućnost puno lakših i jednostavnijih napada na računalne sustave. S obzirom na sve navedeno, izrazito je važno istaknuti potencijalne propuste koji su doveli do kibernetičkih napada od pojave pandemije do danas te izvući bitne prijedloge i smjernice za poboljšanje postojećih procesa.

1.1. Predmet i ciljevi diplomskog rada

Predmet ovog diplomskog rada veže se uz izrazito aktualno područje, kibernetičku sigurnost. Posebna pozornost obratit će se na utjecaj korona virusa na cijelu ekonomiju, a posebno na područje informatičke sigurnosti. S obzirom na to da je ova pandemija negativno zahvatila razne ekonomske djelatnosti, cilj ovog diplomskog rada je prikazati negativan utjecaj virusa na kibernetičku sigurnost u svim granama djelatnosti. Međutim, pojam kibernetičke sigurnosti nije svima jasan, stoga će se u ovom diplomskom radu pobliže objasniti kibernetička sigurnost, aspekti koje obuhvaća, što se podrazumijeva pod samim pojmom kibernetičke sigurnosti i koji sve napadi na računalne sustave postoje. Također će se temeljito obraditi hipoteza da se povećao broj kibernetičkih napada od početka pandemije do danas, te da organizacije, bez obzira na iznimno brzu prilagodbu novom načinu rada od kuće, nisu dovoljno uložile u zaštitu računalnih sustava kao i povezanih resursa.

1.2. Metode istraživanja i izvori podataka

Kao primarni izvori podataka, prilikom pisanja ovog diplomskog rada, koriste se znanstveni članci iz područja informacijske sigurnosti te knjige odabranih autora. Temeljem prikupljenih podataka kao i analizom istih te pomoću istraživanja formirat će se sud i vlastito

mišljenje vezano uz temu utjecaja COVID-19 pandemije na kibernetičku sigurnost. Provest će se anketni upitnik među zaposlenicima odjela IT-a i odjela informacijske sigurnosti raznih Društava te će se ispitati njihova svijest o potencijalnim kibernetičkim napadima unutar Društva u kojem rade, u razdoblju od početka pandemije do danas.

1.3. Sadržaj i struktura rada

Struktura ovog rada definirana je prema unaprijed zadanim akademskim pravilima. Diplomski rad se sveukupno sastoji od 6 poglavlja s pripadajućim potpoglavljima. Rad započinje uvodom u kojem se u kratkim crtama pojašnjava značaj ovog rada te izvori koji su poslužili u formiranju rada. Nakon uvoda u kojem se kratko pojašnjava što se sve obrađuje u diplomskom radu, u drugom poglavlju definira se sam pojam kibernetičke sigurnosti, važnost i utjecaj u 21. stoljeću. Pobliže se objašnjavaju aspekti kibernetičke sigurnosti te se u kratim crtama referira na Zakon o kibernetičkoj sigurnosti kako bi se dočarala važnost ovog područja i ulaganje u isto. Nadalje, unutar sljedećih potpoglavlja definirat će se vrste kibernetičkih napada, njihova učestalost te će se obraditi neki od većih i izrazito bitnih kibernetičkih napada na organizacije u različitim sektorima. Unutar drugog poglavlja osvrnut će se na mitove o kibernetičkoj sigurnosti. U idućem poglavlju definirat će se pojam COVID-19 pandemije, tj. koronavirusa te će prikazati povezanost između koronavirusa i kibernetičke sigurnosti. Definirat će se ranjivosti koje su se pojavile unutar pandemijskog razdoblja te referirati na neke od prijetnji koje su se dogodile od pojave koronavirusa do danas. U četvrtom poglavlju sve hipoteze prikazat će se istraživanjem koje će se provesti među zaposlenicima raznih Društava te će se ispitati njihova svijest o potencijalnim kibernetičkim napadima unutar Društva u kojem rade, u razdoblju od početka pandemije do danas. U predzadnjem poglavlju pažnja se daje rješenjima te kontrolama koje su nužne kako bi se smanjio broj kibernetičkih napada te kako bi se Društva unaprijed bolje pripremila na iste te će se iznijeti zaključak diplomskog rada.

2. Uvod u kibernetičku sigurnost

Danas smo suočeni s aktivnom primjenom informacijske i digitalne tehnologije te s korištenjem suvremenih informacijskih sustava koji se u svome radu posebno oslanjaju na spomenutu tehnologiju budući da im primjena iste omogućava efikasniju provedbu transakcija (Spremić, 2017). Primjena informacijske tehnologije u svakodnevnom poslovanju mijenja procese, čini ih boljima i inovativnijima te pomaže poduzećima da lakše i brže uvedu nove proizvode i usluge. Međutim, intenzivna primjena ovih tehnologija, bez obzira na brojne prednosti, izlaže poduzeća i pojedince novim te neželjenim opasnostima i rizicima. Rizici koji se ovdje javljaju nazivaju se informatički rizici (engl. IT risks), a prema Spremić (2017, str. 61) to su „poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće." Kibernetički rizici su podskup informatičkih rizika, međutim, u navedenom kontekstu, svi informatički rizici ujedno su i kibernetički (Spremić, 2017).

2.1. Značaj i aspekti kibernetičke sigurnosti

Pojam kibernetičke sigurnosti i dalje je nepoznanica za mnoge pojedince, ali i poduzeća. Mnogi pojedinci pretpostavljaju da je kibernetička sigurnost novi pojam koji se relativno počeo spominjati u posljednjem desetljeću. Međutim, povijest kibernetičke sigurnosti seže u sedamdesete godine, prije nego što je većina ljudi uopće posjedovala računala.

U današnje vrijeme kada je cijeli svijet zahvatila pandemija COVID-a 19 (više o navedenome u poglavlju 3.) i kada su sva poduzeća neželjeno doživjela velike promjene u svom poslovanju, kibernetička sigurnost trebala bi biti jedna od važnijih tema. Postoje različite definicije kibernetičke sigurnosti te se javlja problem nedostatka dosljednog značenja navedenog pojma. Pojam kibernetičke sigurnosti nije jednako definiran kroz stručnu, akademsku i državnu literaturu. Međutim, većina definicija sadrži iste ključne komponente koja označavaju jednaka stajališta o ovom pojmu, a to je da je ključni cilj kibernetičke sigurnosti uspostava mjera koje će spriječiti ili ublažiti pojavu prijetnji. Udruga za reviziju i kontrolu informacijskih sustava ISACA (engl. *Information System Audit and Control Association*) u svome rječniku pojmova navodi da se kibernetička sigurnost odnosi na zaštitu informacijske imovine rješavanjem prijetnji informacijama koje se obrađuju,

pohranjuju i prenose putem umreženih informacijskih sustava. Spremić (2017) navodi da kibernetička sigurnost obuhvaća sve mjere kontrole i zaštite koje pojedince i poduzeća štite od informatičkih napada koje je teško otkriti ili spriječiti. Važno je napomenuti kako dobro upravljanje kibernetičkom sigurnosti uključuje korištenje raznih alata, primjenu pravilnika, sigurnosnih mjera te smjernica kao i različite aktivnosti i akcije. Sukladno navedenome potrebna su obučavanja, primjena najboljih praksi i tehnologije kako bi se moglo zaštititi kibernetičko okruženje. Dodatno, prema Zakonu o kibernetičkoj sigurnosti, (NN 64/2018) kibernetička sigurnost definirana je kao „sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru."

Značenje i upravljanje kibernetičkom sigurnosti u današnje vrijeme predstavlja temelj za stabilan i siguran informacijski sustav kao i njegovo okruženje. Važnost se očituje u identificiranju prijetnji, propusta i pogrešaka koje mogu negativno utjecati na poslovanje.

Prema Spremić (2017), informatički rizici su uvijek prisutni te imaju dualnu narav što bi značilo da ako su informatičke inicijative dobro vođene – stvaraju vrijednost, nove prilike te konkurentsku prednost, a ako su loše vođene – uništavaju poslovanje, troše resurse te stvaraju gubitke. Informatički, kao i kibernetički rizici proizlaze iz djelovanja prijetnji, a one se, s obzirom na mjesto nastanka, dijele na unutarnje i vanjske. Razlika je u tome što unutarnje proizlaze iz poduzeća npr. nesvjesno odavanje povjerljivih informacija, a vanjske izvan poduzeća npr. pandemija korona virusa. Spremić (2017) navodi kako su glavne internetske prijetnje danas kibernetički kriminal, kibernetička industrijska špijunaža te kibernetičko ratovanje.

2.1.1. Zakon o kibernetičkoj sigurnosti

U Republici Hrvatskoj postoje brojni zakoni i uredbe koji uređuju područje informacijske i kibernetičke sigurnosti, a to su: Zakon o informacijskoj sigurnosti te pripadajuća Uredba i Pravilnici, Zakon o sigurnosnim provjerama te pripadajuća Uredba, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga s pripadajućom Uredbom te Smjernicama, Nacionalna strategija kibernetičke sigurnosti itd.

Kako se povećavaju zahtjevi iz područja kibernetičke sigurnosti tako se povećava i broj direktiva i uredbi. Sukladno navedenome, na razini Europske unije usvojena je NIS direktiva

(engl. Network and Information Security Directive) kojom su se definirali ključni zahtjevi i mjere. Pomoću definiranih zahtjeva i mjera omogućava se djelotvoran rad i postizanje visoke razine sigurnosti kako mrežnih tako i informacijskih sustava. Navedena direktiva preuzeta je i u hrvatsko zakonodavstvo putem Zakona o kibernetičkoj sigurnosti koji se primjenjuje od 2018. godine. Na temelju Zakona donesena je i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Godinu dana nakon, izrađen je i „Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona i provođenje ocjene sukladnosti“ čija je prvobitna namjena da služi kao implementacijski vodič za operatore ključnih usluga, ali i da služi kao vodič za nadležna tijela.

Prema okviru dobrih praksi, operatori bi trebali biti sukladni sa člancima navedene Uredbe, a oni obuhvaćaju uspostavu i dokumentiranje politike primitaka, provedbu internih nadzora, uspostavu sustava upravljanja rizicima te procjenu rizika, sprječavanje, otkrivanje i rješavanje incidenata te ublažavanje učinka incidenta, zaštitu od zlonamjernog programskog koda itd. Zakon se primjenjuje na osam sektora, a to su energetika, bankarstvo, prijevoz, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura te poslovne usluge za državna tijela.

Za omogućavanje učinkovite provedbe svih Zakona zaslužne su institucije koje djeluju na području informacijske sigurnosti, a najvažnije od njih su Nacionali CERT, Ured Vijeća za nacionalnu sigurnost – UVNS, Zavod za sigurnost informacijskih sustava – ZSIS, Agencija za zaštitu osobnih podataka – AZOP i Sigurnosno obavještajna agencija – SOA.

2.2. Informacijska sigurnost/kibernetička sigurnost/sigurnost informacijskih sustava

Kako bi se preciznije definirao pojam kibernetičke sigurnosti potrebno ga je usporediti s pojmovima informacijske sigurnosti i sigurnosti informacijskih sustava. Svi navedeni pojmovi svakako su međusobno povezani, no postoje i ključne razlike koje ih odvajaju.

Informacijska sigurnost prema Spremić (2017) uključuje tri parametra koja predstavljaju njezin temelj, a to su:

1. povjerljivost,
2. integritet/cjelovitost,

3. raspoloživost/dostupnost.

Kada govorimo o navedena tri parametra često se znamo susresti s pojmom CIA trijade (engl. Confidentiality, integrity and availability triad) što označava kraticu ovih pojmova na engleskome jeziku. Mjere povjerljivosti označavaju zaštitu informacija od neovlaštenog osoblja, odnosno govorimo o sigurnom pristupu informacijama kojima je moguće pristupiti samo ako ste za to ovlaštena osoba (Spremić, 2017). Bitno je voditi računa da sve informacije unutar određenog poduzeća imaju svoju vrijednost i da su sklone ranjivostima. Mjere integriteta ili cjelovitosti označavaju zaštitu cjelovitosti informacija koje se obrađuju i kojima je omogućen pristup, odnosno ovim mjerama informacije se štite od izmjene (Spremić, 2017). Kada govorimo o integritetu i cjelovitosti važno je da zaposlenici mogu mijenjati samo one podatke za koje su ovlašteni, odnosno kojima imaju pristup sukladno svojim ovlaštenjima. Mjere raspoloživosti ili dostupnosti omogućavaju da zaposlenici imaju stalan i nesmetan pristup onim podacima i informacijama za koje su ovlašteni. Upravljanje informacijskom sigurnošću uvelike ovisi o resursima organizacije te o procjeni događaja vjerojatnosti prijetnje ili ranjivosti te je važno napomenuti da su sve mjere koje se poduzimaju s ciljem očuvanja informacijske sigurnosti zapravo rutinske mjere niže razine zrelosti (Spremić, 2017).

Pojam kibernetičke sigurnosti objašnjen je u poglavlju 2.1., a nasuprot navedenome o informacijskoj sigurnosti, kibernetička sigurnost se isključivo odnosi na stvarne, a ne procijenjene prijetnje što označava da su ovakve prijetnje vrlo ozbiljne i dolaze od strane vrlo iskusnih napadača. Samim time, mjere za očuvanje kibernetičke sigurnosti su više razine zrelosti kako bi se moglo efikasno i cjelovito upravljati sa informacijskim sustavom i osigurati visoku razinu zaštite istoga, a bitno je naglasiti da cilj kibernetičke sigurnosti nije samo otkloniti rizike i prijetnje nego ih i previdjeti (Spremić, 2017).

Prema Zakonu o informacijskoj sigurnosti (NN 79/2007), sigurnost informacijskih sustava označava „područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.“ Spremić (2017) navodi da se provedbom navedenih

mjera smanjuju mogući informatički rizici, a sama sigurnost informacijskih sustava očituje se ispunjavanjem sigurnosnih zahtjeva:

i. Zahtjev sigurnosti - veže se na prvi od tri parametra informacijske sigurnosti, a to je povjerljivost, budući da se ispunjavanjem ovoga zahtjeva osigurava nesmetan rad sustava.
ii. Zahtjev raspoloživosti – veže se na zadnji parametar informacijske sigurnosti, dostupnost, jer se ispunjavanjem ovoga zahtjeva osigurava da su informacije koje se obrađuju i kojima se pristupa, dostupne i raspoložive samo onim zaposlenicima koji za to imaju ovlasti.
iii. Zahtjev tajnosti – osigurava da su tajni i povjerljivi podaci dostupni samo određenom broju privilegiranih korisnika.

Sukladno navedenome, važno je da organizacije budu svjesne razlika i sličnosti između navedenih pojmova kako bi efikasno mogle upravljati svojim informacijskim sustavima.

2.3. Kibernetske prijetnje i napadi

Prethodno je već spomenuto kako su se kibernetički napadi, ali i rizici povećali u pandemijskome razdoblju koje do danas obuhvaća otprilike dvije godine (2020.-2022.)

Prema ISACA izvješću o stanju kibernetičke sigurnosti (2021) najčešći kibernetički napadi u 2021. godini odnosili su se na:

- društveni inženjering (engl. Social engineering) – 14%,
- napredne ustrajne prijetnje (engl. Advanced persistent threat, ATP) – 10%,
- ucjenjivački softver (engl. Ransomware) – 9%,
- nezakrpani softver – 9%,
- napade uskraćivanjem usluge (engl. Denial of service, DoS) – 8%,
- napade pogrešne konfiguracije sigurnosti (engl. Security misconfiguration) – 8%.

Spremić (2017) definira društveni inženjering kao krađu osobnih podataka žrtve putem manipulacije na temelju kojih se onda čine različite zloupotrebe istih, npr. lažno predstavljanje. Ucjenjivački softver odnosi se na neovlašteni upad u računalo prilikom kojeg se podaci nužni za poslovanje kriptiraju, a računalni kriminalci za dekriptiranje traže

određeni iznos otkupnine (Spremić, 2017). Nezakrpani softver je zapravo računalni kod koji sadrži razne sigurnosne slabosti koje zatim napadačima omogućuju da iskoriste nezakrpanu grešku pokretanjem zlonamjernog koda. Napade uskraćivanjem usluge, Spremić (2017) svrstava u napade usmjerene na onemogućavanje rada, a definira kao nedopuštene aktivnosti kojima se iskorištavanjem resursa programa, računalne mreže ili sustava (memorija, propusnost, itd.) sprječava i/ili onemogućuje ovlaštena uporaba istih. Pogrešne konfiguracije sigurnosti, kao što i sama riječ govori, odnose se na neuspjeh organizacije da implementira sve sigurnosne kontrole ili da implementacija uključuje pogreške. Centar informacijske sigurnosti (2011) u svom izvješću definira napredne ustrajne prijetnje kao „ustrajne i djelotvorne napade na određeni subjekt." Napadači su obično organizirana skupina ljudi, a napadi traju dulje vremensko razdoblje i ciljaju na točno određene računalne sustave.

Akteri prijetnje općenito se definiraju kao osobe/entiteti odgovorni za incident koji utječe ili ima potencijal utjecati na sigurnost organizacije (Sailio, Latvala i Szanto, 2020).

Prema Sailio, Latvala i Szanto (2020), akteri prijetnje dijele se na:

Akter prijetnje	**Ciljevi aktera prijetnje**
Kibernetički kriminalci	Ciljevi su im izvući vrijednost (novac, vrijedne podatke) i izbjeći pravne posljedice na način da se infiltriraju u mreže koristeći bilo koju dostupnu i iskoristivu ranjivost.
Akteri nacionalne države	Cilj im je prikupljanje obavještajnih podataka ili podrška nacionalnim interesima (npr. prijenos tehnologije).
Ideolozi (haktivisti i teroristi)	Iako su načini djelovanja haktivista i terorista vrlo različiti, oba su aktera ideološki motivirana.
Tragači za uzbuđenjem	Napadaju računalne sustave s ciljem dokazivanja, učenja ili eksperimentiranja. U ranijim godinama bili su poznati pod širim pojmom haker ili haker s bijelim šeširom.

Insajderi (osobe unutar organizacije)	Mogu se podijeliti u dvije kategorije: insajder plaćenik i nezadovoljni zaposlenik. Insajder plaćenik prodaje pristup mreži drugim akterima, dok nezadovoljni zaposlenik uzrokuje probleme organizaciji zbog nezadovoljstva.
Konkurenti	Cilj im je pridobiti što više informacija o snažnijim konkurentima.
Partneri	Koriste povjerenje kao polugu za društveni inženjering.

Tablica 1 Akteri prijetnje kibernetičkoj sigurnosti

Izvor: samostalna izrada autorice rada

Tijekom razdoblja pandemije napadači su usvajali nove strategije te je njihova taktika napada postala nepredvidljiva stoga će se organizacije morati nositi s rastućim sigurnosnim zahtjevima koji proizlaze iz povećanog rizika od kibernetičkih napada (Khan, Brohi i Zaman, 2020).

2.3.1. Najčešće vrste napada te učestalost napada prije COVID-19

Definirani su najučestaliji napadi tijekom 2021. godine koji se odnose na razdoblje pandemije. Kako bi se uočila razlika u napadima prije i tijekom pandemije, definirani su i najučestaliji napadi tijekom 2019. godine.

ISACA izvješće o stanju sigurnosti iz 2019. godine navodi da su krađa identiteta (engl. phishing), zlonamjerni softver (engl. malware) i društveni inženjering na vrhu popisa najučestalijih vrsta napada, a bili su na istom mjestu i prethodne dvije godine. Navedeno ne označava da krađa identiteta i zlonamjerni softveri nisu prisutni u pandemijskome razdoblju. Spremić (2017) definira phishing kao krađu identiteta, odnosno phishing obuhvaća sve aktivnosti kojima je cilj osigurati pristup povjerljivim podacima (npr. broj kreditne kartice, šifra i sl.). Kriminalci koriste razne metode kako bi pristupili povjerljivim podacima, a kada je riječ o phishing-u najčešće korištena metoda su lažne elektroničke poruke. Lažne elektroničke poruke mogu sadržavati različite privitke ili linkove koji sadržavaju zlonamjerne računalne programe, npr. malware. Zlonamjerni softveri su virusi koji

ugrožavaju informacijske sustave te se mogu inficirati u druge sustave, mijenjati ih i lako proširivati. Oni u sustave ulaze tajno, a cilj im je da prouzroče što veću štetu, odnose ugroze informacijski sustav (Spremić, 2017).

U navedenome izvješću također je definirano kako su kibernetički napadi 2018. i 2019. godine doživjeli blagi pad, odnosno kako je 2018. godina bila godina stabilizacije prijetnji i aktera napada.

Jedan od razloga povećanja broja kibernetičkih napada u pandemijskome razdoblju sigurno je i nepovjerenje u sposobnost tima za kibernetičku sigurnost da otkrije i odgovori na kibernetičke prijetnje. Organizacije se, uz navedeno, suočavaju i s nedovoljnim brojem kompetentnih stručnjaka za kibernetičku sigurnost. Svakako treba uzeti u obzir da su mnogi incidenti kibernetičkih napada prošli neprijavljeni, kako u prethodnim godinama, tako i danas.

2.3.2. Primjeri velikih napada na organizacije u različitim sektorima

I prije pandemije COVID-a 19 mnoge organizacije bile su žrtve kibernetičkih kriminalaca i ostalih aktera prijetnji te su neke doživjele velike gubitke za svoje poslovanje. Velike povrede podataka postaju sve češće, jer kao što je već spomenuto hakeri postaju sve sofisticiraniji. Kibernetički napadi nemaju samo negativan utjecaj na organizaciju koju zahvate, nego i negativan utjecaj na kupce, klijente, dioničare, partnere i zaposlenike. U nastavku su opisana dva slučaja kibernetičkih napada na organizacije prema DesJardins, (2014):

Primjer 1. Target

Target Korporacija je američki lanac robnih kuća osnovan 1902. godine i iza sebe ima uspješno, dugogodišnje poslovanje. Target pohranjuje financijske podatke više od milijuna svojih kupaca svake godine i bila je potrebna iznimno jaka zaštita informacijskog sustava kako bi se zaštitile velike količine podataka s kojima su poslovali. No, u prosincu 2013. godine Target je bio meta iskusnih hakerskih napadača koji su 2. prosinca počeli preuzimati podatke s Target-ovih terminala na prodajnim mjestima. Hakerima je posao olakšan budući da Target nije imao u potpunosti uspostavljen sigurnosni softver, odnosno softver je bio u fazi testiranja. Bez obzira na razna upozorenja od strane softvera, koji je uočio proboj u sustav, Target-ov tim nije se obazirao te je proboj uočen tek 10 dana nakon.

U međuvremenu, hakeri su uspjeli prikupiti podatke za više od 40 milijuna debitnih i kreditnih kartica. Podatke su prikupili pomoću „RAM scraping“ procesa (engl. Random Access Memory scraping), a to je oblik pohrane računalnih podataka kojeg koriste sustavi na prodajnom mjestu. Ono što je hakerima bio cilj s prikupljenim podacima je da ih prodaju na internetu preko hakerskih internetskih stranica, a nakon kupnje podaci se mogu pretvoriti u fizičke kartice koje se zatim mogu prodati na crnom tržištu. Zbog prespore reakcije Target-ovih zaposlenika, hakeri su dodatno uspjeli proizvesti kopije kartica koje su zatim prodavali, putem interneta, diljem svijeta.

Primjer 2. Adobe

Adobe je multinacionalna softverska tvrtka osnovana 1982. godine. Bez obzira na to što je imao veliki fokus prema tehnološkom razvoju, Adobe ima povijest sigurnosnih propusta. Tijekom godina, razne ranjivosti u njihovim softverskim proizvodima omogućile su hakerima pristup datotekama na osobnim računalima njihovih zaposlenika. Bez obzira na to što je tvrtka tijekom tih godina ulagala u informacijsku sigurnost zbog navedenih propusta, hakeri su 3. listopada 2013. godine uspjeli probiti Adobe-ovu internu mrežu. Adobe je nakon uočenog propusta objavio da je došlo do povrede podataka koja će utjecati na 3 milijuna ljudi, međutim u roku od tjedan dana od objave, broj pogođenih računa narastao je s 3 milijuna na 150 milijuna. Navedeno je značilo da su podaci milijuna klijenata bili izloženi i to podaci o kreditnim i debitnim karticama, njihova korisnička imena, lozinke i adrese e-pošte. Jedino pozitivno otkriće bilo je što se radilo o staroj bazi podataka unutar koje su brojni korisnički računi bili neaktivni. Međutim, saznalo se da su korisnici aktivnih računa koristili iste lozinke za više internetskih stranica, uključujući one koje sadrže bankovne podatke. Dodatno, otkriveno je da je 1,9 milijuna probijenih računa koristilo "123456" kao svoju lozinku, više od 345.000 koristilo je riječ "lozinka", a 211.000 računa koristilo riječ "adobe123" kao lozinku.

Iz navedenog važno je zaključiti da je vrijeme otkrivanja proboja napadača u informacijski sustav jedna od najbitnijih komponenti kako bi se zaštitio što veći broj informacija. Način na koji organizacije reagiraju na kršenje znatno utječe na njihovo poslovanje i reputaciju. Drugo, ako izostane opsežna i kontinuirana edukacija zaposlenika, izostaje i sigurnost informacijskih sustava unutar organizacije. No, bitno je pronaći način edukacije i za klijente kako bi se postigla optimalna sigurnost za obje strane (DesJardins, 2014).

2.4. Mitovi o kibernetičkoj sigurnosti

U prethodnim poglavljima već je dotaknuta neinformiranost kao i nedostatak svijesti o važnosti kibernetičke sigurnosti. Iznenadna pojava pandemije te rata dale su ovom području veću medijsku pozornosti nego ikad no, još uvijek postoje neke uobičajene zablude o kibernetičkoj sigurnosti koje organizacije, njihove zaposlenike, klijente i dioničare dovode u opasnost što je vidljivo na primjerima u prethodnom poglavlju.

Prema O' Donnell (2020) neki od mitova o kibernetičkoj sigurnosti su:

- „Kibernetička sigurnost nije moja odgovornost“ – Ovaj način razmišljanja javlja se jer pojedinci smatraju kako je kibernetička sigurnost, odnosno općenito IT sigurnost, posao IT odjela. Međutim, svi zaposlenici su dužni voditi računa o tome da okruženje u kojem rade bude sigurno. Takvi pojedinci su nažalost česta meta hakera stoga je nužno pružiti dobru i kvalitetnu edukaciju svim zaposlenicima neovisno o odjelu u kojem rade.
- „Hakeri ne ciljaju mala poduzeća, većinom su meta velike organizacije“ – Istina je da hakeri od većih poduzeća mogu tražiti veće svote otkupnina, međutim, mala poduzeća su zapravo svakodnevna meta hakera zbog slabih sigurnosnih procedura, nedostatka formalnih politika zaporki, nekorištenja sigurnosnog softvera i sl. Upravo zbog toga što mala poduzeća imaju ograničene proračune za ulaganja u kibernetičku sigurnost trebala bi osigurati stručnu i kompetentnu IT podršku koja će sve zaposlenike informirati o mogućim posljedicama kibernetičkih napada.
- „Moje lozinke su dovoljno jake da me čuvaju“ – Prethodno je već spomenuto da su zaposlenici tvrtke Adobe koristili istu lozinku za više internetskih stranica. Dodavanje velikih slova, brojeva i/ili posebnih znakova lozinke od jedne riječi neće učiniti neuništivima jer softver može probiti i takve kratke lozinke bez obzira koliko složene bile i to za nekoliko dana. Zapravo, što je lozinka duža, to je više vremena potrebno za njezino probijanje te se sukladno tome preporučuje korištenje nezaboravne fraze. No, određivanje jake lozinke koja se ne može razbiti samo je prvi korak. Zato je važno koristiti metode dvofaktorske i višefaktorske autentifikacije koje zahtijevaju postavljanje dodatnog koraka provjere.
- „Osnovni antivirusni softver bit će dovoljan da zaštitim svoje poslovanje“ – Nažalost, dani u kojima se mogao instalirati običan besplatni antivirusni softver su prošli. Jednostavan antivirusni softver više nije ni približno dovoljan kako bi se

zaštitilo osobno računalo, a pogotovo nije prikladan za zaštitu poslovanja. Sada postoje namjenski alati za borbu protiv određenih prijetnji (kao što je ucjenjivački softver), a osim toga preporučuje se i korištenje alata za sigurnosno kopiranje i oporavak od katastrofe.

- „Potrebno je zaštiti se samo od hakera“ – Hakeri svakako predstavljaju veliku prijetnju bilo kojem poslovanju, međutim, treba uzeti u obzir interne zaposlenike te članove osoblja koji imaju pristup povjerljivim informacijama. Razna poduzeća svjedoci su krađa povjerljivih podataka od strane zaposlenika. Osim toga, kao što je već navedeno, ukoliko izostane kvalitetna edukacija zaposlenika, veći problem predstavljaju interne prijetnje.
- „Moji podaci ne vrijede“ – ovo je najučestaliji mit, a zapravo najnelogičniji upravo zato što se podaci mogu unovčiti i dijeliti, a to je jedan od razloga zašto su društvene mreže besplatne.

Važnu ulogu u formiranju svijesti zaposlenika kao i u samo ulaganje u kibernetičku sigurnost ima menadžment. Neizvjesna priroda i ozbiljnost kibernetičkih prijetnji otežava donositeljima odluka raspoređivanje sredstava za ulaganje u kibernetičku sigurnost. Ako poduzeće ne doživi nikakve kibernetičke napade, odnosno, ako ih ne otkrije, neće ni imati motivaciju za ulaganje u kibernetičku sigurnost. Iz tog razloga, mnogi menadžeri često nemaju ispravnu percepciju kada je riječ o kibernetičkim rizicima, te se javljaju značajni jazovi između percepcije menadžera i stvarnog stanja kibernetičke sigurnosti njihovih organizacija. Kao rezultat toga, oni mogu podcijeniti učestalost u kojoj bi se incidenti mogli dogoditi i vrijeme koje je potrebno da sposobnosti kibernetičke sigurnosti postanu aktivne u sprječavanju, otkrivanju i reagiranju na incident (S. Jalali, Siegel i Madnick, 2019).

3. COVID-19 i kibernetička sigurnost

Tijekom prethodne dvije godine svako se poslovanje moralo prilagoditi novim zahtjevima, u većem ili u manjem obliku. Uzrok promjena koje su zahvatile cijelu ekonomiju leži u pojavi tada novootkrivene pandemije, COVID-a 19, tj. korona virusa. Prilagodba poslovanja morala se dogoditi u vremenskim rokovima koji su prije pojave spomenutog virusa bili nezamislivi. Naravno, brzina promjene, ne samo poslovanja nego i načina života donijela je sa sobom pojavu novih rizika i ranjivosti. Sve što je prije bilo društveno prihvatljivo kao normalno u doba pandemije gubi svoju vrijednost te su poduzeća, ali i pojedinci prisiljeni prihvatiti „novo normalno“. Prema Ferreira i Cruz-Correia (2021), u kibernetičkoj sigurnosti, kao i u drugim područjima, "normalno" uključuje niske proračune, nedostatak svijesti i obrazovanja kao i nedostatak odgovarajuće infrastrukture. “Normalno” također znači da su privatnost i sigurnost još uvijek dio najvećih izazova. Promjena ovakvih stavova i stanja bila je ključna i prije pojave ove pandemije koja je samo još više naglasila manjkavosti s kojima se susrećemo kada govorimo o kibernetičkoj sigurnosti.

3.1. Osnovne informacije vezane uz COVID-19

Jedna bolest je u 21. stoljeću uspjela uzrokovati promjene u svakom poduzeću na svijetu te u načinu života svakog pojedinca. Bolest pod nazivom COVID-19 uspjela je svakog pojedinca zatvoriti u četiri zida te smanjiti komunikaciju s vanjskim svijetom. Što je to korona virus?

Korona virus (COVID-19) je respiratorna bolest uzrokovana virusom SARS-CoV-2 te je započela 2019. godine kada se iz Kine ovaj virus proširio u mnoge druge zemlje diljem svijeta, odnosno cijeli svijet. Epidemija je prvi put identificirana u Wuhanu, Hubei u Kini u prosincu 2019. godine, a Svjetska zdravstvena organizacija (engl. World Health Organization, WHO) ju je 11. ožujka 2020. godine proglasila kao pandemiju. Globalno, najveći broj slučajeva prijavljen je u dobnoj skupini od 25 do 39 godina, s otprilike 50 % slučajeva u dobnoj skupini od 25 do 64 godine. Problem se javlja jer se ova bolest prenosi s čovjeka na čovjeka bliskim kontaktom. Prijenos se primarno događa kada zaražena osoba kihne ili se zakašlje te se zaraza širi putem respiratornih kapljica koje nastaju kao i drugih respiratornih patogena. Te se kapljice mogu taložiti u ustima ili nosnoj sluznici i plućima

ljudi s udahnutim zrakom. Trenutno još uvijek nije u potpunosti jasno može li se osoba zaraziti COVID-om 19 dodirivanjem zaražene površine ili predmeta, a zatim dodirivanjem usta, nosa ili možda očiju (Isam, Kamil i Shaima R., 2021). Smatra se da razdoblje inkubacije za COVID-19 traje 14 dana nakon izlaganja virusu, a većina slučajeva javlja se otprilike četiri do pet dana nakon izlaganja. Zbog svega navedenoga, primarni cilj bila je zaštita što većeg broja ljudi.

Počele su se nositi zaštitne maske (u pošti, u bolnici, na poslu i sl.) te je bila nužna dezinfekcija prilikom ulaska u bilo koji prostor. Neophodan je bio i razmak među ljudima te se pojavilo pravilo socijalne distance. Svaki pojedinac na svijetu se u ovom trenutku suočio s ogromnim strahom i neizvjesnošću. Velik broj ljudi umire, a javlja se i ograničenje broja ljudi na različitim okupljanjima pa tako i na sprovodima. Velike poslovne konferencije više nisu moguće, a poslovni sastanci premještaju se na online platforme. COVID-19 uzrokuje krizu te se javljaju pitanja sigurnosti hrane, zdravlja, zapošljavanja, cjepiva i sl. Ljudi koji ne mogu raditi tijekom pandemije riskiraju gubitak prihoda i suočavaju se s mogućom nezaposlenošću ako poduzeća propadnu. Sukladno navedenome otvaraju se i pitanja mentalnog i psihičkog zdravlja ljudi, a posebice zbog mjera socijalne izolacije. Navedene mjere imaju teške posljedice za mentalno zdravlje, osobito za one pojedince koji žive sami.

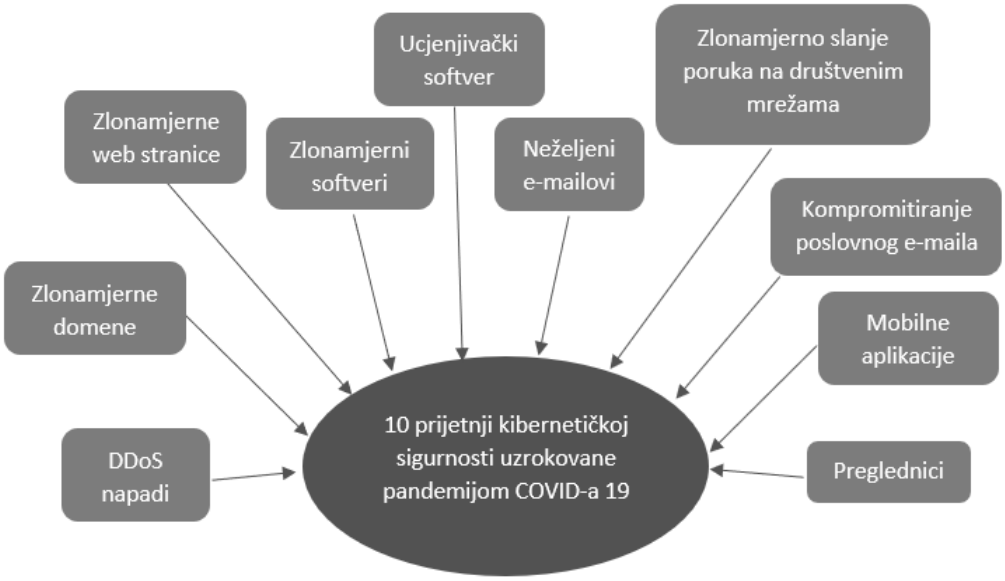
Kako se COVID-19 širio diljem svijeta, društvo počinje biti vođeno tehnologijom, a samim time javlja se niz neselektivnih, a i niz ciljanih kibernetičkih napada (Singh Lallie et al., 2021). Organizacije mijenjaju svoj način rada i javlja se „rad od kuće“. Zašto? Dok je za neke pojedince ovaj virus bio snažan udar na njihovo zdravlje, za neke je djelovao kao obična prehlada. Neki čak nisu imali nikakve simptome te su se morali samoizolirati kako ne bi širili zarazu, ali su se osjećali dovoljno dobro da mogu raditi. Uvođenje rada od kuće bio je spas za organizacije budući da nitko nije mogao utjecati na broj zaraženih, a niti jedna organizacija si ne može priuštiti da posao stane. Rad od kuće tada postaje „novo normalno“.

3.2. Prilike i prijetnje vezane uz COVID-19

Pojavom spomenutog rada od kuće te pojavom mjera socijalne distance COVID-19 otvara nove prilike organizacijama, ali omogućuje i ulazak neočekivanih prijetnji, otkrivanje ranjivosti te iskorištavanje slabosti svake organizacije. Povećava se vjerojatnost i učinak

kibernetičkih napada, a dobre prakse kibernetičke sigurnosti za mnoge organizacije pale su na stranu jer organizacije postaju ovisne o tehnologiji više nego ikad. Također priroda prijetnje se mijenja jer napadači iskorištavaju nesigurnost, situacije bez presedana i brze IT i organizacijske promjene (PwC, 2020).

Firch (2021) navodi kako su se napadi pojavili čim su tvrtke premjestile svoju radnu snagu na fleksibilne modele rada, odnosno rad od kuće, budući da akteri prijetnji iskorištavaju trenutne događaje i promjenjive okolnosti. Dodatno, Firch (2021) tvrdi kako je kibernetički kriminal u cjelini porastao za 600% od početka globalne pandemije. *„Hitnost krize značila je da je sigurnost bila zanemarena čak i dok su organizacije otvarale sustave koji prije nisu bili otvoreni“*, navodi Richard Watson, EY Asia-Pacific Voditelj savjetovanja o riziku kibernetičke sigurnosti (Burg, Maddison i Watson, 2021).



Slika 1 Prijetnje uzrokovane pandemijom COVID-19

Izvor: samostalna izrada autorice rada (prema: Khan, Brohi i Zaman, 2020)

Slika 1 prikazuje 10 prijetnji kibernetičkoj sigurnosti koje su uzrokovane pojavom pandemije COVID-a 19, a to su:

1. Raspodijeljeni napadi uskraćivanjem usluge (engl. Distributed Denial of Service, DDoS) - unatoč kontinuiranom istraživanju anomalija mrežnog prometa, kibernetički napadi poput ovog i dalje su česti i mogu imati brojne negativne posljedice na performanse informacijskih i komunikacijskih sustava i dostupnost

usluga (Cvitić, Peraković, Periša i Jurcut, 2021). Bitno je istaknuti da je velik broj vladinih i zdravstvenih organizacija zabilježilo brz porast napada distribuiranog uskraćivanja usluga zato što napadači preplavljuju web stranice ili sustave organizacija lažnim korisnicima kako bi razrušili normalno funkcioniranje sustava i tako prekinuli komunikacijski kanal (Khan, Brohi i Zaman, 2020).

2. Zlonamjerne domene – pojavljuju se zbog povećanog broja riječi povezanih s COVID-om 19 (npr. korona virus, covid-19 i sl.) koje su se pojavile na velikom broju registriranih domeni na internetu. Bez obzira na to što je velik broj stranica na tim domenama pouzdan i legitiman, napadači su iskoristili ovu mogućnost da svakim danom grade na tisuće novih web domena pomoću kojih šire zlonamjerne softvere ili poslužitelje, kradu identitete ili šire ugrožene spam kampanje (Khan, Brohi i Zaman, 2020).
3. Zlonamjerne web stranice – rastu kao i zlonamjerne domene. Raste broj stranica kojima se jamči da daju pouzdane i točne informacije o virusu te koje zahtijevaju preuzimanje raznih informativnih aplikacija. Međutim, instaliranjem navedenih aplikacija sustav se inficira zlonamjernim softverom koji čini da se zaraženi uređaji ponašaju kao botnet (mreža uređaja pod kontrolom napadača) (Khan, Brohi i Zaman, 2020).
4. Zlonamjerni softveri – šire se putem spomenutih web stranica o korona virusu. Korisnici najčešće preuzimaju zlonamjerne softvere putem neželjenih e-mail poruka, klikom na zaražene linkove i sl. Zlonamjerni softveri i domene zauzimaju prvo mjesto kada govorimo o porastu prijetnji i napada (Khan, Brohi i Zaman, 2020).
5. Ucjenjivački softveri – u doba pandemije pojavili su se u bolnicama, javnim ustanovama, obrazovnim institucijama i domovima zdravlja. To su institucije koje si ne mogu priuštiti „isključenost“ iz svojih sustava te su zbog toga napadači optimistični da će takve institucije platiti bilo koji iznos otkupnine. Ucjenjivački softver može zaraziti sustav (putem privitaka e-pošte, poveznica ili preko zaposlenika čiji su podaci već ugroženi) iskorištavanjem ranjivosti (Khan, Brohi i Zaman, 2020).
6. Neželjeni e-mail-ovi – bili su česta pojava i prije pandemije COVID-a 19 i svatko se barem na mjesečnoj razini susreo sa spam porukom. Kao što je već spomenuto,

pojavom pandemije počele su se širiti nejasne i nepravovaljane informacije što su napadači opet iskoristili kao prednost te se počinju širiti e-poruke sa raznim privicima (npr. pdf datoteke) koji naizgled „podižu svijest i informiranost“ o virusu. U ovim slučajevima bitno je obratiti pozornost na domenu e-mail-a, način komunikacije unutar e-mail-a, ne otvarati linkove niti preuzimati privitke.

7. Zlonamjerne poruke na društvenim mrežama – za napadače su izvrsna prilika budući da su društvene mreže besplatne i dostupne svakom pojedincu. Najčešće prijevare putem društvenih mreža su besplatne pretplate te ako pojedinac „nasjedne“ na link on ga preusmjeri na web stranicu za krađu identiteta. U raznim slučajevima stranice traže podatke za prijavu što napadačima olakšava dohvat podataka, a postoji i mogućnost instalacije spomenutog zlonamjernog softvera putem kojega napadači kradu informacije o pojedincu (osobni podaci, preferencije i sl.) (Khan, Brohi i Zaman, 2020).
8. Kompromitiranje poslovnog e-maila – u doba pandemije je olakšano budući da napadači koriste korona virus kao alat za ulazak u poslovni sustav neke organizacije. Npr. ako napadač cilja na bankovni sustav može ga kompromitirati tako da se koristi podacima klijenta te banci pošalje e-mail zahtjev za promjenom svojih bankovnih podataka, načina plaćanja i sl. Mnoge organizacije bile su meta ovakvih vrsta napada u razdoblju pandemije (Khan, Brohi i Zaman, 2020).
9. Mobilne aplikacije – doživjele su svoj vrhunac u doba sveprisutnog računalstva. Korisnici mobilnih uređaja ne obraćaju pozornost kada skidaju aplikacije niti se obaziru na potencijalne viruse koji ostaju nakon deinstalacije istih. Khan, Brohi, Zaman, 2020. navode postojanje aplikacije pod nazivom „CovidLock“ koja dolazi iz zlonamjerne Android aplikacije. Aplikacija navodno pomaže u praćenju slučajeva COVID-a 19. No, ucjenjivački softver koji se koristi u aplikaciji zaključava uređaje žrtava te žrtve imaju 48 sati da plate 100 USD u bitcoin-ima kako bi napadači otključali uređaj. Ako žrtve ne plate otkupninu prijeti im se brisanjem telefonskih podataka te curenjem podataka o računu na društvenim mrežama.
10. Preglednici – su postali svakodnevno korišteni softveri, a koristi ih zapravo svaki pojedinac koji ima pristup internetu. Povećao se broj usmjerivača koji samostalno

(automatski) otvaraju preglednike te korisnici tako neprimjetno preuzmu zlonamjerni softver koji krade podatke (Khan, Brohi i Zaman, 2020).

Kao što je navedeno, povećao se broj prijetnji kibernetičkoj sigurnosti, a samim time i pitanja privatnosti. No, problem se očituje u tome što to povećanje nije doživjelo svoj vrhunac te stagnaciju, nego se i dalje nastavlja povećavati. S izbijanjem pandemije korona virusa, došlo je do ogromnog porasta broja korisnika koji su svoju komunikaciju morali preusmjeriti na virtualne platforme. Sukladno navedenome, aplikacije za online video konferencije kao što su Zoom, Microsoft Teams i Google Meet svjedočile su eksponencijalnom porastu broja novih korisnika koji se svakodnevno prijavljuju (Khan, Brohi i Zaman, 2020). Napadači su naravno iskoristili, i dalje iskorištavaju, svaku mogućnost za napade na različite platforme bilo radi financijske dobiti ili drugih interesa.

Kada govorimo o prijetnjama povezanim s pojavom pandemije najistaknutiji problemi javljaju se zbog rada od kuće. Kao posljedica toga, tehnologija je postala još važnija u poslovnom i privatnom životu ljudi, ali unatoč navedenome mnoge organizacije u to vrijeme nisu pružile svojim zaposlenicima sigurno kibernetičko okruženje za rad na daljinu, a neke još uvijek ne pružaju. Povećanje broja zaposlenika koji rade na daljinu trebalo je povećati fokus organizacija na kibernetičku sigurnost zbog veće izloženosti kibernetičkom riziku. Sukladno tome, trebala su se povećati i ulaganja u kibernetičku sigurnost i zaštitu općenito (Nabe, 2021). Veliki problem očituje se u nespremnosti organizacija na pandemiju, a jedan primjer toga su male organizacije koje se vode politikom „donesi svoj vlastiti uređaj“ te brojni zaposlenici u poslovne svrhe (npr. pristup korporativnim informacijama) koriste svoja osobna računala. Naravno, ovakve politike ne predstavljaju problem ako IT odjel vodi računa o sigurnoj konfiguraciji računala svojih zaposlenika. Ono što je sigurno je da rad od kuće ne pruža identičnu razinu sigurnosti kao rad iz uredskog okruženja. Najjednostavniji primjer su kućne internetske mreže koje je puno lakše napasti nego korporativnu mrežu budući da je ona zaštićenija. Dakle, jedan od razloga povećanja kibernetičkih napada je što brojne organizacije nisu provjerile jesu li osobni uređaji njihovih zaposlenika opremljeni standardnom sigurnosnom zaštitom prije nego što su zaposlenici krenuli raditi na daljinu, nego su se oslonile na zaštitu korištenjem virtualne privatne mreže (engl. virtual private network, VPN) (Nabe, 2021).

Postoje i brojni drugi razlozi zašto je rad na daljinu povećao broj kibernetičkih napada. Jedan je zasigurno što određeni zaposlenici zaobilaze primjenu dobrih praksi kada naiđu na prepreke u radu. Npr. neki zaposlenici koji smatraju da im se određene datoteke preuzimaju/dijele presporo preko kućne internetske mreže mogu se poslužiti alternativnim (nedozvoljenim) metodama dijeljenja. Rad na daljinu zapravo je većini zaposlenika predstavljao i predstavlja nesigurno okruženje u kojem se javila povećana razina stresa. Rad s nepoznatim tehnologijama u takvom nesigurnom okruženju rezultirao je novim sigurnosnim rizicima, a mogućnosti za pružanje edukacije vjerojatno su u bile ograničene. Navedeno je dovelo do toga da se tehnologije koriste na neprikladan način, da su pogrešno konfigurirane ili se nisu koristile uz sigurnosne mjere koje su za njih bile predviđene. Također, oslanjanje na sustave udaljenog pristupa može učiniti organizacije ranjivijim na raspodijeljene napade uskraćivanjem usluge (DDoS) (PwC, 2020). Ako pozorno promotrimo sve navedeno važno je zaključiti da su mnoga kršenja kibernetičke sigurnosti rezultat ljudskih pogrešaka. Ljudska pogreška bila je glavni izvor kibernetičke nesigurnosti i prije pojave pandemije, a s radom od kuće problem se samo povećao. Ako je organizacijama prihvatljivo da se korporativnim podacima pristupa s osobnih uređaja, onda bi i procjena kibernetičkih rizika i poduzimanje mjera za ograničavanje istih trebala biti prihvatljiva (Nabe, 2021).

U sljedećoj tablici sumirana su rizična ponašanja vezana za kibernetičku sigurnost:

#Broj	Rizično ponašanje
#1	Klikovi na poveznice iz neželjene pošte koja je iz neidentificiranog izvora.
#2	Korištenje iste lozinke na više web stranica.
#3	Preuzimanje besplatnog antivirusnog softvera iz neidentificiranog izvora.
#4	Preuzimanje materijala s web stranice na poslovno računalo bez provjere autentičnosti.
#5	Korištenje javnog Wi-Fi-ja s besplatnim pristupom.
#6	Spremanje informacija organizacije na osobni elektronički uređaj poput prijenosnog računala, tableta ili pametnog telefona.

Tablica 2 Rizična ponašanja vezana uz kibernetičku sigurnost

Izvor: samostalna izrada autorice rada (prema: Wang i Alexander, 2021)

Opseg zašite kibernetičke sigurnosti u eri pandemije trebao je postati veći, mjere su trebale biti strože, a zaposlenicima koji su radili od kuće bilo je potrebno osigurati dodatan sloj sigurnosti i zaštite. No, Burg, Maddison i Watson (2021) navode kako je 81% organizacija zaobišlo kibernetičke procese i nije konzultiralo timove za kibernetičku sigurnost u fazi

planiranja novih poslovnih inicijativa. Prekid komunikacije među ljudima nije bio uzrokovan samo COVID-om 19 i samoizolacijom, nego i radom od kuće. Zbog prekida komunikacije među zaposlenicima i nadređenima odnosi su postali slabi tamo gdje su trebali biti jaki (Burg, Maddison i Watson, 2021).

Međutim, pandemija COVID-a 19 donijela je i velike prilike za područje kibernetičke sigurnosti. Prvo, rad od kuće pokazao je da je umrežavanje ključno za tvrtke koje žele raditi na daljinu. Kaufman i Taniguchi (2021) navode da rad od kuće daje zaposlenicima povećanu fleksibilnost, zadovoljstvo poslom i osjećaj ravnoteže, povećava produktivnost i radno vrijeme. Prijelaz na rad na daljinu zahtijeva da se sam sektor kibernetičke sigurnosti prilagodi kako bi pružio bolje alate za podršku i zaštitu te kako bi se na vrijeme pronašla rješenja za trenutne prijetnje i zahtjeve kibernetičke sigurnosti. Drugo, povećava se potražnja za kvalitetnim i kompetentnim stručnjacima za kibernetičku sigurnost i IT. Međutim, utjecaj COVID-a 19 zahtijeva da, više nego ikada, navedeni stručnjaci imaju šire vještine i kompetencije uključujući učinkovitu komunikaciju, strpljenje, upravljanje vremenom, agilnost, organizaciju i rješavanje problema u ovim nesigurnim vremenima. Sve navedeno zahtijeva velika ulaganja u kibernetičku sigurnost i postavljanje ovog područja na viši organizacijski prioritet.

3.3. COVID-19 i zlonamjerni cyber pokušaji

Prethodno su već navedeni primjeri kibernetičkih napada na organizacije u godinama prije pandemije. U pandemijskome razdoblju broj kibernetičkih napada raste i u Republici Hrvatskoj. U 2021. godini dogodili su se veliki propusti organizacija što je napadačima omogućilo proboj u njihove sustave.

Primjer 1. AAI@EduHr

Prema Pravilniku o ustroju autentifikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr (2008), AAI@EduHr je posrednički sustav koji korisnicima omogućava sigurno i pouzdano upravljanje njihovim elektroničkim identitetima. Međutim, sustavi za e-učenje imaju brojne ranjivosti te su često izloženi kibernetičkim napadima. Problem se dodatno istaknuo pojavom COVID-a 19 zbog povećanog korištenja sustava za e-učenje, a i cijeli obrazovani sustav preselio se na virtualne

platforme. U ožujku 2020. godine, ovaj sustav bio je meta više DDoS napada tijekom migracije sustava zbog navedene pandemije. Prilikom napada korisnici su imali poteškoće u pristupu ili im je pristup bio u potpunosti onemogućen. Prema podacima Hrvatskog sveučilišnog računskog centra (Srce) tijekom ožujka 2020. godine, AAI@EduHr sustav zabilježio je 11.214.236 uspješnih autentifikacija za 517.453 jedinstvena korisnika.
Problem se javio zbog preopterećenja sustava koje je onemogućilo otkrivanje DDoS napada na vrijeme (Cvitić, Peraković, Periša i Jurcut, 2021).

Primjer 2. A1

A1 je hrvatski pružatelj telekomunikacijskih usluga koji je u veljači 2022. godine bio meta kibernetičkog napada. Zbog neovlaštenog pristupa sustavu kompromitirani su podaci više od 100.000 korisnika (ime, prezime, OIB, adresa, broj telefona). Haker je zauzvrat tražio otkupninu u iznosu od 150 ethereum-a (oko 500.000 dolara) u roku od 72 sata. A1 je jedan od telekomunikacijskih pružatelja koji se drži visokih standarda informacijske sigurnosti te su zbog toga djelatnici na vrijeme otkrili propust i sačuvali velik broj podataka.

Primjer 3. INA

INA je vodeća naftna kompanija u Republici Hrvatskoj koja je također u veljači 2020. godine bila meta hakerskog napada. Napad na INA-u trajao je više od 30 dana, a hakeri su sustav napali ucjenjivačkim softverom pomoću kojeg su šifrirali datoteke i onemogućili im pristup. Za otkupninu su tražili 1500 bitcoin-a (oko 100 milijuna kuna) kako bi otključali računalni sustav. INA nije provodila potpuni backup svih svojih podataka te se zbog toga suočila s iznimnim posljedicama u poslovanju.

Unatoč kontinuiranom istraživanju anomalija mrežnog prometa, kibernetički napadi poput navedenog DDoS napada u slučaju AAI@EduHr, i dalje su česti i mogu imati brojne negativne učinke na predviđene performanse informacijskih sustava i dostupnost usluga. Kako se poduzeća transformiraju, pogotovo zbog zahtjeva koje je donijela pandemija COVID-a 19, novi sustavni izazovi i prioriteti se povećavaju, pritom najviše sigurnosni rizici. (Khan, Brohi i Zaman, 2020) Mnoge organizacije i zaposlenici moraju preispitati svoje načine rada jer bez odgovarajućih razmatranja povećavaju rizik od napada na kibernetičku sigurnost (PwC, 2020).

4. Istraživanje utjecaja COVID-19 na kibernetičku sigurnost

Prije prikaza samih rezultata istraživanja važno je definirati korištenu istraživačku metodu, svrhu i ciljeve istraživanja, postavljene hipoteze, izabrane ispitanike te navesti moguća ograničenja. U nastavku je pojedinačno opisan svaki od navedenih elemenata ankete.

4.1. Svrha i ciljevi istraživanja

Kao što je već spomenuto u prethodnim poglavljima, kibernetička sigurnost doživjela je mnoge probleme i prepreke pojavom pandemije COVID-a 19. Sukladno navedenome, istraživanje se ne odnosi samo na jedan ključni cilj, nego na više ciljeva, a to su:

a) utvrditi koliko je zaposlenika prošlo kroz edukacije vezane uz kibernetičku sigurnost u razdoblju od početka pandemije do danas,
b) jesu li organizacije koje su sudjelovale u istraživanju bile izložene kibernetičkim napadima i u kojoj mjeri.

4.1.1. Hipoteze istraživanja

Bitno je iznijeti i hipoteze istraživanja s obzirom da one utječu na prethodno navedeni cilj samog istraživanja:

1) Broj kibernetičkih napada se povećao u razdoblju pandemije.
2) Velik broj zaposlenika i dalje radi od kuće.
3) Značajan postotak zaposlenika nije prošao kroz edukacije o kibernetičkoj sigurnosti prije prelaska na rad od kuće.

4.2. Metode istraživanja

Za potrebe diplomskog rada provedeno je primarno istraživanje putem anketnog upitnika, tj. google obrasca, kojeg su ispitanici popunjavali anonimno putem linka. Anketni upitnik oblikovan je prema prethodnim validnim istraživanjima iz 2020. i 2022. godine koja se

temelje na proučavanju stanja kibernetičke sigurnosti, kao i utjecaju COVID-a 19 na istu. Anketna pitanja oblikovana su uparivanjem navedenih validnih istraživanja prema najrelevantnijim rezultatima istih te su dodatno formirana čitanjem i proučavanjem povezane literature. Link je ispitanicima proslijeđen putem e-maila te su se podaci prikupljali od 29. lipnja do 9. srpnja 2022. godine. U odabrani uzorak ispitanika odabrani su zaposlenici odjela informacijske sigurnosti i zaposlenici odjela IT-a deset poduzeća koja se bave različitim djelatnostima (savjetovanje, telekomunikacije, farmaceutska tvrtka, softverska tvrtka, banka (financije), IT). Navede organizacije birane su i na temelju djelatnosti, ali prilikom odabira najviše se vodilo računa da organizacije imaju razvijene odjele informacijske sigurnosti i IT-a. Unutar anketnog upitnika postavljena su 2 seta pitanja, prvo je informativno o području kibernetičke sigurnosti i radu od kuće, a drugi dio pitanja odnosi se na stavove zaposlenika o kibernetičkim napadima s kojima su se susreli od početka pandemije do danas te o edukacijama vezanim za kibernetičku sigurnost. U anketi je sudjelovalo 50 ispitanika koji se bave poslovima kao što su: voditelj informacijske sigurnosti, stručnjak za kibernetičku sigurnost, konzultant u IT odjelu, programer, voditelj odjela IT razvoja, IT menadžer, IT - tehnička podrška na licu mjesta, itd.

4.3. Istraživačka pitanja i odabir ispitanika

Prilikom sastavljanja anketnog upitnika vodilo se računa da isti odgovara na sljedeća istraživačka pitanja:

i. Koliko zaposlenika i dalje radi od kuće?
ii. Smatraju li zaposlenici da je pandemija COVID-a 19 utjecala na kibernetičku sigurnost?
iii. Jesu li zaposlenici bili educirani o kibernetičkoj sigurnosti u razdoblju od početka pandemije do danas?

Za ispitanike su izabrani zaposlenici odjela IT-a i odjela informacijske sigurnosti organizacija koje se bave različitim djelatnostima, a imaju razvijene navedene odjele. Konkretno se radi o deset hrvatskih poduzeća koja se bave djelatnostima savjetovanja, telekomunikacijama, razvijanjem softverskih rješenja, IT-em, financijama te prodajom (farmaceutska tvrtka). Anketu je popunilo 50 anonimnih ispitanika.

4.4. Moguća ograničenja prilikom istraživanja

Prilikom izbora anketnog upitnika kao istraživačke metode potrebno je voditi računa o mogućim ograničenjima. Tijekom provođenja ovog istraživanja neki od problema su bili:

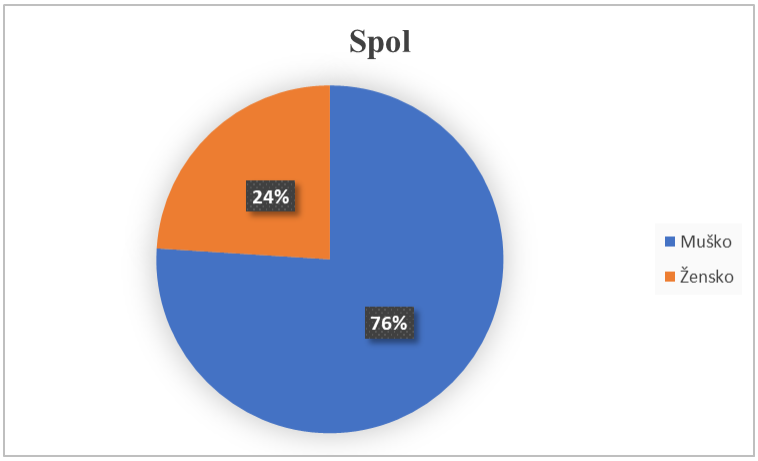
- istinitost rezultata (budući da svaki ispitanik ispunjava anketu na temelju svojih osobnih stavova),
- kompetentnost ispitanika (ne postoji mogućnost provjere svih ispitanika kako bi se utvrdilo jesu li oni isključivo bili zaposlenici odjela IT-a i odjela informacijske sigurnosti),
- pronalazak adekvatnih ispitanika.

Bez obzira na spomenuta ograničenja, istraživanje stavova ispitanika o utjecaju COVID-19 pandemije na kibernetičku sigurnost, uspješno je provedeno.

4.5. Provedba i rezultati istraživanja

Za potrebe istraživanja sastavljeno je 29 pitanja kojima se pokrivaju istraživačka pitanja, ciljevi istraživanja i postavljene hipoteze kako bi se došlo do što relevantnijih rezultata. U sklopu pitanja nalaze se mogućnosti višestrukog odabira, potvrdnih okvira, linearnog mjerila i mreže sa višestrukim odabirom. Kod pitanja višestrukog odabira ispitanici su imali mogućnost odabira samo jednog od ponuđenih odgovora dok su kod pitanja u obliku potvrdnih okvira ispitanici mogli označiti sve što je od odgovora za njih primjenjivo.

1. Spol
    a. Muško (N=38)
    b. Žensko (N=12)

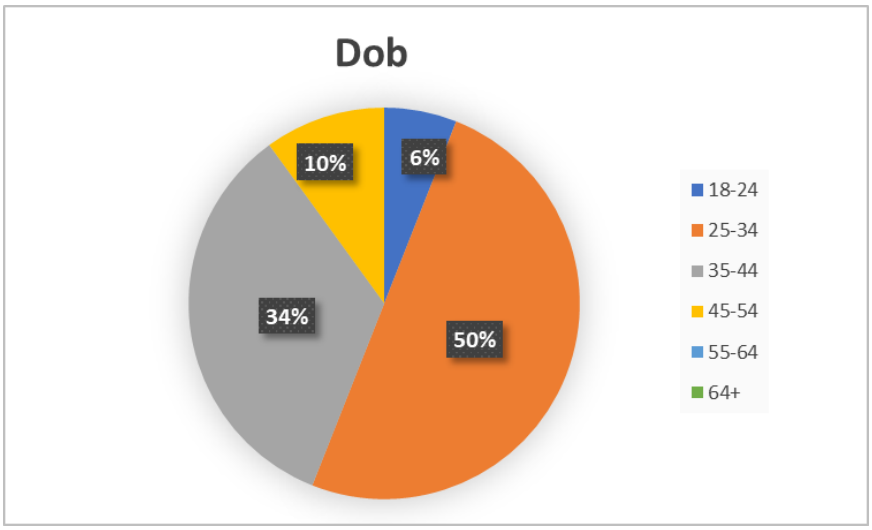


Slika 2 Spol ispitanika

Izvor: samostalna izrada autorice rada

Od ukupno 50 anonimnih ispitanika odjela IT-a i odjela informacijske sigurnosti, njih 76% bilo je muškog spola, a ostatak od 24% ženskog spola.

2. Dob
    a. 18-24 (N=3)
    b. 25-34 (N=25)
    c. 35-44 (N=17)
    d. 45-54 (N=5)
    e. 55-64
    f. 65+

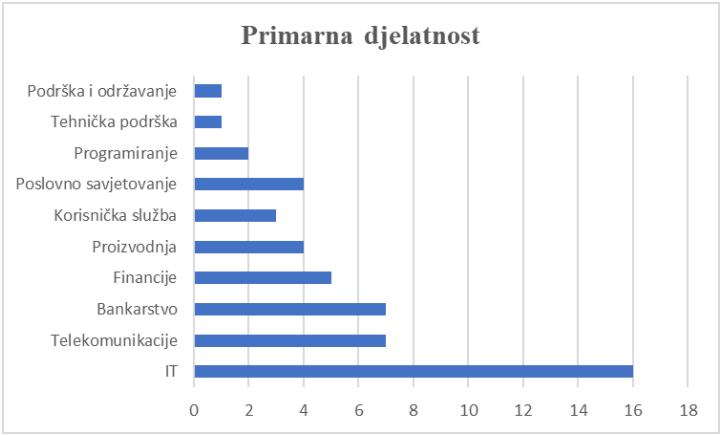


Slika 3 Dob ispitanika

Izvor: samostalna izrada autorice rada

50% ispitanika je dobi od 25-34 godine, 34% ispitanika je dobi 35-44 godina, 10% ispitanika je dobi 45-54 godina te 6% ispitanika je dobi 18-24 godine. Ovaj rezultat može biti malo zabrinjavajući budući da za zaposlenike koji su na sredini karijere (u ovom slučaju 34%) postoji veća mogućnost da će u skorijem vremenu podnijeti ostavku.

3. Koja je primarna djelatnost vaše organizacije?

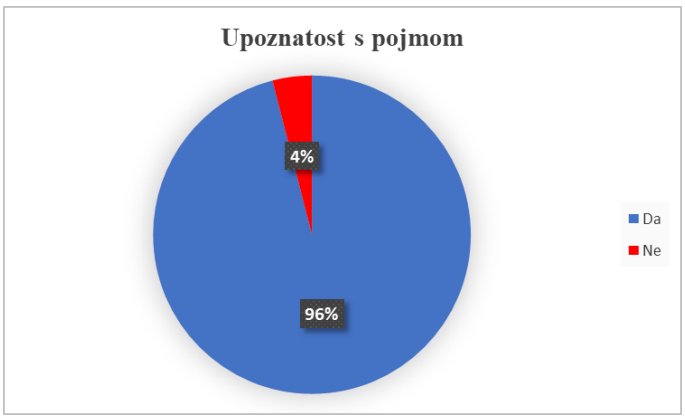


Slika 4 Primarna djelatnost ispitanika

Izvor: samostalna izrada autorice rada

Najveći broj ispitanika (N=16) naveo je IT kao primarnu djelatnost svoje organizacije. Zatim slijede telekomunikacije i bankarstvo (N=7), proizvodnja, financije, te ostale djelatnosti.

4. Jeste li upoznati s pojmom kibernetičke sigurnosti?
    a. Da (N=48)
    b. Ne (N=2)

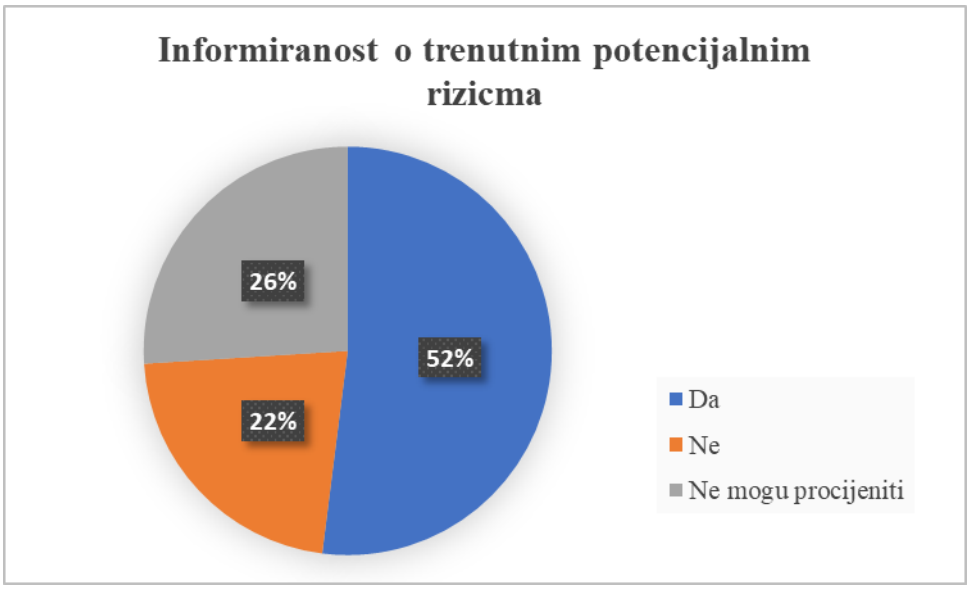


Slika 5 Upoznatost s pojmom kibernetičke sigurnosti

Izvor: samostalna izrada autorice rada

Bez obzira što su ispitanici bili isključivo zaposlenici odjela IT-a i odjela informacijske sigurnosti, anketa pokazuje 2 ispitanika (4%) koja nisu upoznata s pojmom kibernetičke sigurnosti. Navedeno se vjerojatno odnosi na ispitanike koji su nedavno zaposleni u odjelu IT-a.

5. Smatrate li da ste dovoljno informirani o trenutnim potencijalnim rizicima koji proizlaze iz kibernetičke sigurnosti, a posljedica su COVID-19 pandemije?
    a. Da (N=26)
    b. Ne (N=11)
    c. Ne mogu procijeniti (N=13)

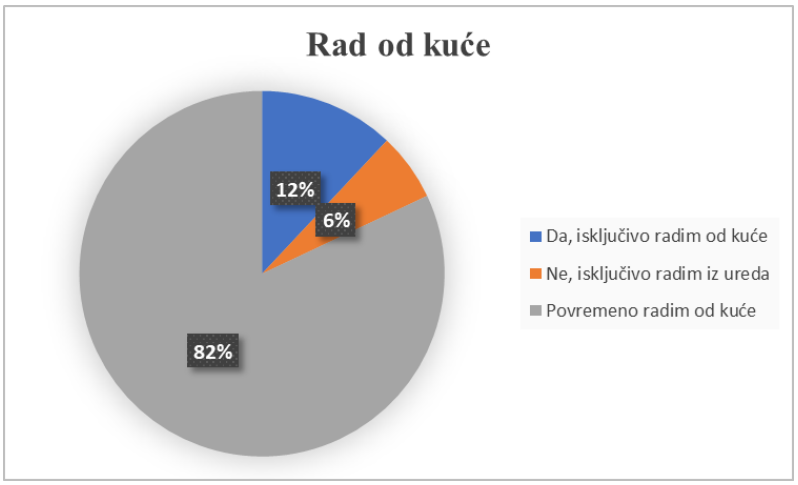


Slika 6 Informiranost ispitanika o potencijalnim kibernetičkim rizicima

Izvor: samostalna izrada autorice rada

Proučavajući grafikon o informiranosti ispitanika o potencijalnim rizicima koji su proizašli kao posljedica COVID-19 pandemije, može se uočiti kako je čak 26% ispitanika odgovorilo kako ne može procijeniti svoju informiranost što bi značilo da neke organizacije nisu redovito i kontinuirano provodile programe podizanja svijesti zaposlenika o kibernetičkoj sigurnosti. 52% ispitanika odgovorilo je kako su upoznati sa potencijalnim rizicima koji su proizašli kao posljedica COVID-19 pandemije što bi značilo da su svjesni novih rizika koji su nastali kao posljedica COVID-a 19.

6. Imate li u svojoj organizaciji mogućnost rada "od kuće"?
    a. Da, isključivo radim od kuće (N=6)
    b. Ne, isključivo radim od iz ureda (N=3)
    c. Povremeno radim od kuće (N=41)

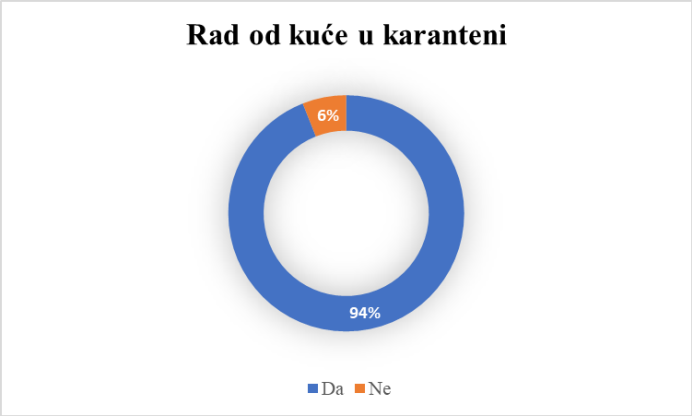


Slika 7 Rad od kuće

Izvor: samostalna izrada autorice rada

82% ispitanika i dalje povremeno radi od kuće, dok samo njih 6% isključivo radi iz ureda. Prema ovim informacijama može se zaključiti kako su organizacije prihvatile hibridan način rada, prilagođavajući se potrebama i željama zaposlenika, ali prvenstveno prilagođavajući se nužnim pandemijskim potrebama. Međutim, u radu je već navedeno kako rad od kuće donosi mnoge probleme, stoga je bitno da organizacije koje su usvojile hibridan način rada kao poslovnu praksu uvedu i potrebne mjere sigurnosti okruženja.

7. Jeste li tijekom karantene (lockdown-a) radili od kuće?
    a. Da (N=47)
    b. Ne (N=3)

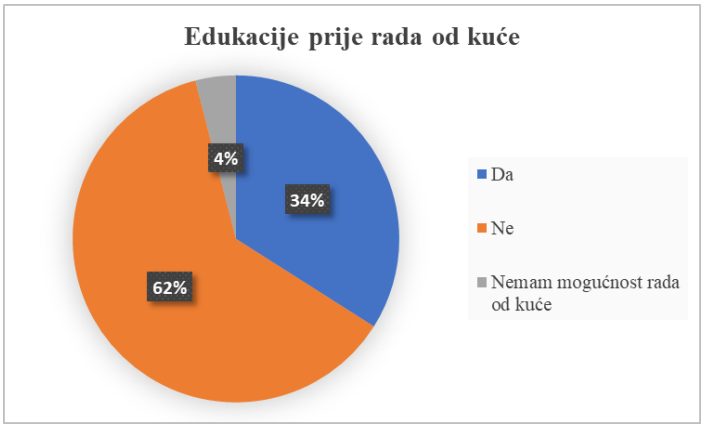


Slika 8 Rad ispitanika u karanteni

Izvor: samostalna izrada autorice rada

U prethodnim poglavljima spomenuto je kako je većina organizacija prešla na rad od kuće prilikom pojave pandemije korona virusa. Navedeno je vidljivo i na grafikonu koji pokazuje da je 94% ispitanika tijekom karantene radilo od kuće.

8. Ako ste na prethodno pitanje odgovorili sa "Da"; jeste li, u sklopu organizacije u kojoj radite, prije prelaska na rad od kuće prošli određenu edukaciju?
    a. Da (N=17)
    b. Ne (N=31)
    c. Nemam mogućnost rada od kuće (N=2)

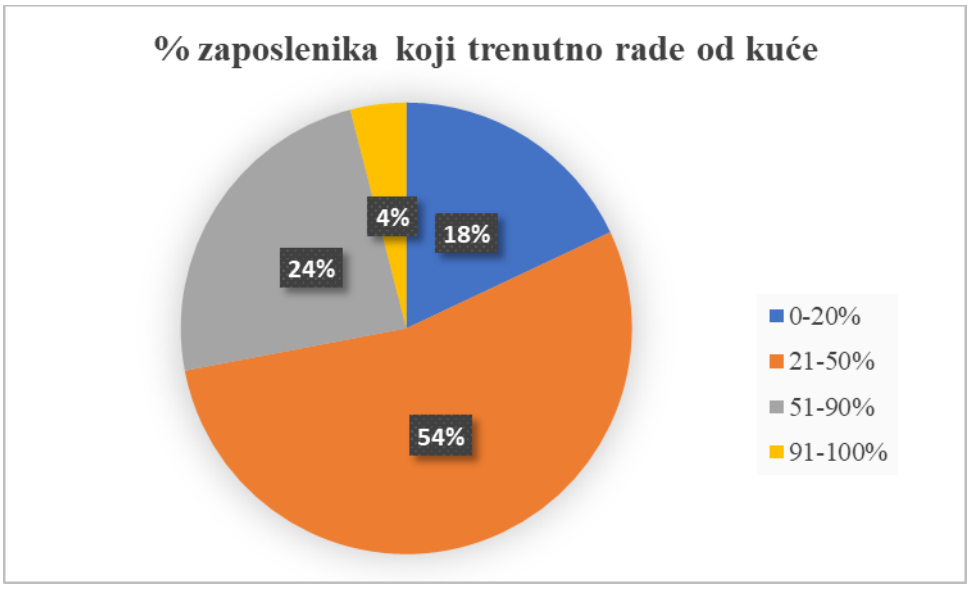


Slika 9 Edukacije zaposlenika prije početka rada od kuće

Izvor: samostalna izrada autorice rada

Pregledom grafikona možemo zaključiti kako čak 62% zaposlenika nije pohađalo nikakve vrste edukacija prije početka rada od kuće. Sukladno navedenome, zaposlenici nisu mogli biti dovoljno osigurani u vlastitom, kućnom okruženju. Prema ovim informacijama jasno je da su kibernetički napadači iskoristili nesigurna okruženja za svoje napade.

9. Kao posljedica COVID-19 pandemije, koji postotak vaših kolega (otprilike) trenutno radi od kuće?
    a. 0-20% (N=9)
    b. 21-50% (N=27)
    c. 52-90% (N=12)
    d. 91-100% (N=2)



Slika 10 % zaposlenika koji trenutno rade od kuće

Izvor: samostalna izrada autorice rada

Kao što je već prethodno spomenuto pregledom Slike 7, vidljivo je kako su organizacije usvojile hibridne načine rada te zaposlenici povremeno rade iz ureda, a povremeno rade od kuće. Čak 21-50% zaposlenika ispitanih organizacija i dalje radi od kuće.

10. Što mislite kako napreduju napori za pružanje podrške većem broju zaposlenika koji rade od kuće (na temelju vaše percepcije ili povratnih informacija zaposlenika)?
    a. Vrlo glatko, bilo je malo ili nimalo smetnji u svakodnevnim operacijama
    b. U redu, bilo je manjih smetnji u svakodnevnom radu
    c. Moglo bi i bolje, bilo je nekoliko poremećaja u svakodnevnom radu, ali idemo u pravom smjeru
    d. Teško, bilo je značajnih poremećaja u svakodnevnom radu

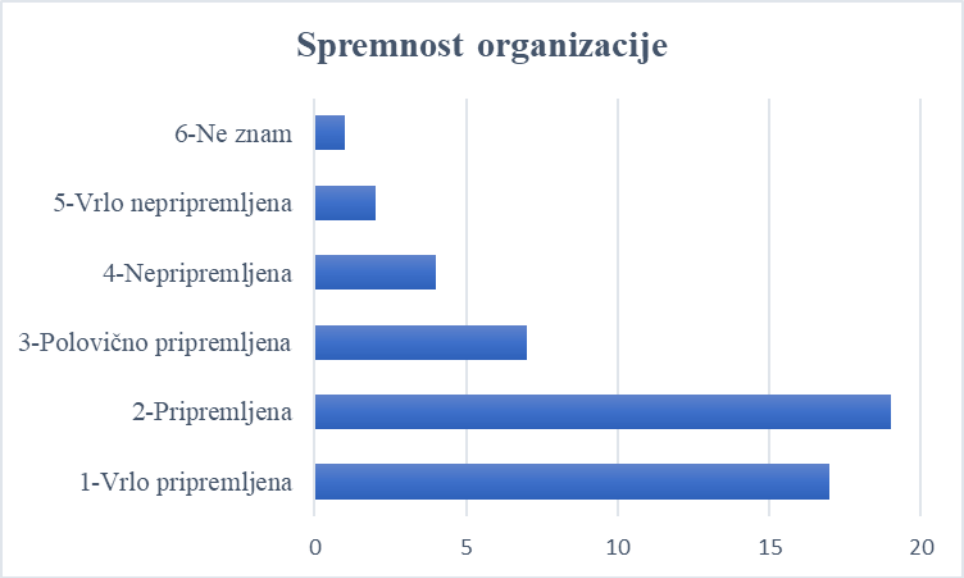
Slika 11 Napori za pružanje podrške zaposlenicima koji rade od kuće

Izvor: samostalna izrada autorice rada

Iako je COVID-19 poremetio mnoge aspekte života pojedinaca, ali i poslovanje organizacije, mnoge od njih uspjele su riješiti neočekivane zahtjeve i prilagoditi se novonastalim uvjetima rada. Kao što je vidljivo, 58% ispitanika izjasnilo se da je bilo samo manjih smetnji u svakodnevnom radu, a 24% njih da je bilo malo ili nimalo smetnji.

11. Koliko je vaša organizacija, po vama, bila spremna za osiguranje uređaja i aplikacija koje će zaposlenici koristiti kod kuće?
    1 - Vrlo pripremljena (N=17, 34%)
    2 – Pripremljena (N=19, 38%)
    3 - Polovično pripremljena (N=7, 14%)
    4 – Nepripremljena (N=4, 8%)
    5 - Vrlo nepripremljena (N=2, 4%)

6 - Ne znam (N=1, 2%)

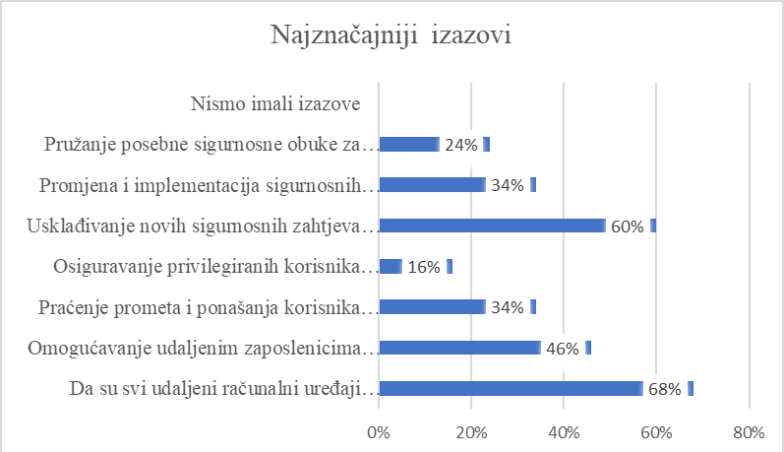


Slika 12 Spremnost organizacija na rad od kuće

Izvor: samostalna izrada autorice rada

Slika 12 prikazuje kako su stručnjaci za kibernetički sigurnost bili spremni osigurati zaposlenicima svojih organizacija uređaje i aplikacije koje su koristili od doma. Čak 38% ispitanika smatra kako su bili pripremljeni osigurati navedene uređaje i aplikacije, a njih 34% smatra kako su bili vrlo pripremljeni.

12. Koji su od sljedećih najznačajnijih izazova povezani s povećanjem populacije zaposlenika koji rade od kuće u vašoj organizaciji?
    - Da su svi udaljeni računalni uređaji zaposlenika sigurno konfigurirani
    - Omogućavanje udaljenim zaposlenicima siguran pristup korporativnoj mreži
    - Praćenje prometa i ponašanja korisnika koji rade od kuće
    - Osiguravanje privilegiranih korisnika koji nikada prije nisu radili od kuće
    - Usklađivanje novih sigurnosnih zahtjeva za rad od kuće s usklađenošću s propisima
    - Promjena i implementacija sigurnosnih politika dizajniranih za udaljene zaposlenike
    - Pružanje posebne sigurnosne obuke za udaljene zaposlenike
    - Nismo imali izazove
    - Ostalo

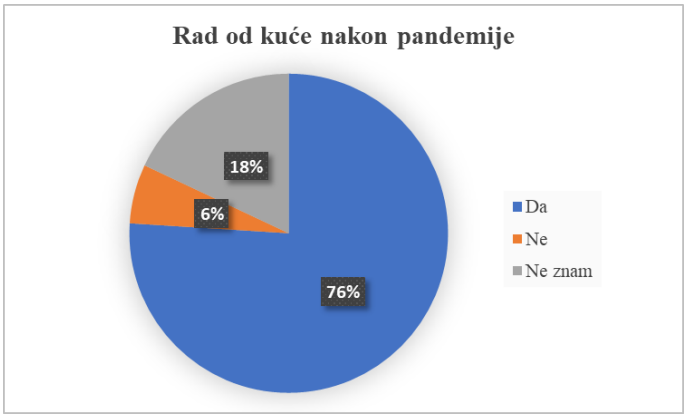


Slika 13 Najznačajniji izazovi povezani s povećanjem zaposlenika koji rade od kuće

Izvor: samostalna izrada autorice rada

Prema Slici 13, organizacijama je najveći izazov predstavljala konfiguracija uređaja zaposlenika koji rade od kuće te usklađivanje novih zahtjeva sa postojećim propisima i procedurama. Također, pozitivno je da je čak 34% ispitanika odgovorilo kako je veliki izazov bio i promjena sigurnosnih politika što znači da su se organizacije u ovom neizvjesnom razdoblju zaista pokušale maksimalno prilagoditi novim sigurnosnim zahtjevima.

13. Smatrate li da će vaša organizacija biti fleksibilnija s pravilima rada od kuće nakon što se trenutna pandemija COVID-19 u potpunosti smiri?
    a. Da (N=38)
    b. Ne (N=3)
    c. Ne znam (N=9)

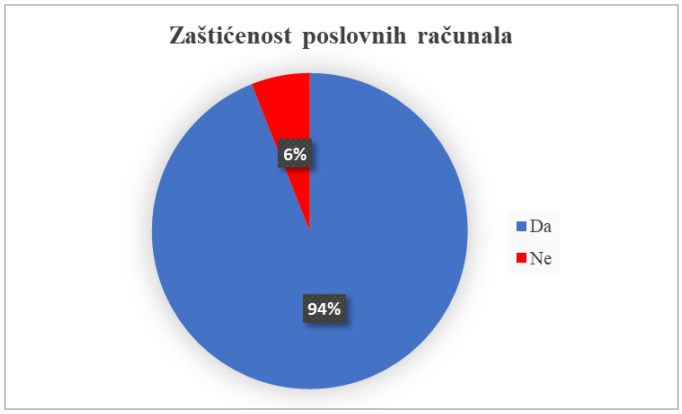


Slika 14 Rad od kuće nakon pandemije

Izvor: samostalna izrada autorice rada

76% ispitanika smatra kako će organizacija u kojoj rade biti fleksibilnija s pravilima rada od kuće nakon što se pandemija u potpunosti smiri. Navedeno znači da zaposlenici očekuju prihvaćanje hibridnog načina rada kao nove poslovne prakse.

14. Smatrate li da su vaša poslovna računala dovoljno zaštićena?
    a. Da (N=47)
    b. Ne (N=3)

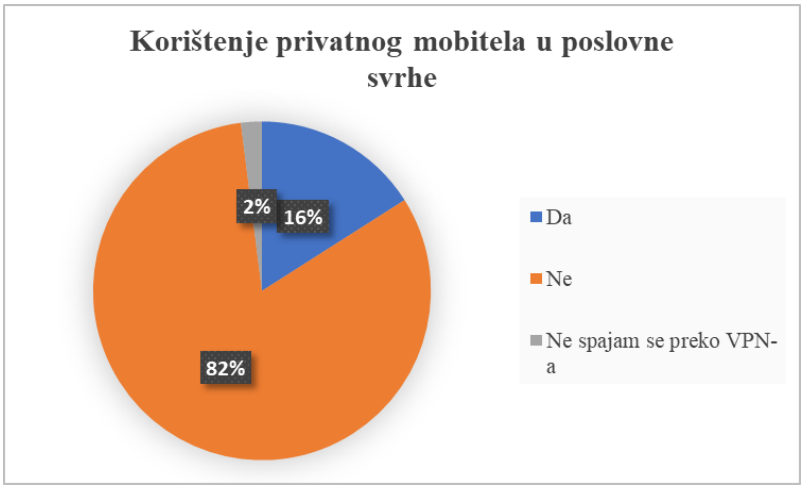


Slika 15 Zaštićenost poslovnih računala ispitanika

Izvor: samostalna izrada autorice rada

94% ispitanika smatra kako su njihova poslovna računala dovoljno zaštićena, dok samo 6% ispitanika smatra kako njihova poslovna računala ipak nisu dovoljno zaštićena.

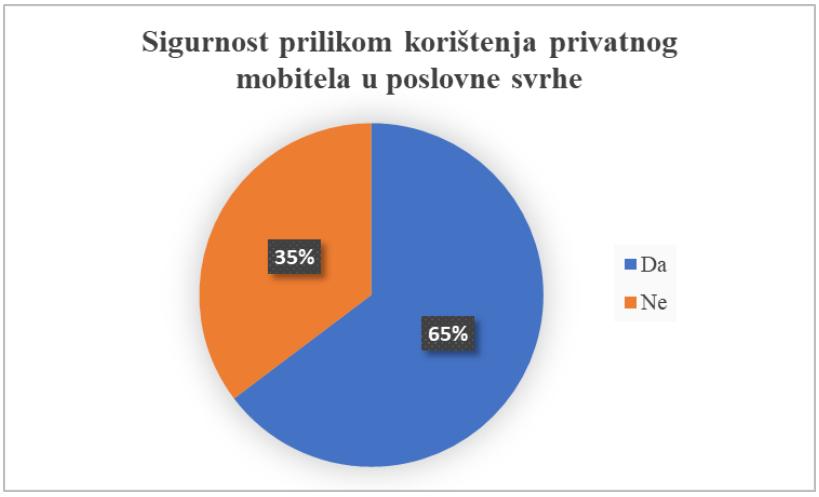
15. Ako se za rad u organizaciji morate spajati preko VPN-a, koristite li za to svoj privatni mobitel?
    a. Da
    b. Ne
    c. Ne spajam se preko VPN-a



Slika 16 Korištenja privatnog mobitela u poslovne svrhe

Izvor: samostalna izrada autorice rada

16. Ako ste na prethodno pitanje odgovorili sa "Da"; osjećate li se sigurno prilikom korištenja privatnog mobitela u poslovne svrhe?
    a. Da
    b. Ne



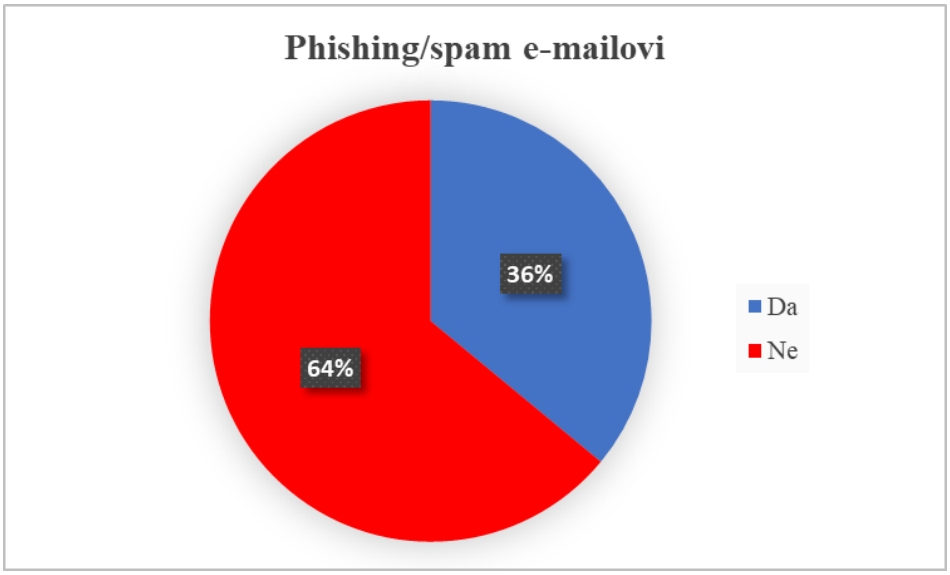
Slika 17 Sigurnost prilikom korištenja privatnog mobitela u poslovne svrhe

Izvor: samostalna izrada autorice rada

Iako 82% ispitanika ne koristi svoj poslovni mobitel kako bi se spojio na VPN, čak 16% ispitanika ipak koristi privatni mobitel u poslovne svrhe. Osim što korištenje privatnog mobitela u poslovne svrhe donosi brojne rizike, dodatno treba naglasiti da se od onih koji koriste privatni mobitel u poslovne svrhe 35% njih ne osjeća sigurno prilikom istog. Organizacije bi svakako trebale omogućiti svojim zaposlenicima sigurno okruženje, a

zaposlenici bi trebali obavijestiti nadređene ukoliko osjećaju nesigurnost prilikom korištenja privatnog mobitela u s poslovne svrhe.

17. Jeste li primijetili povećan broj phishing ili spam e-mailova u vašoj organizaciji od početka COVID-19 pandemije do danas?
    a. Da
    b. Ne

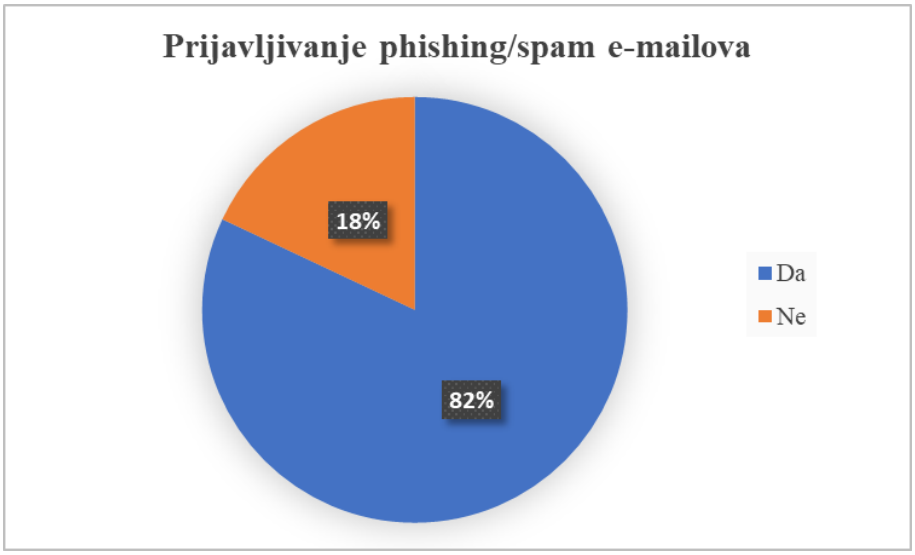


Slika 18 Phishing/spam e-mail-ovi

Izvor: samostalna izrada autorice rada

Bez obzira na povećan broj kibernetičkih napada općenito, 64% ispitanika tvrdi kako nije primijetilo povećan broj phishing niti spam e-mail-ova. Međutim, 34% ispitanika tvrdi kako se ipak povećao broj istih.

18. Prijavljujete li phishing ili spam e-mailove u svojoj organizaciji?
    a. Da
    b. Ne

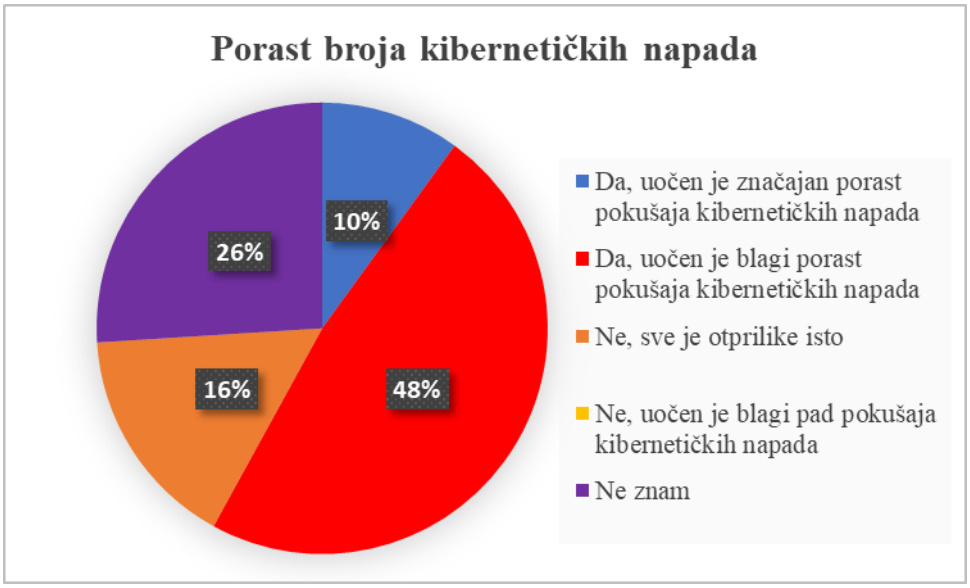


Slika 19 Prijavljivanje phishing/spam e-mail-ova

Izvor: samostalna izrada autorice rada

Slika 19 prikazuje kako 82% ispitanika tvrdi da redovito prijavljuje phishing i spam e-mail-ove. No, 18% ispitanika ne prijavljuje iste, stoga je i ova slika prikaz kako neke organizacije nisu uspostavile kvalitetno i sigurno okruženje za svoje zaposlenike. Kao što je već spomenuto u radu, otvaranje ovakvih e-mail-ova može dovesti do neželjenih posljedica te može ugroziti podatke organizacije jer se otvaranjem poveznica i privitaka iz takvih e-mail-ova mogu neprimjetno instalirati zlonamjerni softveri.

19. Je li vaša organizacija zabilježila porast broja pokušaja kibernetičkih napada (npr. krađa identiteta, napadi socijalnog inženjeringa, itd.) od početka karantene i rada od kuće do danas?
    a. Da, uočen je značajan porast pokušaja kibernetičkih napada (N=5)
    b. Da, uočen je blagi porast pokušaja kibernetičkih napada (N=24)
    c. Ne, sve je otprilike isto (N=8)
    d. Ne, uočen je blagi pad pokušaja kibernetičkih napada (N=0)
    e. Ne znam (N=13)

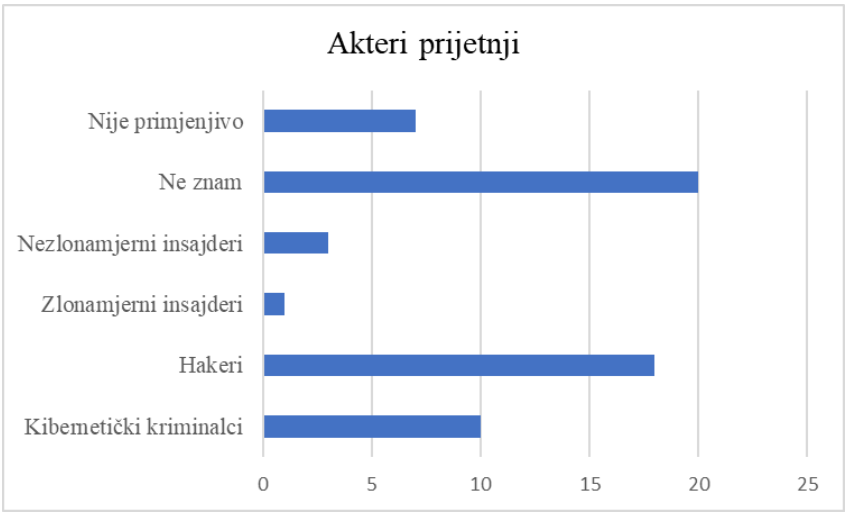


Slika 20 Porast broja kibernetičkih napada u doba pandemije

Izvor: samostalna izrada autorice rada

Slika 20 veže se na hipotezu istraživanja koja glasi da se broj kibernetičkih napada povećao u razdoblju pandemije. 48% zaposlenika odjela informacijske sigurnosti i odjela IT-a, koji su ispitani u sklopu ovog istraživanja, tvrde da su uočili blagi porast pokušaja kibernetičkih napada, a 10% uvidjelo je čak značajan porast istih.

20. Ako je vaša organizacija bila izložena kibernetičkim napadima u posljednje dvije godine, koji su od sljedećih aktera prijetnji bili krivi?
    - Kibernetički kriminalci (N=10, 20%)
    - Hakeri (N=18, 36%)
    - Zlonamjerni insajderi (N=1, 2%)
    - Nezlonamjerni insajderi (N=3, 6%)
    - Ne znam (N=20, 40%)
    - Nije primjenjivo (N=7, 14%)
    - Ostalo

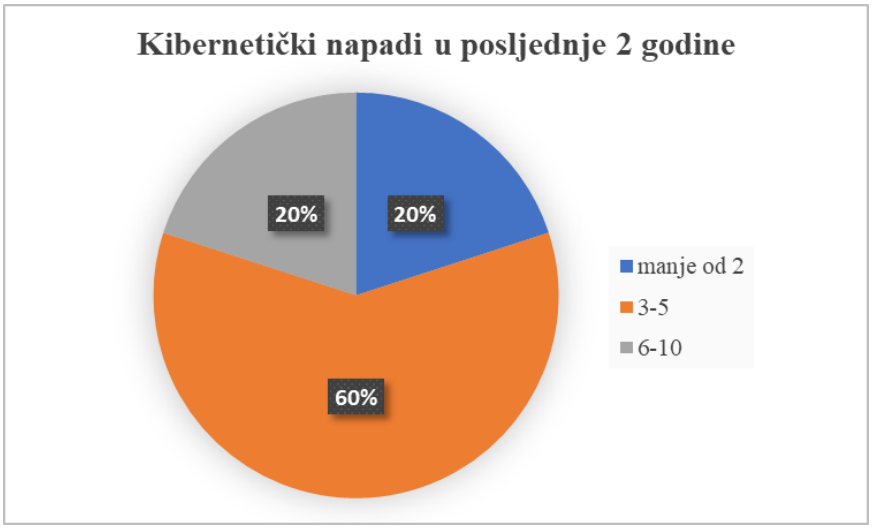


Slika 21 Akteri prijetnji koji su krivi za kibernetičke napade

Izvor: samostalna izrada autorice rada

Ispitanici čije su organizacije bile izložene kibernetičkim napadima tvrde da su hakeri najčešći akteri prijetnji (36%), a slijede ih kibernetički kriminalci (20%).

21. Za koliko ste kibernetičkih napada saznali putem vijesti, internetskih izvora, članaka i sl. u posljednje 2 godine (npr. curenje osobnih podataka klijenata i sl.)
    a. Manje od 2 (N=10)
    b. 3-5 (N=30)
    c. 6-10 (N=10)
    d. Ostalo

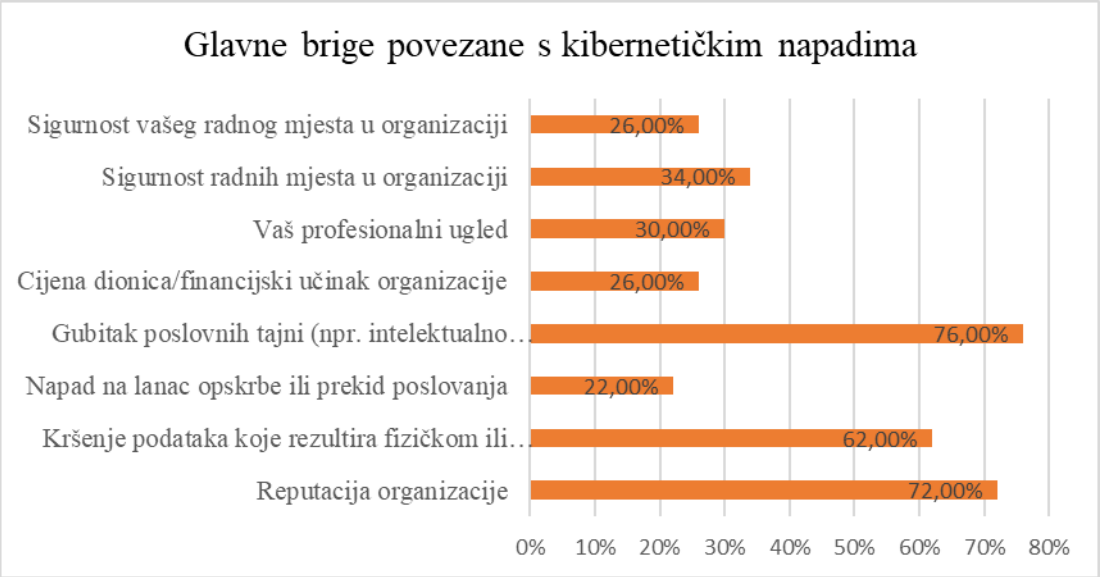


Slika 22 Kibernetički napadi u posljednje 2 godine

Izvor: samostalna izrada autorice rada

60% zaposlenika odjela informacijske sigurnosti i odjela IT-a, ispitanih u sklopu istraživanja, tvrde da su putem medija i internetskih izvora saznali za 3-5 kibernetičkih napada, dok podjednak postotak istih navodi da su čuli ili za manje od 2 ili za 6-10 kibernetičkih napada.

22. Koje bi bile vaše glavne brige u vezi s potencijalnim kibernetičkim napadom na vašu organizaciju?
    - Reputacija organizacije
    - Kršenje podataka koje rezultira fizičkom ili financijskom štetom korisnika
    - Napad na lanac opskrbe ili prekid poslovanja
    - Gubitak poslovnih tajni (npr. intelektualno vlasništvo)
    - Cijena dionica/financijski učinak organizacije
    - Vaš profesionalni ugled
    - Sigurnost radnih mjesta u organizaciji
    - Sigurnost vašeg radnog mjesta u organizaciji
    - Ostalo



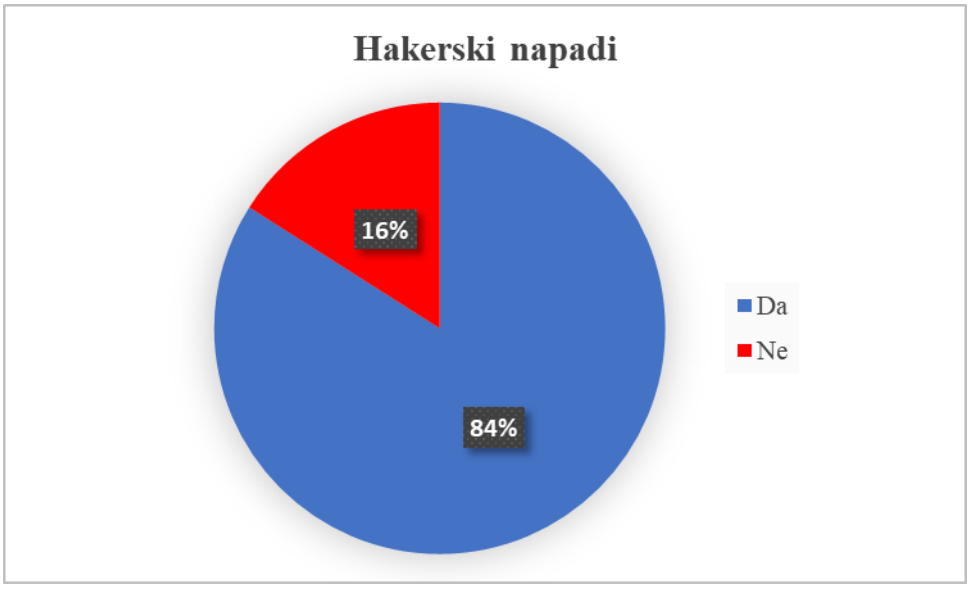
Slika 23 Glavne brige ispitanika u vezi s kibernetičkim napadima

Izvor: samostalna izrada autorice rada

Tri glavne brige ispitanika u vezi s kibernetičkim napadima su gubitak poslovnih tajni (76%), reputacija organizacije (72%) te kršenje podataka koje rezultira fizičkom ili financijskom štetom korisnika (62%). Prema ISACA istraživanju o Stanju kibernetičke

sigurnosti (2022) također su reputacija organizacije i kršenje podataka zauzela prva dva mjesta u glavnim brigama ispitanika.

23. Smatrate li da bi vaša organizacija uspješno izbjegla pokušaj hakerskog napada?
    a. Da (N=42)
    b. Ne (N=8)

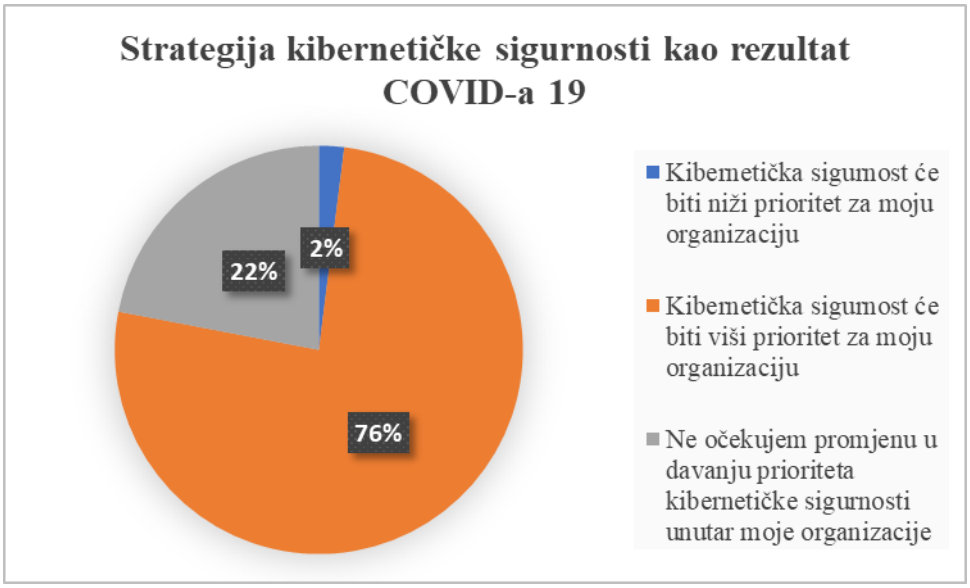


Slika 24 Stavovi ispitanika o hakerskim napadima

Izvor: samostalna izrada autorice rada

84% ispitanika tvrdi kako bi njihova organizacija uspješno izbjegla hakerski napad. No, prema prethodnim podacima iz istraživanja vidljivo je kako su neke organizacije već bile meta napadača, kako u nekim organizacijama nije uspostavljena procedura prijavljivanja neželjenih e-mail-ova, a i velik broj ispitanika nije prošao edukaciju prilikom prelaska na rad od kuće. Sukladno navedenome bitno je naglasiti kako ipak ne bi olako trebalo shvaćati kibernetičke napade. Bez obzira na povjerenje u kibernetičko okruženje organizacije, zaposlenici, a i menadžment trebali bi promijeniti svoje percepcije i prihvatiti činjenicu da su kibernetički napadi u doba pandemije ipak postali sofisticiraniji.

24. Po vašem mišljenju, kako će se strategija kibernetičke sigurnosti vaše organizacije promijeniti kao rezultat COVID-a 19?
    a. Kibernetička sigurnost će biti niži prioritet za moju organizaciju
    b. Kibernetička sigurnost će biti viši prioritet za moju organizaciju
    c. Ne očekujem promjenu u davanju prioriteta kibernetičke sigurnosti unutar moje organizacije



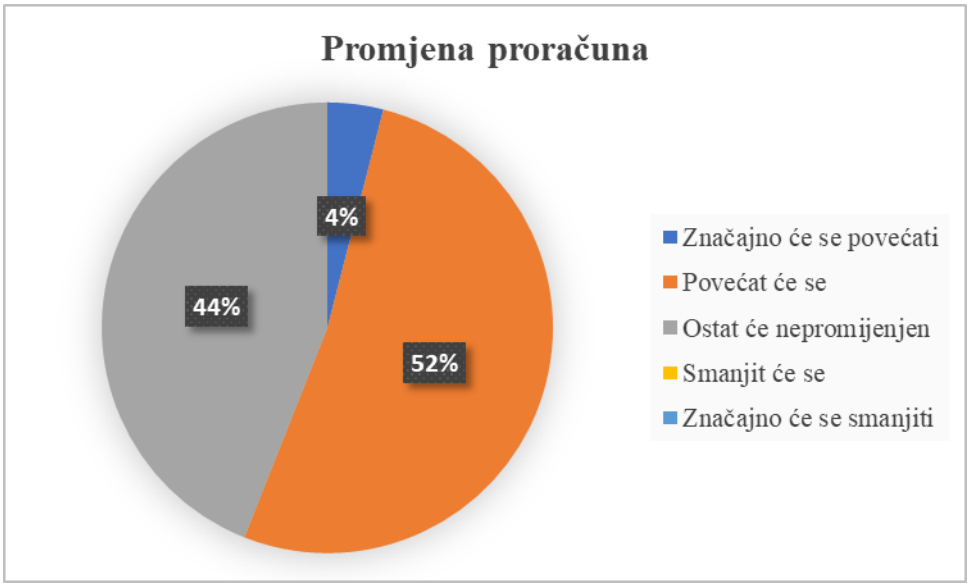
Slika 25 Strategija kibernetičke sigurnosti kao rezultat COVID-a 19

Izvor: samostalna izrada autorice rada

Značajan podatak u ovome istraživanju je taj da čak 76% ispitanika smatra kako će kibernetička sigurnost biti viši prioritet za njihovu organizaciju. Ove organizacije zasigurno će biti vodeće u valu inovacija procesa kibernetičke sigurnosti te primjeni najboljih praksi. Ono što predstavlja brigu je podatak da 20% organizacija smatra da ne očekuju promjenu u davanju prioriteta kibernetičkoj sigurnosti. Ukoliko ove organizacije nemaju zavidne procedure i sigurnosno okruženje, iste će potencijalno biti meta kibernetičkih napada.

25. Kako će se promijeniti proračun vaše organizacije za kibernetičku sigurnost u sljedećih 12 mjeseci?
    a. Značajno će se povećati (N=2)
    b. Povećat će se (N=26)
    c. Ostat će nepromijenjen (N=22)
    d. Smanjit će se (N=0)

e. Značajno će se smanjiti (N=0)

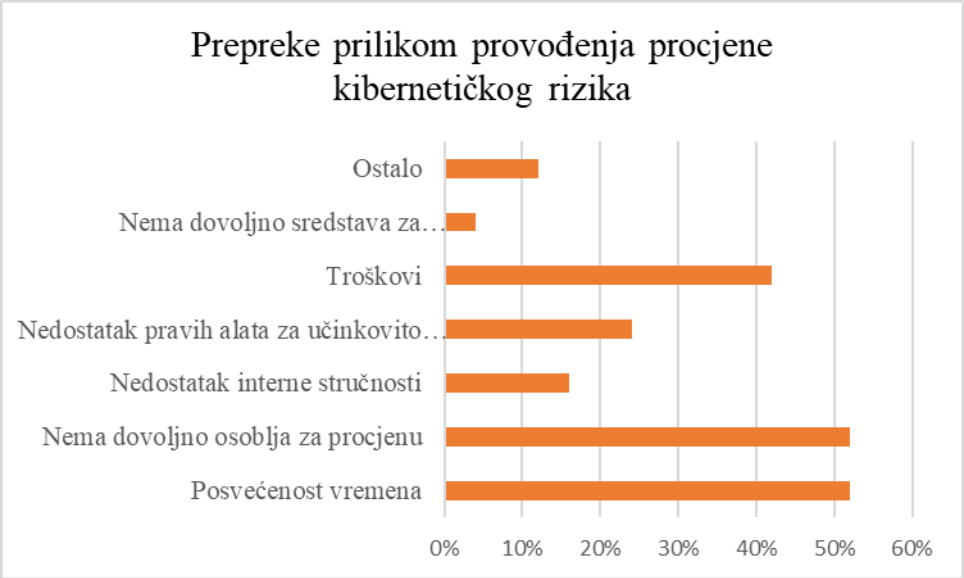


Slika 26 Promjena proračuna za kibernetičku sigurnost kao posljedica COVID-a 19

Izvor: samostalna izrada autorice rada

52% ispitanika pokazuje optimizam kada je u pitanju povećanje proračuna za kibernetičku sigurnost. 4% njih smatra da će se proračun za kibernetičku sigurnost značajno povećati, dok 44% njih smatra kako će proračun ostati nepromijenjen.

26. S kojim se preprekama, ako ih ima, vaša organizacija susreće u provođenju procjene kibernetičkog rizika?
    - Posvećenost vremena
    - Nema dovoljno osoblja za procjenu
    - Nedostatak interne stručnosti
    - Nedostatak pravih alata za učinkovito provođenje procjene
    - Troškovi
    - Nema dovoljno sredstava za eksternalizaciju trećoj strani
    - Ostalo

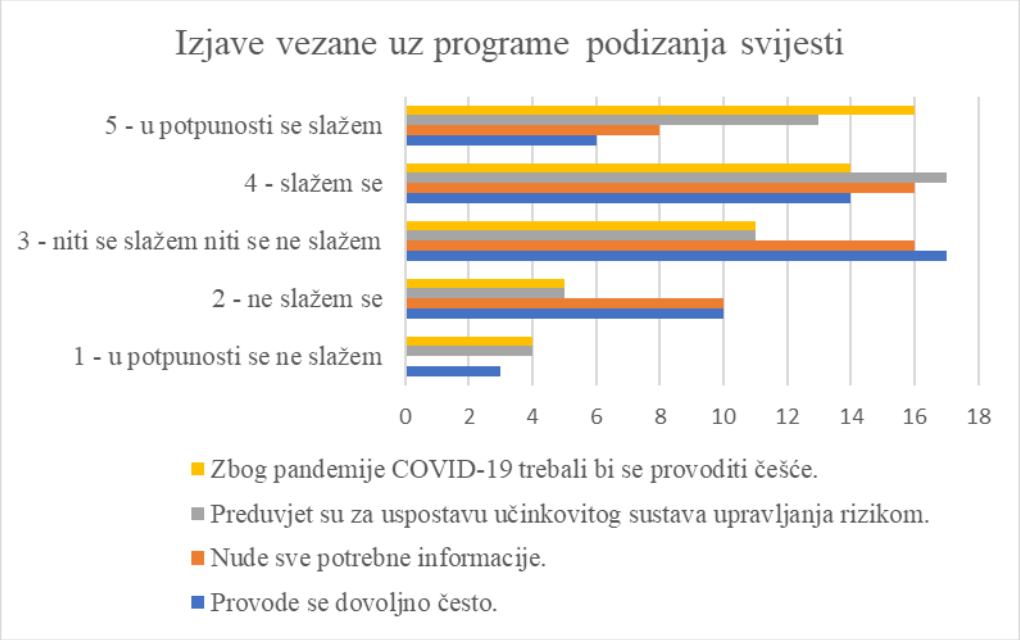


Slika 27 Prepreke prilikom provođenja procjene kibernetičkog rizika

Izvor: samostalna izrada autorice rada

Provođenje procjene kibernetičkog rizika ključno je za učinkovito praćenje čimbenika rizika i poboljšanje sposobnosti odgovora. Međutim, organizacije se susreću sa brojnim preprekama prilikom provođenja procjene. Ispitanici tvrde da su dvije najveće prepreke posvećenost vremena i nedostatak osoblja za procjenu (52%). U radu je već prethodno spomenuto kako nedostaje kompetentnih stručnjaka za kibernetičku sigurnost. Troškovi su također jedna od značajnijih prepreka (42%).

27. Označite u kojoj mjeri se slažete sa sljedećim izjavama vezanim za programe podizanja svijesti o kibernetičkoj sigurnosti. (1 - u potpunosti se ne slažem, 2 - ne slažem se, 3 - niti se slažem niti se ne slažem, 4 - slažem se, 5 - u potpunosti se slažem)
    - Provode se dovoljno često.
    - Nude sve potrebne informacije.
    - Preduvjet su za uspostavu učinkovitog sustava upravljanja rizikom.
    - Zbog pandemije COVID-19 trebali bi se provoditi češće.

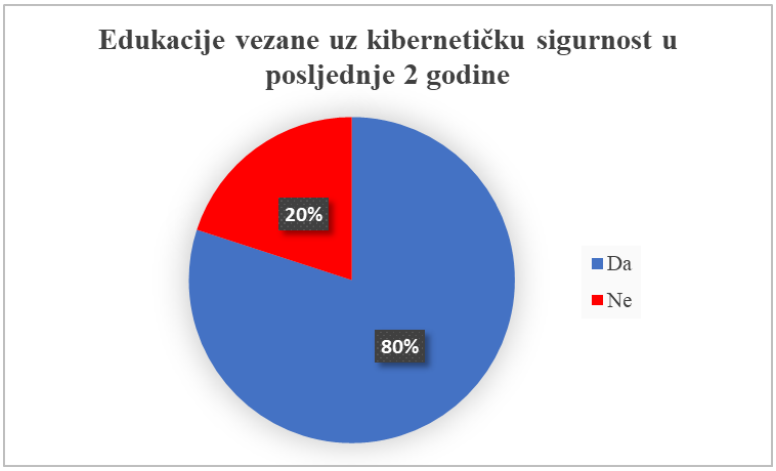


Slika 28 Izjave ispitanika vezane uz programe podizanja svijesti

Izvor: samostalna izrada autorice rada

Za izjavu da se programi podizanja svijesti o kibernetičkoj sigurnosti provode dovoljno često najviše ispitanika odgovorilo kako se sa navedenim ne može ni složiti niti ne složiti, a zatim slijede oni koji se slažu da se provode dovoljno često. Za izjavu da programi podizanja svijesti nude sve potrebne informacije jednak je broj ispitanika koji se s tim slaže s onima koji se s navedenom izjavom ne mogu ni složiti niti ne složiti. Ispitanici se slažu s izjavom da su programi podizanja svijesti preduvjet za uspostavu učinkovitog sustava upravljanja rizikom, a u potpunosti se slažu s izjavom da se zbog pojave pandemije COVID-19 trebaju provodi češće.

28. Jeste li u svojoj organizaciji u posljednje 2 godine sudjelovali u edukaciji vezanoj za kibernetičku sigurnost?
    a. Da (N=40)
    b. Ne (N=10)

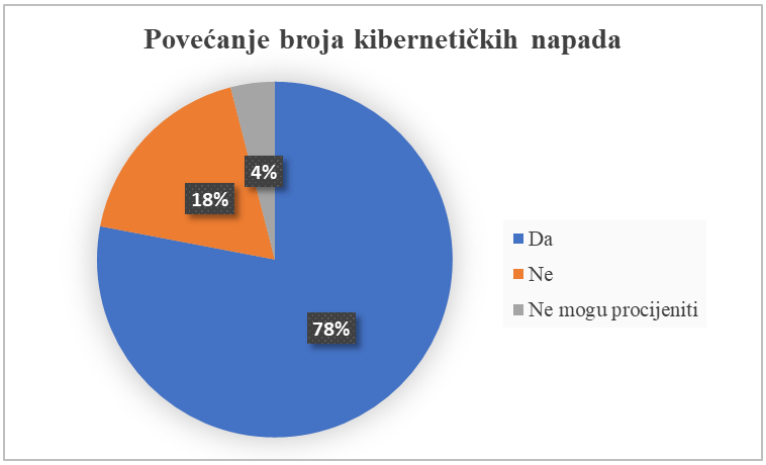


Slika 29 Edukacije vezane uz kibernetičku sigurnost u posljednje 2 godine

Izvor: samostalna izrada autorice rada

80% ispitanika tvrdi kako su u posljednje dvije godine sudjelovali u edukaciji vezanoj za kibernetičku sigurnost. Međutim, 2 godine je dugačak vremenski period, a 20% ispitanika nije sudjelovalo u istima. Bitno je da sve organizacije redovito i kontinuirano provode edukacije zaposlenika, pogotovo u razdoblju pandemije i pogotovo ukoliko su prihvatili hibridan način rada kao svoju poslovnu praksu.

29. Smatrate li (osobno) da se broj kibernetičkih napada povećao od početka COVID-19 pandemije do danas?
    a. Da (N=39)
    b. Ne (N=9)
    c. Ne mogu procijeniti (N=2)



Slika 30 Stavovi ispitanika o povećanju broja kibernetičkih napada u razdoblju pandemije

Izvor: samostalna izrada autorice rada

78% ispitanika smatra da se broj kibernetičkih napada povećao od početka COVID-a 19 do danas, dok 18% smatra da se broj kibernetičkih napada nije povećao.

Rezultati istraživanja pokazali su da su hipoteze postavljene na početku istinite, odnosno da se broj kibernetičkih napada povećao u razdoblju pandemije, da velik broj zaposlenika i dalje radi od kuće te da značajan postotak zaposlenika nije prošao kroz edukacije o kibernetičkoj sigurnosti prije prelaska na rad od kuće. Dodatno, istraživanje je pokazalo da značajan postotak zaposlenika smatra da će kibernetička sigurnost biti veći prioritet za njihovu organizaciju što znači da su organizacije svjesne rizika koji su proizašli pojavom pandemije COVID-a 19. Međutim, napori kako bi se postiglo isto iziskuju vrijeme i ljudski kapital, a oba su deficitarna u organizacijama, što je vidljivo i u istraživanju. Kako bi kibernetička sigurnost uistinu postala viši prioritet za organizacije potrebno je omogućiti dostatne resurse. Također, putem istraživanja moguće je zaključiti kako će hibridan način rada postati redovna poslovna praksa mnogim organizacijama. Kako bi hibridan način rada bio efektivan kao i rad iz uredskog okruženja, potrebno je postaviti dobre komunikacijske i sigurnosne temelje.

5. Rješenja i preporuke vezane uz kibernetičku sigurnost

Pandemija COVID-a 19 zasigurno će postaviti područje kibernetičke sigurnosti na jedan od viših prioriteta svake organizacije. U prethodnim poglavljima navedene su ranjivosti koje organizacije dovode do neefikasnih i propusnih informacijskih sustava koji su laka meta za napadače. Da bi organizacije mogle efikasnije upravljati svojim informacijskim sustavima potrebna je primjena kontrola koja omogućavaju zaštitu istih. Spremić (2017) navodi da se svrha informatičkih kontrola očituje u smanjenju vjerojatnosti da će doći do određenih gubitaka ili neželjenih događaja. Dodano, Spremić (2017) navodi kako se informatičke kontrole razlikuju prema više kriterija, a to su način primjene, svrha, hijerarhijska razina te način funkcioniranja. Nije cilj implementirati što više kontrola u određeni informacijski sustav nego da implementirane kontrole budu što učinkovitije. Svakoj organizaciji koja ima razvijene informacijske sustave navedene su kontrole već poznate i obvezne u primjeni.

U nastavku su navedene samo neke od preporuka kako bi se smanjile potencijalne ranjivosti uočene u razdoblju pandemije COVID-a 19:

i. **Informiranje**

   Kako je vidljivo i u provedenom istraživanju 84% zaposlenika smatra da bi njihova organizacija uspješno izbjegla hakerski napad. Takva uvjerenja imaju i zaposlenici i menadžeri. Navedeno se može promijeniti ako se zaposlenike konstantno informira o kibernetičkim napadima i o kibernetičkoj sigurnosti. Na primjer organizacija bi mogla implementirati da u određenom periodu (npr. svakih deset dana) putem e-pošte šalje zaposlenicima primjere napada koji su se dogodili u tom razdoblju te ih informira o vjerojatnosti događaja istog ili sličnog napada u njihovoj organizaciji. Uspostavljanje dijaloga sa zaposlenicima i pravovremeno informiranje o kibernetičkoj sigurnosti pomoći će u oblikovanju uvjerenja i interesa organizacije (Fichtenkamm, F. Burch i Burch, 2022).

ii. **Pravovremene radnje**

   Menadžeri moraju pronaći načine da promjene stavove svojih zaposlenika po pitanju kibernetičke sigurnosti (18% ispitanika ne prijavljuje neželjenu e-poštu). Prvenstveno je potrebno da svaka organizacija ima uspostavljenju politiku za upravljanje kibernetičkom sigurnosti te da prema njoj propiše koliko često i u kojoj mjeri će se provoditi programi podizanja svijesti i edukacije zaposlenika o kibernetičkoj sigurnosti. Od početka pandemije prošlo je već izvjesno razbolje te su

organizacije do sada trebale uspostaviti određene mjere zaštite npr. osigurati računalne uređaje s ažuriranim softverima za sve zaposlenike koji rade od kuće, omogućiti sigurnu konfiguraciju mreže (uključujući VPN), omogućiti zaštitu od zlonamjernog softvera na svim računalnim uređajima, ukloniti sve osobne uređaje iz mreže, češće revidirati korisničke privilegije, osobito privilegirane korisnike te periodično revidirati uređaje zaposlenika.

Brojne od ovih mjera u nekim organizacijama bile su implementirane i prije pandemije. No, pojavom pandemije organizacije su mjere sigurnosti pomaknule na niži prioritet (Fichtenkamm, F. Burch i Burch, 2022).

iii. Okruženje

Nakon usvojenih metoda potrebno je da organizacije pojačaju praćenje aktivnosti svojih zaposlenika i prijetnji u novom okruženju (82% ispitanika i dalje povremeno radi od kuće). Bitno je da njihove metode upravljanja kibernetičkom sigurnosti ne ostanu na istoj razini kao i prije pandemije, odnosno potrebno je restrukturirati postojeće procese i metode tako da odgovaraju trenutnim zahtjevima ovog neizvjesnog razdoblja. Navedeno uključuje povećanje ulaganja u kibernetičku sigurnost i postavljanje kibernetičke sigurnosti na veći organizacijski prioritet. Samim time, organizacije bi trebale omogućiti dovoljan broj kibernetičkih stručnjaka koji će svoje vrijeme posvetiti zašiti informacijskih sustava i organizacije općenito. Fichtenkamm, F. Burch i Burch (2022) navode da korištenje umjetne inteligencije, automatizacije ili usvajanje sigurnosnog okvira nultog povjerenja (engl. zero trust security framework) može biti neophodno u trenutnom neizvjesnom okruženju.

Sumarno, IT menadžeri moraju imati širi pogled i početi razmišljati kao kibernetički kriminalci kako bi razvili najefikasnije protokole za upravljanje rizikom. Navedeno uključuje identifikaciju kritične infrastrukture, analizu postojećih i mogućih rizika te razvijanje akcijskih planova za uklanjanje i/ili minimiziranje rizika. Organizacije bi trebale češće provoditi penetracijska testiranja kao i simulacije krize kako bi educirali zaposlenike o ponašanju u hitnim situacijama. Kao što je već navedeno, mjere, postupci i pogled na kibernetičku sigurnost ne mogu ostati isti budući da se u razdoblju pandemije promijenio i kibernetički svijet (Fichtenkamm, F. Burch i Burch, 2022). Dodatno, Arbanas, Spremić i Zajdela Hrustek (2021) navode važnost uravnoteženog pristupa u području informacijske

sigurnosti, odnosno smatraju da je potrebno uključivanje društveno-organizacijskog konteksta. Navedeno proizlazi iz činjenice da informacijska sigurnost više nije samo tehničko pitanje nego i ljudski problem koji zahtijeva uključenost višeg rukovodstva i potrebu za proučavanjem kulture informacijske sigurnosti na holistički način.

6. Zaključak

Ključni cilj kibernetičke sigurnosti je uspostava mjera koje će spriječiti ili ublažiti pojavu prijetnji. Intenzivna i aktivna primjena digitalne i informacijske tehnologije, kao i pojava pandemije, postavile su kibernetičke sigurnosne zahtjeve na jednu potpuno novu razinu. Pojavom pandemije korona virusa područje kibernetičke sigurnosti doživjelo je mnoge promjene. Od otkrivanja novih ranjivosti i prijetnji do suočavanja sa zahtjevima koji bi mogli biti potencijalne prilike za rast.

Samoizolacije, mjere socijalne distance i sl. usmjerile su organizacije na rad od kuće, a sigurnosno okruženje u koje su radnici odlazili raditi nije bilo dovoljno sigurno. Bez obzira na brzu prilagodbu organizacija na nove načine rada i upravljanja, promjene su donijele i posljedice. Iz sigurnosne perspektive, organizacije se suočavaju s porastom kibernetičkih prijetnji, potaknutih prijevarama vezanim uz COVID-19 i povezanim porastom kibernetičkog kriminala.

Budući da je sva komunikacija u doba pandemije bila prebačena na virtualne platforme, smanjila se komunikacija među timovima što je utjecalo na unutar organizacijske odnose. Provedeno istraživanje pokazalo je kako su organizacije usvojile hibridan način rada te zaposlenici povremeno rade od kuće, a povremeno iz ureda. Ovakve brze promjene i prihvaćanje u potpunosti novog načina upravljanja donijele su sa sobom pojavu dodatnih rizika i ranjivosti. COVID-19 i rad od kuće morat će promijeniti prioritete sigurnosnih stručnjaka, ako već nisu, a zasigurno su povećali opterećenje i promijenili njihove interne navike.

Sukladno navedenome, važno je da organizacije postanu svjesne važnosti značenja i upravljanja kibernetičkom sigurnosti u današnje vrijeme koje predstavlja temelj za stabilan i siguran informacijski sustav kao i njegovo okruženje. Prema istraživanju čini se da je sada rad od kuće „novo normalno“, a većina stručnjaka za kibernetičku sigurnost očekuje da će njihove organizacije biti fleksibilnije u pogledu istog i nakon što pandemija u potpunosti završi. S obzirom na to, stručnjaci za kibernetičku sigurnost trebali bi biti spremni distribuirati sigurnosne kontrole, modificirati politike i pojačati prikupljanje, obradu i analitiku sigurnosnih podataka. Da bi sve od navedenog bilo moguće važno je da sve organizacije pravovremeno procjene okruženje u kojem posluju, informiraju i educiraju zaposlenike o ponašanju prilikom rada od kuće i rada iz ureda. Međutim, ono što je trenutno najbitnije je educirati studente koji mogu postati budući kibernetički stručnjaci i popuniti

prazna mjesta u odjelima informacijske sigurnosti. Kibernetička sigurnost je toliko važna da nedostatak vremena i nedostatak osoblja ne bi trebali biti izgovori za neprovođenje sigurnosnih mjera, pogotovo ne u neizvjesnim razdobljima, kao što je ovo.

Popis literature

1. AAI@EduHr (2008.), Pravilnik o ustroju autentifikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr (verzija 1.3.1.) [EPub], preuzeto 1.7.2022. s https://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf
2. Arbanas, K., Spremić, M., Zajdela Hrustek, N. (2021.), Holistic framework for evaluating and improving information security culture, preuzeto 1.7.2022. s https://www.bib.irb.hr/1140143
3. Burg, D., Maddison, M., Watson, R. (2021.), EY Global Information Security Survey 2021, preuzeto 31.1.2022. s https://www.ey.com/en_vn/ey-global-information-security-survey-2021
4. CIS (2011.), Advanced Persistent Threat napadi [EPub], preuzeto 1.7.2022. s https://www.cis.hr/files/dokumenti/CIS-DOC-2011-11-031.pdf
5. Cvitić, I., Peraković, D., Periša, M., Jurcut, A. D. (2021.), Methodology for Detecting Cyber Intrusions in e-Learning Systems during COVID-19 Pandemic, preuzeto 31.1. 2022. s https://link.springer.com/article/10.1007/s11036-021-01789-3
6. DesJardins, S. (2014.), Cyber Attacked: Could You Be Next?, preuzeto 1.7.2022. s https://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1025&context=honorscollege_business
7. Ferreira, A., Cruz-Correia, R.J. (2020.), COVID-19 and cybersecurity: finally, an opportunity to disrupt?, preuzeto 1.7.2022. s https://www.researchgate.net/publication/349907348_COVID19_and_cybersecurity_finally_an_opportunity_to_disrupt_Preprint
8. Fichtenkamm, M., F. Burch, G., Burch, J. (2022.), Cybersecurity in a COVID-19 World [EPbub], preuzeto 1.7.2022. s https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2022/volume-2/cybersecurity-in-a-covid-19-world_joa_eng_0422.pdf
9. Firch, J. (2021.), 10 Cyber Security Trends You Can't Ignore In 2021, preuzeto 31.1.2022. s https://purplesec.us/cyber-security-trends-2021/
10. ISACA (b.d.), Glossary [EPub], preuzeto 1.7.2022. s https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/glossary.pdf

11. ISACA (2021.), Navigating the 2021 Cyberthreat Landscape [EPub], preuzeto 1.7.2022. s https://www.isaca.org//media/files/isacadp/project/isaca/resources/infographics/state-of-cybersecurity-2021-part-2-infographic_0721.pdf
12. ISACA (2019.), State of Cybersecurity 2019 Part 2: Current Trends in Attacks, Awareness and Governance [EPub], preuzeto 1.7.2022. s https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619
13. ISACA (2022.), State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations, preuzeto 20.6.2022. s https://www.isaca.org/go/state-of-cybersecurity-2022
14. Isam, Z., R. Banoon, S., Kadhim Lawi, Z.K. (2021.), Review about COVID-19, preuzeto 1.7.2022. s https://www.researchgate.net/publication/350344822_Review_about_COVID-19
15. Kaufman, G., Taniguchi, H. (2021.), Working from Home and Changes in Work Characteristics during COVID-19, preuzeto 31.1.2022. s https://journals.sagepub.com/doi/epub/10.1177/23780231211052784
16. Khan, N.A., Brohi, S.N., Zaman, N. (2020.), Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic, preuzeto 31.1.2022. s https://www.researchgate.net/publication/341324576_Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic
17. Meinert, E. (2021.), COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt, preuzeto 31.1.2022. s https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8104279/
18. Nabe, C. (2021.), Impact of COVID-19 on Cybersecurity, preuzeto 31.1.2022. s https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
19. O'Donnell, B. (2022.), 5 cybersecurity myths and how to address them, preuzeto 1.7.2022. s https://www.techtarget.com/whatis/post/5-cybersecurity-myths-and-how-to-address-them

20. Oltsik, J. (2020.), ESG Research Report: The Impact of the COVID-19 Pandemic on Cybersecurity, preuzeto 20.6.2022. s https://www.esg-global.com/research/esg-research-report-the-impact-of-the-covid-19-pandemic-on-cybersecurity

21. PwC (2020.), Managing the impact of COVID-19 on cyber security, preuzeto 31.1.2022. s https://www.pwc.com/jg/en/topics/covid-19/managing-impact-of-covid-19-on-cyber-security.html

22. Roohparvar, R. (2022.), Common Cybersecurity Myths Busted, preuzeto 1.7.2022. s https://www.infoguardsecurity.com/common-cybersecurity-myths-busted/

23. Sailio, M., Latvala, O., Szanto, A. (2020.), Cyber Threat Actors for the Factory of the Future, preuzeto 1.7.2022. s https://www.researchgate.net/publication/342426828_Cyber_Threat_Actors_for_the_Factory_of_the_Future

24. Singh Lallie, H., Shepherd, L.A., Nurse, J., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021.), Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, preuzeto 31.1.2022. s https://www.researchgate.net/publication/349845621_Cyber_Security_in_the_Age_of_COVID-19_A_Timeline_and_Analysis_of_Cyber-Crime_and_Cyber-Attacks_during_the_Pandemic

25. S. Jalali, M., D. Siegel, M., E. Madnick, S. (2018.), Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment, preuzeto 1.7.2022. s https://www.researchgate.net/publication/327825777_Decision-making_and_biases_in_cybersecurity_capability_development_Evidence_from_a_simulation_game_experiment

26. Spremić, M. (2017.), Digitalna transformacija poslovanja, Sveučilište u Zagrebu, Ekonomski Fakultet

27. Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Ekonomski Fakultet

28. Zakon o informacijskoj sigurnosti, Narodne novine br. 79/2007 (2007.)

29. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine br. 64/18 (2018.)

30. Wang, L., Alexander, C.A. (2021.), Cyber security during the COVID-19 pandemic, preuzeto 31.1.2022. s https://www.aimspress.com/aimspress-data/electreng/2021/2/PDF/electroneng-05-02-008.pdf

Popis tablica

Popis slika

Životopis studenta

Petra Perković

Datum rođenja: 05/06/1998 | **Državljanstvo:** hrvatsko | (+385) 915008857 |

perkovicp1@gmail.com | Zagreb, Hrvatska

RADNO ISKUSTVO

16/11/2020 – TRENUTAČNO – Zagreb, Hrvatska

IT AUDIT INTERN – ERNST&YOUNG SAVJETOVANJE D.O.O

- ispitivanje i pregled dokumenata kako bi se osiguralo poštivanje politika i postupaka poduzeća i odjela
- priprema radnih revizijskih dokumenata
- izrada raznih IT testova
- sudjelovanje na regulatornim revizijama
- sudjelovanje na AQR projektu
- samostalno vođenje sastanaka
- komunikacija s klijentima

09/2019 – 11/2019 – Zagreb, Hrvatska

TAJNICA – CROATA (POTOMAC D.O.O.)

- preuzimanje pošte
- ovjera dokumenata
- organizacija registratora
- povremeni odlazak kod javnih bilježnika

07/2019 – 08/2019 – Zagreb, Hrvatska

ADMINISTRATORICA – MIKROCOP D.O.O.

- provjera i unos anketa u digitalne sustave
- organizacija registratora

OBRAZOVANJE I OSPOSOBLJAVANJE

2017 – 09/2022 – Hrvatska

STUDENTICA – Sveučilište u Zagrebu, Ekonomski fakultet - smjer Menadžerska informatika

https://www.efzg.unizg.hr/

JEZIČNE VJEŠTINE

Materinski jezik/jezici: **HRVATSKI**

Drugi jezici:

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna produkcija	Govorna interakcija	
ENGLESKI	C1	C1	B2	C1	B2

Razine: A1 i A2: temeljni korisnik; B1 i B2: samostalni korisnik; C1 i C2: iskusni korisnik

DIGITALNE VJEŠTINE

Moje digitalne vještine

MS Office (Word Excel PowerPoint) | Rad na računalu | Timski rad | Organiziranost | Razvijene komunikacijske vještine | Samostalnost u obavljanju zadataka | Celonis Process Mining Certificate