Utjecaj znanja na kibertnetičku sigurnost poslovne organizacije

Bobić, Tomislav

SVEUČILIŠTE SJEVER
SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 390/PE/2022

UTJECAJ ZNANJA NA KIBERNETIČKU SIGURNOST POSLOVNE ORGANIZACIJE

Tomislav Bobić

Varaždin, srpanj 2022.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij: Poslovna ekonomija

DIPLOMSKI RAD br. 390/PE/2022

UTJECAJ ZNANJA NA KIBERNETIČKU SIGURNOST POSLOVNE ORGANIZACIJE

Student:

Tomislav Bobić,0135179700

Mentor:

izv.prof.dr.sc. Ljerka Luić

Varaždin, srpanj 2022.

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR-42000 Varaždin

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL: Odjel za ekonomiju

STUDIJ: diplomski sveučilišni studij Poslovna ekonomija

PRISTUPNIK: Tomislav Bobić | MATIČNI BROJ: 0135179700

DATUM: 10. 6. 2022. | KOLEGIJ: Informacijska sigurnost i zaštita podataka

NASLOV RADA: Utjecaj znanja na kibernetičku sigurnost poslovne organizacije

NASLOV RADA NA ENGL. JEZIKU: The impact of knowledge on cybersecurity in business organizations

MENTOR: izv. prof. dr. sc. Ljerka Luić | ZVANJE: doktor znanosti

ČLANOVI POVJERENSTVA:
1. prof. dr. sc. Ante Rončević, predsjednik
2. doc. dr. sc. Petar Mišević, član
3. izv. prof. dr.sc. Ljerka Luić, mentor
4. prof. dr. sc. Anica Hunjet, zamjenski član
5.

Zadatak diplomskog rada

BROJ: 390/PE/2022

OPIS:

U uvodnom dijelu rada potrebno je elaborirati teorijski okvir problematike kojom se rad bavi, obrazložiti cilj i predmet istraživanja, izvore podataka, metode i metodologiju istraživanja. Potom je potrebno dati prikaz strukture rada kroz kratki opis sadržaja rada te navesti istraživačko pitanje i hipoteze.

U poglavljima koja slijede potrebno je: (1) Dati određenje ključnih pojmova vezanih uz temu rada te na osnovu pregleda relevantne literature iznijeti spoznaje dosadašnjih istraživanja kibernetičke sigurnosti sagledane iz povijesnog i tehnološkog aspekta; potom je potrebno (2) Sistematično prikazati utjecaj udaljenog načina rada na povećani broj kibernetičkih napada, a u nastavku rada zadanu temu obraditi kroz istraživačko pitanje: "Kakav utjecaj ima znanje na kibernetičku sigurnost poslovne organizacije?". U drugom dijelu rada potrebno je (3) Opisati materijal i metodologiju istraživanja, potom vizualno i deskriptivno (4) Prikazati rezultate istraživanja provedenog primjenom SPSS alata, te u okviru diskusije (5) Elaborirati postavljene hipoteze i kroz odgovor na istraživačko pitanje (6) Sistematizirati zaključke do kojih se došlo, ocijeniti ostvarenje cilja istraživanja i predložiti korake za podizanje znanja o kibernetičkoj sigurnosti unutar poslovnih organizacija.

ZADATAK URUČEN: 28. 07. 2022. | POTPIS MENTORA:

SVEUČILIŠTE SJEVER

SAŽETAK

Kibernetička sigurnost danas predstavlja sve češći pojam kada se govori o digitalnoj transformaciji i hibridnom načinu rada. Razvoj znanja koja su potrebna za svladavanje izazova budućnosti i prilagodbe zaposlenika na nove tehnologije ključni su za poslovanje svake poslovne organizacije. Ovaj rad u teorijskom dijelu daje prikaz povijesnog razvoja kibernetičkih prijetnji, vrste napada i načine zaštite od istih, definira što je znanje te koji su suvremeni oblici pismenosti. Glavno istraživanje koje je provedeno kroz anketu fokusirano je na utjecaj znanja na kibernetičku sigurnost poslovne organizacije te utjecaj COVID-19 pandemije na prelazak na udaljeni način rada (rad od kuće) koji je omogućio veći broj kibernetičkih napada. Kroz anketu su testirane dvije hipoteze kao i odgovor na istraživačko pitanje. Nadalje, ista je provedena na 168 ispitanika te kroz istraživanje dostupnih materijala koji su usmjereni na kibernetičku sigurnost u doba COVID-19 pandemije. Dobivenim rezultatima potvrđena je povezanost znanja i kibernetičke sigurnosti poslovne organizacije je utjecaj COVID-19 pandemije na povećani broj kibernetičkih napada radi promjene načina rada (rad od kuće). Radi specifičnosti teme u radu su korišteni izrazi iz engleskog govornog područja.

Ključne riječi: znanje, kibernetička sigurnost, poslovne organizacije, COVID-19, rad od kuće

SUMMARY

Cybersecurity today is a hot topic when discussing digital transformation and hybrid whey of work. Developing knowledge necessary to manage future challenges and adjusting employees to new technologies is critical for any business organization. This document has a theoretical part that shows the development of cybersecurity threats through history, the most common cybersecurity attacks, the ways we can protect ourselves from them, and what knowledge and modern types of literacy are. The primary research has been done through questionnaires focused on how the knowledge of people that work in an organization affects the cybersecurity of that organization and how the COVID-19 pandemic has impacted work from home that has allowed cybercriminals to attack more. Testing of two hypotheses and the answer to the main question was given thru questionnaires that 168 persons answered and thru materials that were focused on cybersecurity in COVID times. The results confirmed that the knowledge of employees has a direct impact on the cybersecurity of business organizations and that COVID-19 pandemic has impacted on a high number of cyberattack!

Key words: knowledge, cyber security, business organizations, COVID-19, work from home

Popis korištenih kratica

CPU - Central Processing unit (centralna jedinica za obradu podataka)

SQL - Structured Query Language (standardni jezik upita)

IKT - Informacijska komunikacijska tehnologija

OECD - Organisation for Economic Co-operation and Development (organizacija za ekonomsku suradnju i razvoj)

ARPANET - advanced research projects agency network (napredna istraživačka mreža za projekte)

XSS – Cross site scripting (skriptiranje na više web mjesta)

HTML – Hyper text markup language (prezentacijski jezik za izradu web stranica)

DOS – Denial of service (odbijanje usluge)

DDOS – Distributed denial of service (distribuirano odbijanje usluge)

WPA – Wi Fi protected access (zaštićeni pristup mreži)

DHCP – dinamic host configuration protocol (dinamički protokol za konfiguraciju)

MAC- adresa kontrole pristupa

XDR – xtended detection and response (napredno detektiranje i odgovor)

DLP- data loss prevention (prevencija gubitaka podataka)

BEC – business email compromise (kompromitiranost poslovnim mailova)

SADRŽAJ

1. Uvod ... 1

1.1. Predmet i cilj rada ... 2

1.2. Izvori podataka i metode prikupljanja ... 2

1.3. Istraživačko pitanje i hipoteze rada ... 3

1.4. Struktura rada ... 3

2. Suvremene poslovne organizacije ... 5

2.1. Poslovni informacijski sustavi ... 6

2.2. Tehnološki aspekt ... 7

2.2.1. Hardver ... 7

2.2.2. Softver ... 8

2.3. Organizacijski aspekt ... 9

2.3.1. Liveware ... 9

3. Znanje ... 11

3.1. Upravljanje znanjem ... 12

3.2. Suvremeni oblici pismenosti ... 13

4. Kibernetički napadi i zaštita ... 17

4.1. Povijesni pregled ... 17

4.2. Trenutno stanje ... 20

4.2.1. Vrste hakera i njihovi motivi ... 20

4.2.2. Vrste zlonamjernih softvera ... 22

4.3. Načini zaštite ... 24

4.4. Komercijalna rješenja za zaštitu od kibernetičkih napada ... 27

5. Materijali i metode ... 30

5.1. Istraživački materijali ... 30

5.2. Metode istraživanja ... 30

5.3. Postupak provedbe istraživanja ... 31

5.4. Metode obrade podataka ... 31

6. Rezultati istraživanja ... 33

6.1. Rezultati desk-metoda ... 33

6.2. Rezultati ankete field-metoda ... 38

7. Diskusija rezultata ... 46

7.1. Interpretacija rezultata istraživanja ... 46

7.2. Elaboracija istraživačkog pitanja i hipoteza ... 47

7.3. Primjena rezultata i preporuke ... 47

8. Zaključak ... 49

9. Popis literature 50
Popis ilustracija 52
Prilog 1. Anketni upitnik 54

1. Uvod

Da nema nedodirljivih i da kibernetičke prijetnje i u Hrvatsku ulaze na velika vrata, ukazuje sve veći broj hakerskih napada. Na ranjivost informatičkih sustava stručnjaci iz cijelog svijeta upozoravaju odavno no čini se da je svijest i zainteresiranost zaposlenika i dalje na niskoj razini. Samim time ne čudi što prosječni djelatnik neke poslovne organizacije ne zna što je to kibernetička sigurnost i na koji se način zaštititi. Prema Državnom zavodu za statistiku uporaba mobilnog širokopojasnog pristupa internetu je porasla za 13% u odnosu na prošlu godinu te je preko 46% korisnika interneta kupovalo robu i usluge putem interneta. Kada se pogledaju brojevi za poslovne organizacije 94 % poduzeća upotrebljava računala s pristupom internetu a 69% poduzeća ima vlastitu mrežnu stranicu. Cloud uslugama se koristi 39% poduzeća. (https://novac.jutarnji.hr/novac/next/pojedinci-koriste-internet-najvise-za-slanje-poruka-informacije-o-proizvodima-i-citanje-dnevnih-novosti-15130105 pristupio 8.6.2022)

Kibernetička sigurnost je skup procesa i mjera kojima se štite računala, mreže i podaci od malicioznih napada. Kibernetička sigurnost je važna iz mnogo različitih razloga, a tri najbitnija su: zaštita od narušavanja reputacije, troškovi nastali usred kibernetičkog napada te kazne vezane za određene odredbe.

Najčešće vrste prijetnji kibernetičkoj sigurnosti su *malware* (maliciozni softver) koji predstavlja zloćudni software, zatim *phishing* (pecanje) koji se najčešće događa putem maila, *man in the middle* (čovjek u sredini) vrsta napada gdje se hakeri umetnu u komunikaciju između dviju strana te napadi na lozinke. Kako bi se osiguralo te spriječilo moguće kobne gubitke potrebno je usmjeriti pozornost na tri stupa kibernetičke sigurnosti, a to su: tehnologija, ljudi i procesi.

Pojavom COVID-19 pandemije u 2020.godini veliki broj organizacija morao je prijeći na hibridan način rada (udaljeni pristup) te se na taj način povećao broj uređaja koje treba zaštiti, a s druge strane zaposlenici koji su tada radili od kuće nisu imali adekvatnu zaštitu niti znanje za obranu od mogućih prijetnji.

Rad je podijeljen u šest poglavlja u kojima je definirano što su suvremene poslovne organizacije, što je znanje i kako je definirano, koji su suvremeni oblici pismenosti, kibernetički napadi i zaštita gdje je također povijesni pregled kibernetičkih napada i trenutna situacija te zaključno i rezultati provedenog istraživanja te diskusija istih.

1.1. Predmet i cilj rada

Problem kojim se bavi ovaj rad je sve veći broj raznih kibernetičkih napada i preniska ulaganja u edukaciju djelatnika te posljedično i nisko znanje djelatnika o kibernetičkoj sigurnosti.

Cilj ovog diplomskog rada je doprinijeti svijesti o važnosti kibernetičke sigurnosti i naglasiti ulogu zaposlenika u tom procesu zaštite te prikazati utjecaj COVID-19 pandemije na kibernetičku sigurnost poslovnih organizacija. Također cilj istraživanja je pokazati kako je poboljšanjem znanja djelatnika o kibernetičkoj sigurnosti moguće utjecati na razinu sigurnosti neke poslovne organizacije te na koji način osigurati zaštitu mailova, *endpointa* (krajnja točka) i mreže s naglaskom na hibridni način rada (rad od kuće).

Predmet istraživanja su metode i vrste kibernetičkih napada te razina znanja djelatnika o kibernetičkoj sigurnosti.

1.2. Izvori podataka i metode prikupljanja

Za potrebe izrade ovoga diplomskog rada, na temelju definiranog predmeta i cilja istraživanja, korištene su znanstvene metode u svrhu evaluacije postavljenih hipoteza. U prvom dijelu istraživanja aktivnosti su bile usmjerene na pretragu sekundarnih izvora podataka s dvostrukim ciljem: analizirati stručnu i znanstvenu literaturu u području informacijskih sustava, kibernetičke sigurnosti te znanja. Zadatak ovog dijela istraživanja je bio pripremiti podlogu za teorijski dio rada.

Podaci su prikupljeni iz raznih izvora a najznačajniji su: HRČAK – portal hrvatskih znanstvenih i stručnih časopisa, Science Journals i Oxford Journals. Korišteni su i raspoloživi materijali Sveučilišta Sjever, fundus Knjižnice grada Zagreba i kućne biblioteke, te razni Internet izvori. Uz to dio korištenih materijala su interni podaci tvrtki kao što su Trend Micro, Proofpoint, Thales, Crowdstrike, Fortinet koji su dostupni autoru ovog rada putem poslovne suradnje s navedenim tvrtkama.

Drugi dio istraživanja je anketa. U anketi je sudjelovalo 168 ispitanika od kojih se tražilo da procjene svoju razinu znanja vezano uz kibernetičku sigurnost te su im nakon toga bila

postavljena pitanja o istoj. Pitanja su se odnosila na način zaštite podataka i razumijevanje osnovnih pojmova kibernetičke sigurnosti.

1.3. Istraživačko pitanje i hipoteze rada

U odnosu na definirani predmet i cilj istraživanja postavljeno je istraživačko pitanje koje glasi: *Kakav utjecaj ima znanje na kibernetičku sigurnost poslovne organizacije*? te sljedeće hipoteze:

H1: Razina obrazovanja utječe na znanje o kibernetičkoj sigurnosti.

H2: Prelazak na udaljeni način rada uzrokovan COVID-19 pandemijom značajno je utjecao na povećani broj kibernetičkih napada.

1.4. Struktura rada

Rad je sastavljen od sedam poglavlja plus zaključak. U prvom dijelu dat je uvod u rad te su postavljena istraživačka pitanja i hipoteze.

U drugom dijelu rada koji nosi naziv suvremene poslovne organizacije definirani su pojmovi kao što je informacijski sustav te što su poslovni informacijski sustavi. Dan je pregled osnovnih komponenti informacijskog sustava: *hardware (hardver), software (softver) i liveware (ljudi).*

U trećem dijelu objašnjava se što je znanje, kako se upravlja istim te se govori o suvremenim oblicima pismenosti.

Četvrti dio daje osvrt na kibernetičke napade i zaštitu. Dan je povijesni pregled razvoja kibernetičkih napada, vrstama hakera i njihovim motivima. Opisane su najčešće vrste napada uz smjernice na koji način se zaštititi.

U petom dijelu objašnjeni su materijali i metode obrade podataka.

U šestom dijelu opisani su dobiveni rezultati kroz provedenu anketu. Prezentacija rezultata temelji se na vizualnom prikazu, podacima dobivenim analizom rezultata u programu „IBM SPSS“ te na prikupljenim podacima *desk*- metodom.

U sedmom, završnom dijelu, iznijeta je diskusija rezultata i smjernice za daljnju primjenu.

U osmom dijelu dan je zaključak.

2. Suvremene poslovne organizacije

Da bi bolje razumjeli koncept informacijske sigurnosti, potrebno je razumjeti pojam informacije koja je osnova informacijskih i komunikacijskih tehnologija. Informacija je strukturirani i korelirani podatak. Da bi se moglo koristiti određene podatke potrebno ih je pretvoriti u informacije. Podaci koji se koriste u informacijskim sustavima u obliku tekstualne poruke, mogu se prenositi do krajnjeg korisnika na strukturiran način. Koncept informacijske sigurnosti naglašava pojam sigurnosti koji uključuje osobna računala i mreže, korporativne i nacionalne mreže te pokriva informacijske sustave u širem smislu. Informacijski sustavi na korporativnoj razini uključuju i *softwere*, korisnike trećih strana i tehničke sustave podrške. Informacijska sigurnost znači garantiranje sigurnog skladištenja i procesiranja podataka bez da ih promijenimo te zaštitu od neautoriziranog pristupa u digitalnom okruženju. Kako bi se to moglo garantirati potrebno je definirati sigurnosne politike te iste i primijeniti. Politike koje će nadgledati aktivnosti nakon prikupljanja podataka, evaluaciju podataka te njihovo nadograđivanje te brisanje podataka. Općenito, informacijska sigurnost se može gledati kao dio cjelokupne sigurnosti sustava. S druge strane informacijska sigurnost u širem smislu je povezana sa kriptologijom, upravljanjem rizicima te sigurnosnom kulturom. Glavni pojmovi koji su povezani s informacijskom sigurnosti su informacijski sustavi i informacijska infrastruktura (Aytakin Nazim Ibrahimova (2020) – The definitions of infromation and security; history of information security development URL: https://www.zurnalai.vu.lt/open-series/article/view/22387/21645).

Informacijski sustav je taktički, upravljački i suportni sustav koji se primjenjuje na korisnike i informacijske tehnologije. U recipročnim interakcijama Informacijski sustav se ne može smatrati samo dijelom informacijske i komunikacijske tehnologije nego kao način na koji ljudi koriste te tehnologije za komuniciranje s tehnologijama koje podupiru njihov posao i život. Danas su informacijski sustavi bazirani na računalima, no zajedno s računalima, internetom i opremom konekcijski sustavi su vrlo važni za aktivnosti vezane uz informacijske sustave bazirane na digitalnim tehnologijama. S druge strane osim osobnih računala, jaki informacijski sustavi kao što su superračunala posjeduju mogućnost zadržavanja informacija, pristupa informacijama i pohranu (Aytakin Nazim Ibrahimova (2020) – The definitions of infromation and security; history of information security development URL: https://www.zurnalai.vu.lt/open-series/article/view/22387/21645).

Iz perspektive informacijske sigurnosti, uloga informacijske infrastrukture je krucijalna. Još uvijek ne postoji jedinstven pristup infrastrukturi u svijetu. Svaka zemlja ima svoj koncept informacijske infrastrukture unutar svojih potreba. Iako, ako sagledamo zajedničke značajke, moguće je dati pregled mreža, sustava i strukture koja može imati negativan utjecaj na održavanje kontinuiteta rada javnih servisa ili obavljanja javnih usluga u slučaju da ne izvode svoje funkcije djelomično (Aytakin Nazim Ibrahimova (2020) – The definitions of infromation and security; history of information security development URL: https://www.zurnalai.vu.lt/open-series/article/view/22387/21645).

Cilj informacijske sigurnosti je pružiti stalnu, sigurnu i kvalitetnu uslugu te implementirati aktivnosti informacijskog sustava. S druge strane održavanje pouzdanosti, zaštite podataka te sprječavanje neovlaštenog pristupa su ključni ciljevi i prioriteti svakog informacijskog sustava. Glavni problem informacijske sigurnosti je spriječiti bilo kakav napad na integritet, povjerljivost i korištenje informacijskog sustava te eliminirati sve sigurnosne slabosti koje mogu uzrokovati te prijetnje. Iako je jako teško održati sigurnost informacijskih sustava u doba sve većih kibernetičkih napada, bitno je znati koje su prijetnje i rizici informacijskih sustava. Postoje mnogi propisi i regulative koje se odnose na informacijsku sigurnost no među njima su najbitnije: računalna i mrežna sigurnost, sustavi upravljanja informacijskom sigurnošću, kriptologija, kibernetička sigurnost, kibernetički zločini, povjerljivost podataka i zaštita podataka, nacionalna sigurnost (Aytakin Nazim Ibrahimova (2020) – The definitions of infromation and security; history of information security development URL: https://www.zurnalai.vu.lt/open-series/article/view/22387/21645).

2.1. Poslovni informacijski sustavi

Poslovni informacijski sustav moguće je definirati kao grupu povezanih komponenata koje zajednički rade kako bi osigurale unos, procesiranje, izlaz, pohranu i kontrole aktivnosti koje pretvaraju podatke u informacijske proizvode koji se mogu koristiti za planiranje, predviđanje, kontrolu, koordinaciju i donošenje odluka unutar neke organizacije. U kontekstu komponenti koje se koriste za ove radnje možemo ih razvrstati u pet osnovnih resursa: ljudi, hardware, software, komunikacije i podatci. Ljudski resursi uključuju korisnike, developere i

one koji održavaju sustave kao što je tehnička podrška. Hardverski resursi uključuju računala i ostale uređaje kao što su printeri. Softverski resursi se odnose na kompjuterske programe. Komunikacijski resursi uključuju mrežu, hardver i softver potreban za podršku. Podatkovni resursi pokrivaju podatke kojima organizacija ima pristup kao što su računalne baze podataka i kriptirani podaci (Business Information System: Meaning, Features and Components (yourarticlelibrary.com) pristupio 10.6.2022)

U većini organizacija poslovni informacijski sustavi koriste informacijske tehnologije kao što su osobna računala. Razlog zbog kojeg su računalni poslovni informacijski sustavi postali popularni su njihove prednosti kao što su brzina, preciznost i neovisnost. Isti posjeduju i veliku razinu fleksibilnosti. Postoje i neki nedostaci poslovnih informacijskih sustava kao što su manjak kreativnosti ljudi te nemogućnost predviđanja određenih faktora u procesu donošenja odluka.

Informacijski sustavi se mogu podijeliti u dvije kategorije, odnosno na sustave koji podržavaju dnevne operativne radnje i sustave koji podupiru donošenje odluka na višoj razini. Operacijski informacijski sustavi se obično bave kontrolom procesa, transakcijama i komunikacijom. Upravljački informacijski sustavi se bave pružanjem podrške u donošenju menadžerskih odluka.

2.2. Tehnološki aspekt

U okviru tehnološkog aspekta suvremene poslovne organizacije sagledana je podjela hardvera i softvera te njihova primjena.

2.2.1. Hardver

Hardver opisuje fizičku komponentu računalnog sustava koja se može okarakterizirati kao ulazni uređaj, CPU, unutarnja i vanjska memorija i izlazni uređaj. Ulazni uređaji se koriste za unos podataka u računalo. Najčešće se koriste miš i tipkovnica a izbor načina unosa podataka uvelike ovisi o količini podataka koje treba unijeti. Unošenje manjeg broja podataka obično odrađuju ljudi koristeći tipkovnicu i miš. CPU odrađuje procesuiranje odrađivanjem zadataka zadanih od strane računalnih programa te ih pohranjuje u memoriju. Povećana brzina računala je primarni rezultat povećanja CPU brzine. Brzina procesuiranja podataka ovisi o nekoliko različitih faktora kao što su *clock speed (brzina ciklusa) i bus width (širina bita)*. *Clock speed*

određuje koliko uputa u sekundi može procesor izvršiti određenu radnju. *Bus width* opisuje koliko komada podataka se može prenositi odjednom. U oba slučaja što je viša vrijednost to je jači procesor. Unutarnja memorija se koristi kao privremeno sredstvo za pohranu podataka i uputa dok se vanjska memorija koristi za pohranu podataka izvan računala. Računalna memorija se koristi za pohranu podataka koji čekaju obradu, upute koje se dobiju iz softvera se koriste za obradu podataka ili kontrolu računalnih sustava. Izlazni uređaji prevode rezultate procesuiranja u čitljive podatke (https://www.techtarget.com/searchnetworking/definition/hardware pristupio 13.6.2022)

2.2.2. Softver

Softver možemo definirati kao seriju detaljnih uputa koji kontroliraju rad računalnih sustava u obliku programa koje razvijaju programeri. Dvije su glavne kategorije softvera: sustavski softver i aplikacijski softver. Sustav softver upravlja i kontrolira operacije unutar računalnih sustava na način da izvodi zadatke u ime korisnika. Sastoji se od tri osnovne kategorije: operacijskog sustava, programa za razvoj softvera i *utility* (korisno) programa. Operativni sustavi surađuju s hardverom, nadgledaju i šalju upute za upravljanje računalnim resursima. Operativni sustav funkcionira kao posrednik između funkcija koje korisnik treba izvesti (npr. pretraga baze podataka) i kako se te radnje prenose prema hardveru u obliku klika miša i prikaza na monitoru. Osnovne funkcije operativnog sustava uključuju: upravljanje resursima sustava, slaganje rasporeda korištenja resursa i praćenje aktivnosti računalnih sustava. Programi za razvoj softvera omogućuju korisnicima razvoj svojeg vlastitog softvera kako bi izvršili određene zadatke korištenjem programskih jezika. Prva generacija programskih jezika je zahtijevala da programer radi s nulama i jedinicama kako bi prikazao slova i brojke. Ovaj zadatak koji je uzimao puno vremena je pojednostavnjen kodovima i nazvan je jezik sastavljanja. Veliki napredak je došao s trećom generacijom jezika kao što su Fortan, Cobol, Basic, Pascal i C koji su smanjili vrijeme potrebno za izradu koda. Četvrta generacija jezika kao što je SQL su izgrađeni oko baze podataka što omogućava još lakše generiranje koda. *Utility* programi omogućuju niz alata koji podržavaju upravljanje računalnim sustavom. Program koji nadzire rad sustava ili pruža sigurnosne kontrole su neki od primjera *utilyti* programa (https://www.techtarget.com/searchapparchitecture/software pristupio 13.6.2022)

2.3. Organizacijski aspekt

U okviru organizacijskog aspekta suvremene poslovne organizacije sagledana je uloga čovjeka unutar poslovne organizacije.

2.3.1. Liveware

Liveware se odnosi na ljude koji koriste računala i koji imaju koristi od kompjuterskih sustava. Obično se radi o stručnjacima unutar IT područja. *Liveware* uključuje procesuiranje podataka, rješavanje problema, produktivnost, dokumentiranje podataka itd. Primjeri livewara su softverski inženjeri, hardverski inženjeri, menadžeri, mrežni inženjeri itd. Ideja liveweara je organizacija prijenosa informacija kao posljedica interpersonalne komunikacije. Dizajniran je kao komunikacijsko okružje gdje su poveznice slučajne, ne događaju se redovno te je potrebno maksimalno iskoristiti svaku priliku za razmjenu podataka. Isto se razlikuje od protokola za računalnu komunikaciju koji su predvidljivi osim u slučaju kvara. Podaci su uvijek dostupni što zahtjeva stalnu komunikacijsku infrastrukturu. *Liveware* je dizajniran oko tri ključna principa: simetrija – razmjena podataka uvijek mora biti dvosmjerna, prijelaznost – korisnici se koriste kao prijenosnici tuđih informacija i transparentnost – komunikacija mora biti transparentna i ne bi trebala zahtijevati veliki osobni trud. Prvi princip omogućuje da se maksimalno iskoristi svaka komunikacijska prilika. Kada se informacija širi na konvencionalan način ona se kopira od izvora do primatelja i nikakva komunikacija se ne odvija u suprotnom smjeru osim da je informacija isporučena. No kada su konekcije rijetke treba maksimizirati protok informacija u oba smjera. Obje strane nadopunjuju svoju bazu podataka te će svaka strana imati što ponuditi. Ovo pojednostavnjuje komunikaciju koja postaje simetrična te svaka strana radi na ažuriranju podataka kad god je to moguće. Drugi princip je isto namijenjen kako bi se poboljšao protok informacija. Kada su komunikacijske prilike rijetke jedini način da dvije strane razmijene podatke je kroz posrednike. Interpersonalna komunikacija često primjenjuje ovaj pristup.

Treći princip je namijenjen kako bi se iskoristila svaka komunikacijska prilika. Jako je bitno da korisnici nisu u kušnji da isključe komunikaciju jer im ometa njihov prioritete. Iako možda nemaju ništa trenutno za dobiti iz te razmjene podataka kvaliteta razmjene podataka je maksimizirana ako se svaka prilika iskoristi.

Informacije unutar *liveware* baze podataka se kreiraju i modificiraju na distributivan način, na različitim lokacijama u različito vrijeme. Kada dvije baze podataka susretnu asimetrično ažuriranje se napravi kako bi obje baze došle na istu razinu. Ovaj način spajanja podataka se treba izvršiti automatski kako bi se minimalizirao upad. Kako bi se osiguralo da se ovo ažuriranje odradi automatski baze podataka su podijeljene u dijelove informacija, od koje svaka ima jedinstveni identifikacijski kod, jednog korisnika koji je može izmijeniti i vremenski pečat. Pomoću ovih informacija minimalni set nadogradnji koje su potrebne kako bi dvije baze podataka dovele na istu razinu se lako mogu determinirati. Prema načinu na koji *liveware* funkcionira mora se omogućiti pristup informaciji bez obzira je li ona osobna ili nije. Točno jedna osoba mora biti odgovorna za svaki dio informacije, odnosno za njenu nadogradnju u odnosu na prijašnje verzije. Korisnici mogu raditi ažuriranje podataka/informacije bilo kada bilo gdje na bilo koju verziju dok god samo zadnja verzija ostaje aktivna (Ian H. Witten et al. ,(1991) Liveware: a new approach to sharing dana in social networks URL: https://www.academia.edu/14656697/Liveware_a_new_approach_to_sharing_data_in_social_networks)

3. Znanje

Znanje je apstraktni koncept bez ikakve reference prema opipljivom svijetu. Grčki filozofi i stručnjaci za upravljanjem znanjem su pokušali definirati znanje a rezultati su i dalje vrlo pomiješani. Prema (Neta i Pritchard, 2009) znanje je opravdavanje vlastitih uvjerenja iako je takvo razmišljanje nepouzdano i ograničeno vlastitim uvjerenjima. Takva definicija obuhvaća tri osnovna uvjeta koje neki autori nazivaju „*tripartite account of knowledge*“. Ti su uvjeti slijedeći :

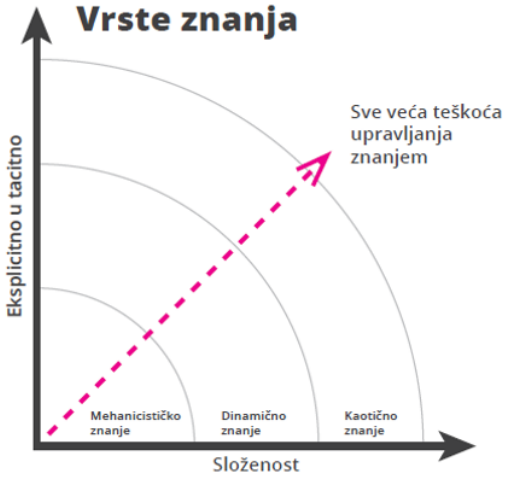
- Uvjet istine koji radi razliku između mišljenja i znanja. Ovaj uvjet definira da ako netko zna određenu tvrdnju onda ta tvrdnja mora biti istinita, ako tvrdnja nije istinita onda ta osoba ne zna ono što tvrdi da zna.
- Uvjet uvjerenja koji nalaže ako netko zna tvrdnju onda i vjeruje u tu tvrdnju.
- Uvjet opravdavanja.

Kada spojimo ove uvjete, možemo zaključiti da su uvjeti za znanje o nečemu da ono što tvrdimo znamo da je istina, da smo sigurni u to i treće da isto možemo opravdati. S druge strane osoba može potpuno vjerovati u nešto što nije istina. U literaturi se taj problem naziva „Gettier problem“.

Postoje tri vrste znanja: iskustveno znanje, vještine, tvrdnje znanja. Sve tri vrste su povezane ali imaju i neke specifičnosti. Iskustveno znanje je ono koje dobijemo u direktnom kontaktu s okruženjem kroz naš senzorni sustav (oči, uši, nos, koža…) te koje obradi mozak. Iskustveno znanje je osobno jer svaka osoba ima drugačija iskustva. Vještine znače znanje kako nešto napraviti. Bazira se na iskustvenom znanju ali je dobro strukturirano i akcijski orijentirano. To je znanje koje stječemo ponavljajući određene radnje ili zadatke te učeći kroz njih. Tvrdnje znanja je ono što znamo ili mislimo da znamo. Eksplicitno znanje je nešto što učimo u školi i čitajući knjige. Jezik je ključna komponenta koja nam omogućava da naše emocionalno i duhovno iskustvo prenesemo u eksplicitno znanje. (Ettore Bolisani, 2018. the elusive definition of knowledge URL: https://www.researchgate.net/publication/318235014_The_Elusive_Definition_of_Knowledge).

3.1. Upravljanje znanjem

Upravljanje znanjem je bitna tema u svim poslovnim organizacijama. Iako sam izraz upravljanje znanjem može sugerirati jednostavan pojam, ima puno različitih mišljenja što upravljanje znanjem ustvari jest. Radi sve većeg i ubrzanog razvoja poslovnih organizacija zadatak efektivnog upravljanja organizacijom postaje krucijalan za daljnji razvoj. Ispravno razumijevanje i implementacija upravljanja znanjem može biti koristan alat za poslovnu transformaciju kao i ključ kompetitivne prednosti. Mnogi definiraju upravljanje znanjem kao prakticiranje ili selektivno korištenje znanja stečenog prijašnjim iskustvima kroz donošenje odluka za buduće događaje i situacije kako bi poboljšali efikasnost organizacije. Isto tako upravljanje znanjem se može definirati kao sustav stvoren za pohranu, pristup i ponovno korištenje znanja. Percepcija je da upravljanje znanjem i sustavi upravljanja znanjem holistički kombiniraju organizacijska i tehnička rješenja kako bi postigli ciljeve i poboljšali donošenje odluka. (Murray E. Jennex 2007- What is Knowledge management URL: https://www.researchgate.net/publication/314500732_What_is_Knowledge_Management?



Slika 1: *Vrste znanja*

Izvor: Vlastita izrada prema (Internetske tehnologije, Nikolina Smolović URL: https://slidetodoc.com/upravljanje-znanjem-znanje-internetske-tehnologije-profesorica-nikolina-smilovi/)

Dolaskom interneta i njegov strelovit razvoj te sve veći broj ljudi koji ima pristup internetu putem raznih pristupnih točaka a posebno napredak u području razvoja softvera doveli su do

sad već dobro poznatog koncepta Web 2.0. Ova tehnologija je usmjerena prema ljudima i potrebno ju je usvojiti u procesu upravljanja znanjem.

Slika 2 : Proces upravljanja znanjem
Izvor: Žugaj, M., Schatten, M.: Informacijski sustav za upravljanje znanjem u hipertekst organizaciji, Ekonomski vjesnik: Review of Contemporary Entrepreneurship, Business, and Economic Issues, Vol. XXI No. 1-2, 2008, str. 21.

„*Upravljanje znanjem 2.0 je skup aktivnosti i procesa namijenjenih identificiranju, prikupljanju, stvaranju i dijeljenju eksplicitnog i tacitnog znanja unutar organizacije, koristeći web 2.0 alate i druge alate vezane uz nove informacijske i komunikacijske tehnologije. Upravljanje znanjem 2.0 je društvena tehnologija, odnosno tehnologija u kojoj pojedinci stvaraju znanje zajedno s drugima (pomak od individualnog prema kolektivnom) te dijele svoje znanje s drugima uz pomoć novih tehnologija. Cilj Upravljanja znanjem 2.0 poboljšati učinkovitost i efektivnost zaposlenika, ostvariti organizacijske ciljeve i unaprijediti konkurentski položaj organizacije na tržištu (*Marta Muzer at al. (2014) – Upravljanje znanjem , priručnik za poduzeća URL: https://bib.irb.hr/datoteka/740473.KM_2.0_HR.pdf)."

3.2. Suvremeni oblici pismenosti

„Informatička pismenost, ponekad nazivana i računalnom, kompjuterskom ili IKT pismenošću, određena je razinom umješnosti u uporabi i operiranju računalnim sustavima, programima i mrežama (Mijatović, 2000; Špiranec, 2003; Kralj, 2006; Catts, Lau, 2008). Riječ je, dakle, o vještinama uporabe suvremenih računalnih alata, a osnovne su joj sastavnice:

hardverska pismenost J. Vrkić Dimić: Suvremeni oblici pismenosti Šk. vjesn. 63, 3 (2014) 381-394 384 (uporaba osobnog računala, laptopa, Tipkovnice, pisača, skenera i sl.), softverska pismenost (poznavanje rada s operativnim sustavima i njihovim komponentama, npr. operativni sustav Windows) i aplikacijska pismenost (sposobnost uporabe posebnih, specijaliziranih softverskih paketa, npr. za vođenje financija), (Stričević, 2011). Suvremeni značaj informatičke pismenosti ocrtava podatak da s višom razinom računalnih znanja i sposobnosti koje je osoba razvila, raste i njezin socijalni status. Dakle, danas se često upravo s obzirom na stupanj i način uporabe računalne tehnologije određuje pojedinčev položaj u društvu (Dmitrenko, 2005). Informatička se pismenost vrlo često izjednačava s informacijskom pismenošću, iako je razlika između njih značajna (Špiranec, 2003; Kralj, 2006; Catts, Lau, 2008; Stričević, 2011). Zbog količine informacija danas dostupnih u elektroničkom obliku, da bi pojedinac bio informacijski pismen, on mora biti i informatički pismen – riječ je o međusobno uvjetovanom odnosu. Zamijenimo li mjesta dviju polaznih komponenti, dolazimo do situacije koja nije nužno međusobno uvjetovana: informatička pismenost ne pretpostavlja informacijsku pismenost. Prilikom kreiranja obrazovne politike potrebno je spomenutu razliku posebno imati na umu. Osvrćući se na navedeni odnos između informatičke i informacijske pismenosti, Catts i Lau (2008) ističu da se vještinama informacijske pismenosti nužno koristiti usporedno s vještinama rješavanja problema i komunikacijskim vještinama. One zajedno tvore integrirani set vještina koje su nužne kako bi ljudi postali učinkoviti u svim aspektima svoga života. Tu se informacijska pismenost sagledava odvojeno od informatičke pismenosti, iako među njima, kao što smo već vidjeli, u suvremenom digitalnom okruženju postoji uzajamna povezanost. Informacijska pismenost, dakle, uključuje šire teme vezane uz načine na koje se unutar suvremenih tehnoloških okvira pristupa informacijama, kao i vještine potrebne za njihovo interpretiranje te sigurnu i učinkovitu uporabu (Špiranec, 2003; Kralj, 2006; Catts, Lau, 2008). Kako su u razvijenijim društvima digitalna tehnologija i elektroničke baze podataka sveprisutne i predstavljaju jedan od primarnih izvora informacija, vještine informacijske pismenosti razvijaju se u konjunkciji s vještinama informatičke pismenosti.Dakle, danas je nužna kombinacija kognitivnih i tehničkih vještina kako bi se informacijama pristupilo i kako bi ih se adekvatno koristilo. Samo informacijski pismeni pojedinci imaju koristi od obilja informacija raspoloživih u različitim formatima (usmenom, papirnom, elektroničkom formatu). Informacija bez transformacije samo je sirov podatak (Bindé, 2007). Informacije omogućuju stvaranje znanja, ali s njime se ne mogu poistovjetiti. Kako bi informacije zaista i postale izvor znanja, i kako bi se svi s lakoćom mogli kretati u brzom protoku informacija, ključno je izgrađivanje kritičkog pristupa J. Vrkić Dimić: Suvremeni oblici pismenosti Šk. vjesn. 63, 3 (2014) 381-394

385 dostupnim informacijama. Takav bi pristup trebao omogućiti da se informacije pravilno analiziraju, razvrstavaju i ugrađuju u logički strukturirane sustave znanja. Tu je neophodno da obrazovanje odigra odlučujuću ulogu u razvijanju vještina kreativnog i kritičkog mišljenja. Upravo obrazovanje u kojem je učenik smješten u središnju poziciju, obrazovanje koje promovira i ostvaruje aktivne oblike učenja (i poučavanja) omogućuje razvijanje informatičke i informacijske pismenosti . Učenici koji posjeduju takve pismenosti ujedno posjeduju temelj i potencijal za svoj daljnji razvoj u društvu obilježenom brzim protokom i otvorenom dostupnošću informacija. Transformiranje informacija u znanje zahtijeva ovladavanje kognitivnim vještinama, uključujući kritičko mišljenje. U protivnom, „informacije neće biti ništa drugo doli nakupine nejasnih podataka" (Bindé, 2007: 19). Stroga je neopravdano pretjerano usmjeravanje na stvaranje što učinkovitijeg prijenosa i razmjene informacija, ako se pritom ne obraća dovoljna pozornost na jednake mogućnosti pristupa obrazovanju. Postoji jasna korelacija između vještina korištenja informacijsko komunikacijskih tehnologija i informacijske pismenosti , ali i opće pismenosti . OECD je kroz svoj projekt pod nazivom International Adult Literacy Survey (ILAS) identificirao navedenu korelaciju. Ustvrđeno je da oni ljudi koji imaju razvijene vještine informatičke pismenosti vjerojatno imaju i više razine opće pismenosti (OECD, 2005). Navedena korelacija može se uočiti kada se usporede zemlje s visokim i niskim stupnjem pristupa informacijsko-komunikacijskim tehnologijama, međutim m, ona je prisutna i unutar zemalja. Tako je primjerice utvrđeno da 15- godišnjaci s pristupom kućnim računalima imaju veće vještine čitanja u odnosu na svoje vršnjake bez kućnog pristupa računalima. Važno je napomenuti kako je uočeno da navedena korelacija postoji, dakle utvrđen je odnos, ali nije utvrđen i uzrok. Omogućen kućni pristup informacijsko-komunikacijskim tehnologijama otvara daljnju mogućnost pristupa mnogim pogodnosti ma suvremenih društava, uključujući obrazovanje, što je jedan od mogućih uzroka viših razina pismenosti (Catts, Lau, 2008). Možemo zaključiti da informatička i informacijska pismenost nisu sinonimi, već, u suvremenim okolnostima, međusobno uvjetovan niz vještina i kompetencija. Pritom razvijene vještine informatičke pismenosti predstavljaju temelj za izgrađivanje vještina informacijske pismenosti . Digitalna ili internetska pismenost podrazumijeva sposobnost čitanja i razumijevanja hiperteksta ili multi medijskih tekstova, što uključuje razumijevanje slika (npr. grafičkih prikaza procesa, dijagrama toka i sl.), zvukova i teksta prikazanog u obliku dinamičnog, nelinearnog hiperteksta (Špiranec, 2003). Riječ je o baratanju informacijama dostupnima putem interneta, ali se odnosi i na digitaliziranu građu dostupnu, npr. u knjižnicama, muzejima, suvremenim vodičima kroz kulturne spomenike i sl. Digitalna pismenost uključuje pouzdanu i J. Vrkić Dimić: Suvremeni oblici pismenosti Šk. vjesn. 63, 3

(2014) 381-394 386 kritičku uporabu informacijsko-komunikacijske tehnologije na poslu, u slobodnom vremenu i u komunikaciji (Demunter, 2006). Ona objedinjuje i sposobnosti uporabe novih informacijsko-komunikacijskih alata, ali i vještine medijske pismenosti radi mogućnosti snalaženja sa slikovnim, tekstualnim i audiovizualnim sadržajima koji se stalno pojavljuju diljem globalnih računalnih i komunikacijskih mreža (ISPL, 2006). Konkretne vještine obuhvaćene sintagmom digitalne pismenosti uključuju sposobnost prosuđivanja o on-line izvorima, pretraživanje interneta, upravljanje multi medijalnom građom, komuniciranje putem mreže (Špiranec, 2003) te kreiranje i razmjenu informacija, kao i participaciju u virtualnim zajednicama (Demunter, 2006). Iako se koncept digitalne pismenosti donekle preklapa s konceptom informacijske pismenosti, informacijska je pismenost daleko širi koncept koji, pored informacija u elektroničkom obliku, obuhvaća sve informacije dostupne u različitim oblicima (J.Vrkić Dimić, 2014.)."

4. Kibernetički napadi i zaštita

U svijetu kibernetičke sigurnosti postoje razne vrste napada kojima je cilj iskoristiti slabosti određenog sustava kako bi nanijeli štetu nekoj tvrtki ili pojedincu. Kako se razvijaju nove tehnologije te je sve više uređaja spojeno na Internet tako i količina prijetnji raste iz dana u dan. S obzirom na to da uređaji dolaze, mijenjaju se i odlaze iz mreže, potrebno je mrežu promatrati kao područje koje se konstantno mijenja. Potrebni su posebni alati koji će omogućiti bolju kontrolu prometa i vidljivost prijetnji. (Mark S. Kadrich 2007.- Endpoint security (16))

4.1. Povijesni pregled

Gotovo dva desetljeća nakon kreiranja prvog digitalnog računala 1943. godine, izvođenje kibernetičkih napada je bilo izazovno. Pristup velikim elektroničkim strojevima je bio ograničen malom broju ljudi i oni nisu bili umreženi, samo je nekolicina ljudi znalo raditi s tim računalima tako da prijetnje nisu ni postojale. S druge strane teorija o računalnim virusima je objavljena 1949. godine kada je računalni pionir John von Neumann pretpostavio da se računalni programi mogu razmnožiti. U kasnim 1950-ima pojavilo se prisluškivanje telefona. Ovaj pristup se bazirao na otimanju protokola koji su omogućili telekom inženjerima da rade na mreži udaljeno kako bi obavljali besplatne pozive i izbjegli naplatu. Počinitelji su postali zajednica koja izdaje novine te su uključivali i tehnološke istraživače kao što je Steve Wozniak i Steve Jobs. U šezdesetima se pojavljuje prva referenca malicioznog hakiranja u Massachusett institute of technology novinama. Do sredine šezdesetih većina računala su bili ogromni strojevi zaključani u sobama s reguliranom temperaturom. Ti su strojevi bili vrlo skupi tako da je pristup programerima ostao ograničen. Postojali su neki pokušaji hakiranja od strane onih s pristupom (često studenata). U ovom stadiju napadi nisu imali nikakve komercijalne i geopolitičke benefite. Većina hakera je samo bila znatiželjna te je pokušavala unaprijediti sustav da radi brže i efikasnije. Godine 1967 IBM je pozvao studente da isprobaju njihovo novo računalo. Nakon istraživanja dijelova koji su bili pristupačni studenti su istraživali dublje učeći sustavski jezik i dobivali su pristup drugim dijelovima sustava. To je bila vrijedna lekcija kompaniji te su izrazili zahvalnost studentima koji su uspjeli uništiti sustav što je rezultiralo izgradnjom defenzivnih mjera i defenzivnom načinu razmišljanja koji će se kasnije pokazati kao neophodan. Kako su

se računala počela proizvoditi sve manja i postojala sve jeftinija, veliki broj kompanija je ulagao u tehnologije koje su pohranjivale podatke. Pohranjeni podaci su bili zaštićeni lozinkom.

Pojam kibernetičke sigurnosti se počeo razvijati 1972. godine kao projekt ARPANET (*the advanced research projects agency network)* koji je bio preteča internetu. Istraživač Bob Thomas kreirao je kompjuterski program pod nazivom Creeper koji se mogao kretati kroz ARPANET mrežu i ostavljajući trag gdje je bio. Pisalo je „ja sam kreeper ulovi me ako možeš". Ray Tomlinson, izumitelj e-maila napisao je program Reaper koji je pronalazio i brisao Creeper. Reaper nije bio samo prvi pravi antivrus software nego je bio i prvi program koji se samo replicirao čime je postao prvi računalni crv. Rješavanje izazova i prijetnji u novim tehnologijama je postalo jako bitno sa sve većim brojem kompanija koje su koristile telefon kako bi kreirale udaljene mreže. Svaki povezani hardver je predstavljao novu ulaznu točku koju treba zaštititi. Kako su se računala počela koristiti sve više i umrežavanje je raslo postalo je jasno vladama da je sigurnost vrlo bitna i da bi neautorizirani pristup podacima mogao imati katastrofalne posljedice. Kreiranje prvih zaštita računala je bilo u suradnji ESD i ARPA sa U.S. Air Fore i ostalim organizacijama koje su radile zajedno kako bi izgradile sigurnosnu jezgru za kompjuterski sustav (HIS level 68). ARPa-in projekt vezan uz analizu zaštite je istraživao sigurnost operativnih sustava, identificiranjem automatizirane tehnike detektiranja prijetnji unutar softwarea. Do sredine 1970-te koncept kibernetičke sigurnosti se razvio i postao glavna tema. Godine 1979-te 16-godišnji Kevin Mitnick je hakirao ARK – računalo koje se nalazilo u korporaciji digitalne opreme koje se koristilo za izgradnju operativnih sustava te je napravio kopiju softvera.

Godina1980. donijela je povećanje u broju napada visoke važnosti uključujući one na CSS, AT&T i Los Almos nacionalnu knjižnicu. Godine 1983. se prvi put počinju koristiti izrazi trojanski konj i kompjuterski virus. Za vrijeme hladnog rata razvila se kibernetička špijunaža. Godine 1985. US departmant of defense je objavilo kriterije za sigurnost računalnih sustava koja je davala informacije kako procijeniti razinu povjerenja koju se može imati u softver te koje sigurnosne mjere su potrebne. Unatoč tome 1986. godine njemački Hacker Mrcus Hess je iskoristio *gateway* (mrežni usmjerivač) kako bi se spojio na ARPANET te je hakirao 400 vojnih računala kako bi prodao informacije KGB-u. Korisnici su shvatili vrlo brzo da povećanje u veličini datoteka može značiti pokušaj hakiranja pa je tako smanjenje memorije operativnog sustava do danas ostao znak pokušaja hakiranja.

Godine 1987. je početak komercijalnog antivirusa i to NOD, McAfee antivirusnih rješenja. Do 1988. godine veliki broj kompanija u svijetu je bilo etablirano po pitanju kibernetičke sigurnosti, kao što je Avast.

Kompanijama je postalo jasno da mogu reagirati samo na postojeće napade a sami *update* (nadogradnja) je bilo teško „deplojati" odnosno pustiti u rad.

Godine 1990. je kreiran prvi polimorfni virus (kod koji mutira dok originalni algoritam čuva neizmijenjen kako bi izbjegao detekciju). Prvi antivirusi su se bazirali na digitalnom potpisu koji je uspoređivao zapise s bazom potpisa virusa. To je značilo da su se često događala „*false positives*" ili lažna upozorenja. Koristilo se puno računalne energije što je frustriralo korisnike. Godine 1992. se pojavio prvi anti-antivirus program. Do 1996. godine veliki broj virusa je koristio nove tehnologije i inovativne metode, uključujući prikrivanje, polimorfnost i makro viruse koji su stavljali nove izazove za antivirusne kompanije. 90- ih je broj *malwarea* i virusa eksplodirao s 10-ak tisuća na preko 5 miliona. Svake godine do 2007. pojavilo se heurističko detektiranje kao nova metoda koja se može nositi sa velikim brojem varijanti virusa. Počeli su se koristiti generički potpisi kako bi se detektirali virusi iako bi prijetnja bila skrivena unutar beznačajnog koda. Krajem 1990. godine e-mail je otvorio put novim virusima. Godine 1999. Melisa virus je pušten. Ulazio je na korisnikovo računalo putem word dokumenta i tada je slao e-mailom kopije na prvih 50 email adresa u Microsoft Outlooku. Do danas ostaje jedan od najbrže šireći virusa a šteta je bila oko 80 milijuna dolara.

S pojavom interneta u sve više domova i ureda kibernetički kriminalci su imali sve više uređaja i softvera koje su mogli iskoristiti za svoje napade a s obzirom na sve veći broj podataka imali su sve više i više za ukrasti. Godine 2001. se pojavila nova vrsta prijetnji gdje korisnici nisu morali skinuti datoteku nego je bilo dovoljno posjetiti zaraženu web stranicu. Razvoj napada nultog dana koji su koristili rupe u sigurnosnim mjerama za nove aplikacije i softver je učinilo Antivirus beskorisnim. Ključni izazov je bio u tome što antivirusni program usporava računalo. Rješenje je bilo da se softver prebaci u „cloud" ili oblak.

Godine 2007. panda *security* (sigurnost) je kombinirala cloud tehnologiju s *threat inteligence* (istraživanje prijetnji) u svom antivirusnom proizvodu. Još jedna inovacija je bila OS-sigurnost – kibernetička sigurnost koja je bila ugrađena u operativni sustav te je omogućila dodatni nivo zaštite. Godine 2010. se povećao broj velikih napada koji su utjecali na nacionalnu sigurnost

zemalja te koje su napravile štete u milijunima dolara. Godine 2017. WannaCry ransomeware je inficirao 230,000 računala u jednom danu.

Digitalizacija koja traje omogućava kibernetičkim kriminalcima nove prilike za iskorištavanje i napade. Kibernetička sigurnost koja je prilagođena određenoj vrsti posla je postala sve traženija. Godine 2011. Avast je lansirao prvi proizvod za poslovne organizacije. Kako su se razvijali antivirusni programi tako su i kibernetički kriminalci razvijali nove metode napada kao što su multi-vector napadi i socijalni inženjering. Kibernetička sigurnost nove generacije koristi drugačije pristupe kako bi povećali detekciju novih prijetnji, a paralelno smanjuje broj „*false-positive*“ napada. Koristi metode kao šti su multi više faktorska autentifikacija, analiza ponašanja mreže, zaštita u stvarnom vremenu, pješčanik i druge (https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/ pristupio 13.6.2022)

4.2. Trenutno stanje

S razvojem računalnih tehnologija i sve većih brzina interneta povećala se površina napada (više računala i aplikacija povezanih na mreži). Dobro je poznato da su informacije imovina koja ima vrijednost a tu činjenicu najviše iskorištavaju hakeri. Kibernetička sigurnost zato danas postaje sve važnije područje dok očuvanje podataka postaje sve veći izazov za kompanije.

4.2.1. Vrste hakera i njihovi motivi

„Hakeri početnici“ se odnosi na pojam koji opisuje hakere koji nisu baš vješti i oslanjaju se na alate dostupne online i koje su im omogućili drugi hakeri. Alternativna imena za ovu vrstu hakera su *Script kiddies, New bies i System challenger*. Definira ih njihova znatiželja, zloglasnost i rekreacija. Studenti nemaju maliciozne namjere, ali isto rade kako bi stekli znanje i motivira ih znatiželja. *Cyberpunks* su niže do srednje rangirani hakeri koji hakiraju radi zabave. Alternativna imena za ovu vrstu hakera su *Crashers, Thugs i Crackers*. Motivira ih financijska dobit, zloglasnost osveta i rekreacija. Old gard ili Stara garda kao studenti su ne-

malicizoni hakeri koji nemaju osjećaj za privatnost te se tu ubrajaju *White hates, Sneakers, Grey hats i Tourists.* Motivira ih znatiželja, zloglasnost, rekreacija i ideologija. *Insideri* su nezadovoljni trenutni ili bivši zaposlenici koji zloupotrebljavaju prava pristupa kako bi dobili što žele. Tu se ubrajaju *Internals, User, Malcotents i Corporate raiders*. Motivirani su financijskom dobiti, osvetom i ideologijom. *Petty thiefs* se odnosi na kriminalce koji su se prebacili iz stvarnosti u online i motivirani su financijskom dobiti i osvetom. Tu se ubrajaju *Extortionsts, Scammers, Fraudsters, Thives i Digital robbers. Digital pirates* znani kao i *copyright infrigners* posjeduju i upuštaju se u ilegalno dupliciranje, distribuciju, skidanje ili prodaju zaštićenog materijala a motivira ih financijska dobit. *Crime facilitators i suporteri* pružaju potrebne alate i tehnički *know-how* kibernetičkim kriminalcima i na taj im način omogućuju da lansiraju sofisticirane napade koji inače ne bi bili mogući. Mogu imati specifične vještine ili ekspertizu i obično su financijski motivirani. Profesionalci su individualci s velikim vještinama koje ljudi unajmljuju za ciljane napade ili rade za samostalno napredovanje bogatstva. Motivira ih financijska dobit i osveta a poznati su i pod imenom *Black hats, Elites, Organized criminals, Information brokers i Thieves. Nation state* hakeri su vrlo istrenirani i izuzetno vješti te rade direktno ili indirektno za neku vladu kako bi destabilizirali, distruptirali ili uništili mrežu neke vlade. Motivirani su financijskom dobiti, osvetom ili ideologijom. Ova kategorija uključuje i *Information warriors, Cyber terrorists, Cyber warriors, State actors i Spies. Crowdsources* su individualisti koji se udružuju kako bi riješili problem, često koristeći upitne metode. Motivira ih zloglasnost, osveta, rekreacija i ideologija. Hacktivisti znani i kao politički aktivisti i idelolozi koriste svoje vještine kako bi pomogli svojim političkim preferencijama ili koriste Internet kao alat za političke promjene. Motivira ih zloglasnost, osveta, rekreacija i ideologija (Samuel Chng, at al., 2022.)

Hacker Types	Motivations						
	Curiosity	Financial	Notoriety	Revenge	Recreation	Ideology	Sexual Impulses
Novices	✓	–	✓	–	✓	–	–
Cyberpunks	–	✓	✓	✓	✓	–	–
Insiders	–	✓	–	✓	–	✓	–
Old Guards	✓	–	✓	–	✓	✓	–
Professionals	–	✓	–	✓	–	–	–
Hacktivists	–	–	✓	✓	✓	✓	–
Nation States	–	✓	–	✓	–	✓	–
Students	✓	–	–	–	–	–	–
Petty Thieves	–	✓	–	✓	–	–	–
Digital Pirates	–	✓	–	–	–	–	–
Online Sex Offenders	–	–	–	–	–	–	✓
Crowdsourcers	–	–	✓	✓	✓	✓	–
Crime Facilitators	–	✓	–	–	–	–	–

Slika 3 : Vrste Hakera i njihovi motivi

Izvor: Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau ;Computer in Human Behavior reports, Hacker types, motivations and strategies : A comprehensive framework(2022)

4.2.2. Vrste zlonamjernih softvera

SQL injection attack (napad SQL inekciom) je postao čest problem za web stranice na osnovi baze podataka. Napadi se događaju kada se pokrene SQL upit od strane kibernetičkih kriminalaca te se upit pošalje na bazu podataka. Isti se isporučuje od klijenta do poslužitelja putem ulaznih podataka.

SQL naredba se često ubacuje kao input umjesto lozinke ili login podataka. To omogućava kriminalcima da pokreću svoje predefinirane SQL komande. Kada je SQL napad uspješan, osjetljive i povjerljive informacije se mogu pročitati, ukrasti, modificirati , ubaciti ili izbrisati. Isto tako kriminalci mogu izvršiti određene naredbe kao što je gašenje baze podataka, vraćanje podataka pa čak i izdavanje naredba operativnom sustavu.

Phishing napad omogućava kriminalcima da šalju mailove koji izgledaju kao da dolaze iz povjerljivih izvora. Cilj ovakvih napada je prikupljanje povjerljivih podataka pojedinca ili kako bi utjecali na pojedinca da učine nešto štetno. Mail može sadržavati privitak koji kada se preuzme instalira *malware* na uređaj. S druge strane mail može biti link na lažnu web stranicu kako bi uvjerili nekoga da preda svoje povjerljive informacije ili da na prevaru preuzmu neki maliciozni software. *Spear phishing (ciljano pecanje)* je bolje usmjereni *phishing* napad te ova vrsta napada zahtjeva od napadača da obavi dobro istraživanje mete koju napada. U ovakvoj vrsti maila polje „from“ unutar maila može izgledati kao da je od poznate osobe ili osobe unutar kompanije koja zahtjeva uplatu novca. Još jedan od način *spear phishinga* je kloniranje web stranice i na taj način prevarom navesti metu da unese svoje login podatke ili osobne informacije.

Malware, ili “maliciozni software,” je neželjeni software instaliran na sustav ili uređaj bez našeg znanja ili dopuštenja. Malware često infiltrira sustav tako što se pripoji stvarnom kodu. Može se sakriti unutar aplikacija ili se duplicirati pomoću interneta. Postoje više vrsta *malwarea* i svake ih je godine sve više, ali najpoznatiji su :

- *System or Boot-Record Infectors*
- *Macro Viruses*
- *File Infectors*
- *Trojans*
- *Stealth Viruses*

- *Logic Bombs*
- *Ransomware*
- *Adware*
- *Spyware*

Botnet se sastoji od osobnih računala i uređaja koji surađuju kako bi ostvarili neki zadatak. Zovemo ih *Botnet* zato što ti programi inače znani kao *botovi* ili roboti postoje na mreži uređaja. Jedan *bot* ne može napraviti puno štete no skupno su opasni i moćni. *Botnetovi* se koriste od strane kriminalaca kako bi izvršili razne kibernetičke! napade. Mogu omogućiti „*denial of service* „napad koji preplavljuje web stranicu s prometom velike količine kako bi ju srušio. Takvi napadi mogu koštati kompaniju milijune dolara u gubitcima, globama i klijentima. *Botnetovi* se koriste i za krađu lozinki i povjerljivih informacija, širenje spama i distribuiranje virusa. Popularno su oružje kibernetičkih kriminalaca jer su jeftini i efektivni. *Bot* napad se može koristiti kako bi izbjegli sigurnosne mjere *firewala* (vatrozid) i potencijalno može zaraziti tisuće uređaja pretvarajući ih u *botove*. Ti *botovi* će ostati povučeni dok ne uspostave komunikaciju sa *comand and control serverom* (server za upravljanje), nakon čega se mogu lansirati razni napadi.

Cross-site scripting (više strane skripte) napadi, znani i kao XSS napadi koriste web resurse trećih strana kako bi izveli skripte u programu ili web pregledniku neke osobe. XSS napadi uključuju da napadač ubacuje podatke zaražene zlonamjernim JavaScriptom u bazu podataka web stranice. Ako žrtva pokuša posjetiti stranicu na ovoj web stranici, stranica se prenosi s korisnim opterećenjem kao dijelom HTML tijela. To se zatim prenosi u preglednik željene žrtve, koji aktivira skriptu. Skripta može poslati korisnikove kolačiće na server napadača što će omogućiti napadaču da ih izveze i koristi za pokušaj otimanja sesije. XSS može imati i puno ozbiljnije posljedice ako bi se koristio za iskorištavanje drugih slabosti, koje bi omogućile napadaču da napravi sliku zaslona te zabilježi aktivnost tipkovnice, ukrade mrežne podatke pa čak i upravlja sa žrtvinim uređajem iz daljine. XSS se može koristiti za pokretanje napada iz *ActiveX, Flash, VBScript, i JavaScript* programa.

A denial-of-service (odbijanje usluge) (DoS) napad se koristi od strane hakera kako bi preopteretili sustavske resurse a što uzrokuje da sustav ne može obraditi zahtjev.

Distributed denial-of-service (distribuirano odbijanje usluge) (DDoS) napad cilja sustavske resurse, ali izvor napada dolazi od velikog broja uređaja od kojih je svaki zaražen i pod kontrolom cyber kriminalca.

DOS napad radi zajedno sa *bot-netsima* i omogućuje potpuno onemogućavanje web stranice i njihovih usluga. Isto rade na način da opterete metu sa stotinama ili tisućama zahtjeva raznih uređaja u botnet-u. U odnosu na druge napade koji su usmjereni na dobivanje pristupa napadača od DOS napada sam napadač nema dobiti osim ako je meta napada konkurentna kompanija. Još jedan razlog zašto bi napadač mogao koristiti DoS ili DDoS napade je da učini sustav ranjivim na druge napade. Rušenjem sustava s mreže kibernetički kriminalac može koristi otimanje sesija kako bi postigao svoj cilj (https://www.dnsstuff.com/common-types-of-cyber-attacks pristupio 13.6.2022)

Postoji nekoliko vrsta DDoS napada :

- *TCP SYN Flood Attacks:*
- *Smurf Attacks:*
- *Ping of Death Attacks:*
- *Teardrop Attacks*

4.3. Načini zaštite

Pristup zaštiti mora biti proaktivan i to na način da se ukloni iz mreže sve što nije potrebno, da se onesposobi sve što se ne koristi te da se ograniči pristup ključnim podacima (Donald I. pipkin 1992. – Halting the hacker (269))

„*Pristupni uređaji koji služe za ostvarivanje pristupa internetu važan su dio sigurnosti te prečesto nedovoljno dobro prilagođeni služe zlonamjernim napadačima u kriminalnim aktivnostima korisnici interneta nedovoljno shvaćaju ozbiljnost uređaja u svojim domovima, posebice pritom misleći na mrežne usmjerivače (eng. Router) kao jedne od najbitnijih uređaja u svojem domu.“*

„Mrežni usmjerivači omogućavaju korisnicima spajanje na internet, fiksno ili bežično (eng. Wireless) ovisno o izvedbi samog uređaja, stoga je potrebno posvetiti potrebnu pažnju prilikom rukovanja odnosno korištenja takvog uređaja. S ciljem prevencije i sprječavanja zlonamjernih radnji s računalnih mreža potrebno je postaviti si nekoliko pitanja na koja je potrebno imati pozitivan odgovor.“

- *Je li mrežnom preklopniku (eng. Router) onemogućen fizički pristup znatiželjnim posjetiteljima?*
- *Pristup mrežnom preklopniku omogućen je isključivo dopuštenim uređajima te se konfiguracijskom sučelju preklopnika može pristupiti isključivo putem korisničkog imena i snažne lozinke (promjene su tvorničke postavke)?*
- *Mrežnom preklopniku podešeno je automatsko ažuriranje novim inačicama?*
- *Bežični mrežni preklopnik (eng. Wireless router) koristi aktualne metode enkripcije kao što je algoritam WPA 2? Navedeni algoritam odnosi se na poboljšanu i sigurniju inačicu WPA algoritma za sigurniju komunikaciju putem bežičnih mreža.*
- *Bežičnom mrežnom preklopniku onemogućen je fizički pristup znatiželjnim posjetiteljima?*
- *Pristup bežičnom mrežnom preklopniku omogućen je isključivo dopuštenim uređajima te se konfiguracijskom sučelju može pristupiti isključivo putem korisničkog imena i snažne lozinke (promjene su tvorničke postavke)?*
- *Bežičnom mrežnom preklopniku podešeno je automatsko ažuriranje novim inačicama?*
- *Bežičnom mrežnom preklopniku onemogućen je pristup putem WPS mogućnosti? WPS označava olakšani način pristupanja bežičnoj mreži.*
- *Gostima i posjetiteljima kreirana je posebna bežična mreža za pristup internetu?*
- *Onemogućena je vidljivost bežične mreže odnosno isključeno je oglašavanje SSID-a (ime odnosno vidljivi naziv bežične lokalne mreže)?*
- *Mrežnim uređajima podesili ste fiksne IP adrese? IP adresa je jedinstvena brojčana oznaka računala na internetu.*
- *Onemogućili ste DHCP funkcionalnost mrežnom uređaju kako biste onemogućili spajanje nepoznatih uređaja? DHCP je mrežni protokol korišten od strane mrežnih računala za dodjeljivanje IP adresa i ostalih mrežnih postavki.*
- *Omogućili ste pristup mrežnom preklopniku isključivo dozvoljenim uređajima odnosno njihovim MAC adresama (eng. Media Access Control Address je adresa upisana u ROM (eng. Read Only Memory) svakog mrežnog uređaja)?"*

„*Računala su najčešći izvori zaraze, stoga treba obratiti posebnu pažnju prilikom planiranja i implementacije zaštitnih mjera. Računala su sredstva za rad diljem svijeta te su kao takva u virtualnom svijetu najizloženija nizu prijetnji i raznim vektorima napada, zlonamjernih napadača. Uspješno izvršenim napadima, napadači često ostvaruju uvid i pristup cjelokupnoj*

mreži, odnosno i svim ostalim uređajima koji nisu odgovarajuće zaštićeni kao što su računala, poslužitelji i mrežni uređaji.“

„Nedovoljno zaštićena računala omogućavaju napadačima, uz već navedeno, također pristup povjerljivim informacijama kao što su: omiljene stranice, tekući računi, kreditne kartice, elektronička pošta te ostali podaci na računalu. S ciljem prevencije i sprječavanja zlonamjernih radnji na računalu, postavite si nekoliko pitanja na koja je potrebno imati pozitivan odgovor.“

- *Ažurirate li operativni sustav sigurnosnim zakrpama?*
- *Upotrebljavate li antivirusnu zaštiti koja se redovito ažurira?*
- *Aplikativna rješenja na računalu redovito ažurirate najnovijim inačicama?*
- *Koristite aplikativna rješenja za izradu sigurnosne pohrane podataka ili istu redovito izrađujete samostalno na eksternom mediju, udaljenom mrežnom mjestu ili u oblaku?*
- *Ne otvarate sumnjive poveznice i neprovjerene stranice?*
- *Elektroničku poštu i privitke otvarate isključivo od provjerenih pošiljatelja?*
- *Poruke elektroničke pošte brišete ili telefonski provjeravate s pošiljateljem ako vam se nešto čini nesuvislim ili sumnjivim?*
- *Poruke elektroničke pošte brišete ili telefonski provjeravate s pošiljateljem ako iste sadržavaju zahtjeve ili usluge koje niste zatražili?*
- *Poruke elektroničke pošte brišete ili telefonski provjeravate s pošiljateljem ako u istima postoje poveznice na sumnjiva mrežna mjesta?*
- *Koristite na računalu ugrađeni ili dodatni vatrozid?*
- *Ako je vaše računalo zaraženo zlonamjernim sadržajem, isti samostalno ili uz stručnu pomoć brišete s računala?*
- *U slučaju da zlonamjerni sadržaj nije moguće očistiti, tada ponovno vraćate računalo na tvorničke postavke ili reinstaliram operativni sustav samostalno ili uz stručnu pomoć?“*

E-mail je možda i najpopularniji sustav za razmjenu poslovnih informacija putem interneta (ili bilo koje druge računalne mreže). Na bazičnom nivou email procesi se mogu podijeliti na dvije komponente: mail servere koji služe za dostavu, prosljeđivanje i pohranu mailova i mail klijenti

koji omogućuju korisnicima da čitaju, slažu, šalju i pohranjuju mailove. Mail serveri i mail klijenti su često ciljani od strane napadača. Zbog toga što su mrežne tehnologije koje su vezane za email jednostavne za razumijevanje, napadači mogu kreirati metode napada koje će iskoristiti sigurnosne slabosti. Mail serveri su isto tako ciljani jer moraju komunicirati s nepouzdanim trećim stranama. Dodatno mail klijenti su ciljani radi ubacivanja *malwarea* u strojeve i širenja koda na druge uređaje. Zbog svega toga mail serveri, mail klijenti i mrežna infrastruktura mora biti zaštićena (https://rdd.gov.hr/izdvojeno/kiberneticka-sigurnost-1436/zastita-racunalnih-mreza/1441 pristupio 21.6.2022).

4.4. Komercijalna rješenja za zaštitu od kibernetičkih napada

Kako bi se za neku organizaciju moglo reći da je zaštićena protiv kibernetičkih napada (iako 100% zaštita ne postoji) mora sadržavati zaštitu za sva tri glavna stupa infrastrukture, a to su mrežna zaštita, *endpoint* (krajnja točka) zaštita te zaštita mailova. Danas je na tržištu veliki broj ponuđača koji se bave kibernetičkom zaštitom od koji je Trend Micro vodeći prema Gartnerovom nezavisnom istraživanju o XDR zaštiti.

Trend Micro u svom portfoliu ima kompletna rješenja za sva tri infrastrukturna polja od kojih je *Apex one* za zaštitu *endpointa* jedno od najbolje rangiranih rješenja. *Apex one* nudi napredno i automatizirano detektiranje prijetnji u što je uključen i *ransomware (otkupnina)*. Dakle, isti nudi kompletno rješenje; zaštitu od *malwarea i ransomwarea,* brani *endpointe* od *malwarea i ransomwarea* te malicioznih skripti. Napredne mogućnosti zaštite omogućuju zaštitu od još nepoznatih prijetnji.

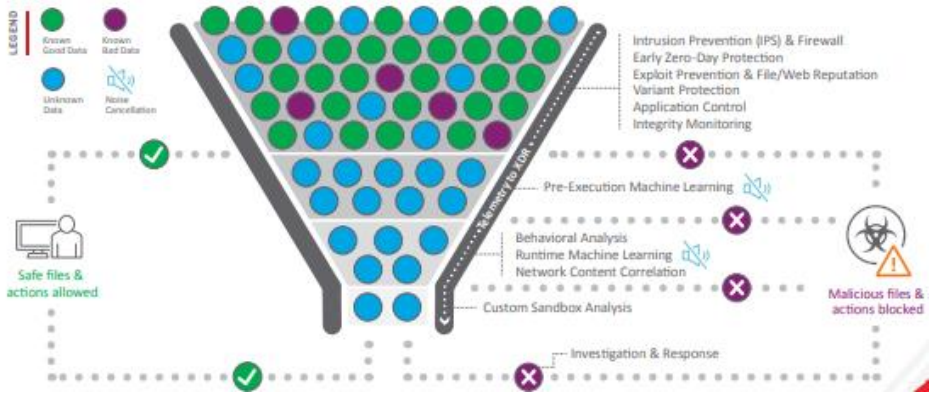
Napredne mogućnosti detekcije i otklanjanja *malwarea* u jednoj konzoli – XDR omogućava detekciju kroz sve nivoe sustava te istragu kroz pregled mailova, *endpointa*, servera, aplikacija u cloudu i mreže.

Omogućuje virtualnu zakrpu ili „*patching*“ – zaštita od prijetnji omogućuje virtualnu zakrpu kako bi zaštitili sustav i prije nego je zakrpa omogućena regularnim putem.

Ransomeware rollback – detektira *ransomware* pomoću strojnog učenja i seta pravila kako bi blokirao enkripciju podataka u milisekundama. Rollback vraća sve podatke koji su kriptirani prije same detekcije.

Povezne detekcije prijetnji- Trend Micro Apex one se može integrirati s ostalim sigurnosnim proizvodima i rješenjima putem clouda, koji omogućava tzv. *sandboxing.*

Trend Micro as a Service omogućuje fleksibilnu adaptaciju te štedi vrijeme i novac i uvijek je ažurirano sa zadnjom verzijom zaštite.



Slika 4. Trend Micro Endpoint protection proces

Izvor: https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html (pristupio 4.7.2022)

Trend Micro *Tipping point -threat protection system (sistem za zaštitu od prijetnji)* je jaka platforma za zaštitu mreže koja nudi zaštitu od poznatih i neobjavljenih ranjivosti sustava. Pruža pokrivenost protiv svih vektora prijetnji kao što su *malware i phising* napadi. *Tipping point* koristi kombinaciju tehnologija uključujući i *deep pocket* inspekciju, reputaciju prijetnji, reputaciju URL-ova i naprednu analizu *malwarea* kako bi spriječio napade na mreži .

Neki od glavnih značajki ovog rješenja su :

Tipping point extended to the Cloud – Trend Micro TP je moćno online rješenje koje omogućava pregled i hibridnog okruženja.

SSL inspekcija – noviji napadi koriste enkripciju kako bi izbjegli detekciju, *tipping point* taj problem rješava tako da smanjuje slijepe točke kreiranjem kriptiranog prometa.

Skalabilnost performansi – povećanje konsolidacije podatkovnih centara cloud okruženja zahtjeva sigurnosna rješenja koja se mogu prilagođavati povećanju obujma prometa.

Fleksibilan licenčni model – uz *pay as you grow (plaćanje uz rast)* pristup i fleksibilne licence koje se mogu preraspodijeliti preko cijelog *Tipping point* bez promjene infrastrukture.

Strojno učenje u stvarnom vremenu – *Tipping point* koristi statističke modele koji su razvijeni pomoću strojnog učenja kako bi detektirao i uklonio prijetnje u stvarnom vremenu.

Uklanjanje prijetnji – brzo uklanja prijetnje integrirajući procjenu prijetnji s portfolijom *tipping pointa* proizvoda. Korisnici mogu povući informacije s raznih ponuđača usluga koji se bave odgovorima na prijetnje.

Napredna analiza prijetnji – protekcija od nepoznatih prijetnji kroz Trend Micro-v proizvod *Deep Discovery Analyzer (analizator za dubinsku provjeru),* poznate prijetnje i potencijalne prijetnje koje se šalju u *sandbox.*

Visoka dostupnost – idealno za online implementaciju. *Tipping point* ima više sigurnosnih sustava.

E-mail je glavna točka upada većine kibernetičkih napada od kojih su *ransomeware i business email compromise* vodeći načini napada. *Trend Micro E-mail security* zaustavlja gotovo sve *phishing, ransomeware* i BEC napade. Koristi se strojnim učenjem, analizom *sandboxa,* DLP-om i drugim metodama kako bi spriječio većinu prijetnji. Ovo rješenje smanjuje radne sate SOC-a i integrira se sa drugim rješenjima Trend Micro kako bi razmjenjivali podatke o prijetnjama te pružili centralnu vidljivost nad svim nivoima.

Glavne značajke ovog rješenja su sljedeće:

Zaštita po slojevima – pruža zaštitu od *phishinga, spam-a* pomoću raznih tehnika koje uključuju analizu pošiljatelja, privitaka i slika te strojno učenje.

Zaštita od email prijevara – štiti od BEC napada pomoću naprednog strojnog učenja koji analiza i pošiljatelja i sadržaj emaila. Uključuje i Trend Micro provjeru stila pisanja kao dodatnu zaštitu.

Detekcija zloćudnih dokumenata – detektira napredne *malware* i zaražene PDF datoteke, te ostale dokumente kao što su Excel, Word.

Napredna zaštita od prijetnji – otkriva nepoznate *malware* koristeći razne tehnike provjere uzoraka koji sadrže strojno učenje prije pokretanja programa, *sandbox* tehnologiju i druge.

Izvlačenje dokumenata koji su zaštićeni lozinkom – izvlači i otvara datoteke zaštićene lozinkom koristeći kombinaciju pred definiranih lozinki.

URL vrijeme klika- blokira mailove sa sumnjivim URL-ovima prije isporuke i radi dodatnu provjeru URL-a kada se na njega izvrši klik.

5. Materijali i metode

U cilju istraživanja povezanosti razine znanja i kibernetičke sigurnosti poslovne organizacije provedena je anketa od 20 pitanja. Ujedno je provedeno i istraživanje dostupnih on line materijala po pitanju utjecaja COVID-19 pandemije na hibridni način rada te broj kibernetičkih napada u istom periodu. Anketni upitnik kreiran je putem „Google obrasca“ te je poslan elektroničkom poštom a i objavljen je na društvenim mrežama autora ovog rada (Facebook, Instagram, WhatsApp).

5.1. Istraživački materijali

U ovom radu korišteni su sekundarni i primarni izvori podataka. Od sekundarnih izvora podataka korišteni su podaci iz knjiga, znanstvenih časopisa, web izvora te izvori koji nisu javno dostupni (privatni materijali vendora kao što su *Trend Micro, Simantec, Fortinet, Crowdstrike, Proofpoint*) a koji su dostupni autoru rada. Primarni podaci dobiveni su putem provedene ankete koja je bila namijenjena svim zaposlenima u dobi između 18 i 65 godina.

Anketni upitnik poslan je na privatne mail adrese te je objavljen na društvenim mrežama autora ovog rada. Ispunjavanju ankete je pristupilo 168 osoba od kojih je 5% dalo odgovor da nisu zaposleni te su njihovi odgovori izuzeti od ukupnih rezultata.

5.2. Metode istraživanja

Istraživački dio rada temelji se na kvantitativnoj metodi istraživanja, odnosno anketi. Prema tehnikama prikupljanja empirijskih podataka provela se metoda ispitivanja, odnosno anketiranja pomoću anketnog upitnika kreiranog na platformi Google-forms.

Anketno ispitivanje provedeno je prvenstveno zbog mogućnosti kontakta sa većim brojem pojedinaca te zbog obuhvaćanja većeg uzorka populacije.

Anketni upitnik sadržavao je 20 pitanja a odgovori koji se uzimaju u obzir su odgovori svih koji su zaposleni.

5.3. Postupak provedbe istraživanja

Anketno istraživanje je provedeno na uzorku od 168 ispitanika: muškarci (37,9%) i žene (62,1%); u dobi od 18 do 65 godina, pretežito visokoobrazovani (više od 60% ispitanika ima završen fakultet ili viši stupanj obrazovanja). Najveći broj ispitanika radi u društvenim, socijalnim i osobnim uslužnim djelatnostima (36%) a najmanje u prerađivačkoj, istraživanje i razvoj, poljoprivreda lov i šumarstvo (2%). Ovaj uzorak prikladan je za dobivanje indikativnih rezultata i donošenja općih zaključaka o utjecaju obrazovanja na znanje o kibernetičkoj sigurnosti.

Anketno istraživanje provedeno je u razdoblju od 14 dana – od 1.6.2022 do 14.6.2022 godine.

Ograničenja ovog istraživanja uključuju dob ispitanika te zastupljenost ispitanika prema vrsti i sektoru zaposlenja te različite razine obrazovanja. Samoprocjena ispitanika je često individualna te nemaju svi ispitanici jednake kriterije u procjenjivanju pojedinih faktora. Također, istraživanje je provedeno u online okruženju i nekontroliranim uvjetima, pa se ne može procijeniti pouzdanost rezultata. Vjerojatno i starije dobne skupine ispitanika ne koriste Internet u jednakoj mjeri, što utječe na malu zastupljenost starijih ispitanika. Nadalje, ispitanici u ovom istraživanju pretežito su visokoobrazovani te postoji mogućnost drugačijih rezultata u slučaju da je zastupljenost ostalih obrazovnih stupnjeva veća.

5.4. Metode obrade podataka

Obrada dobivenih podataka je podijeljena u dva dijela. Anketni rezultati su obrađeni IBM,SPSS alatom te su se unutar tog alata napravljene slijedeće statističke obrade : Cronbach alpha, deskriptivna statistika i Anova.

Cronbach Alpha (α) koeficijent koristi se za mjerenje pouzdanosti mjerne ljestvice ili testa. Pouzdanost se definira kao mogućnost da određeni produkt, sustav ili usluga odrade svoje funkcije na adekvatan način u određenom vremenskom periodu, ili da će funkcionirati u određenom vremenu bez greške. Kada se radi mjerenje nekog procesa za koji se pretpostavlja da je konzistentan u vremenu tada i rezultati koje dobijemo moraju biti konzistentni. Pouzdanost testiranja i retestiranja je mjera koja određuje da li je to u stvarnosti tako. Cronbachov Alpha je mjera konzistentnosti odnosno koliko su bliski setovi određenih podataka unutar neke grupe.

Koeficijent se kreće od 0 do 1. Što je bliže 1, stavke će biti međusobno usklađenije (i obrnuto). S druge strane, mora se uzeti u obzir da što je test duži, to je alfa (α) veća.

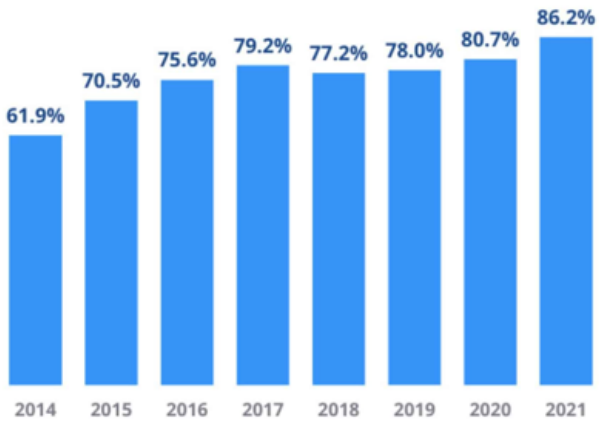
Na primjer ako test ima pouzdanost od 0.80 tada je 0.36 varianca pogreške u tim podacima (0.80*0.80=0.64; 1-0.64= 0.36). Što se procjena pouzdanosti povećava to se smanjuje postotak variance pogreške. Neispravno korištenje alphe može dovesti do situacija gdje će ili test ili mjerilo biti odbačeno ili će se test okarakterizirati kao nepouzdan. Kako bi izbjegli takve situacije jednodimenzionalnost može pomoći kako bi poboljšali uporabu alphe. Fundamentalno koncept pouzdanosti podrazumijeva da jednodimenzionalnost postoji u određenom broju testiranih objekata. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/, pristupio 1.7.2022)

6. Rezultati istraživanja

Problem koji se istražuje ovim radom je sve veći broj raznih kibernetičkih napada i preniska ulaganja u educiranje djelatnika te posljedično i nisko znanje djelatnika o kibernetičkoj sigurnosti.

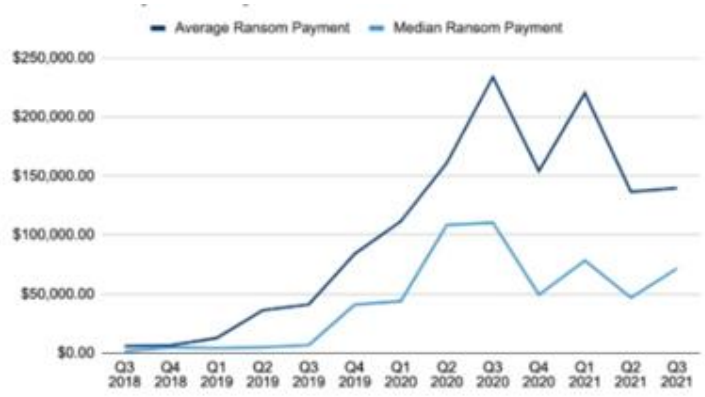
Cilj ovog diplomskog rada je doprinijeti svijesti o važnosti kibernetičke sigurnosti i naglasiti ulogu zaposlenika u tom procesu zaštite te prikazati utjecaj COVID-19 pandemije na područje kibernetičke sigurnosti.

6.1. Rezultati desk-metoda



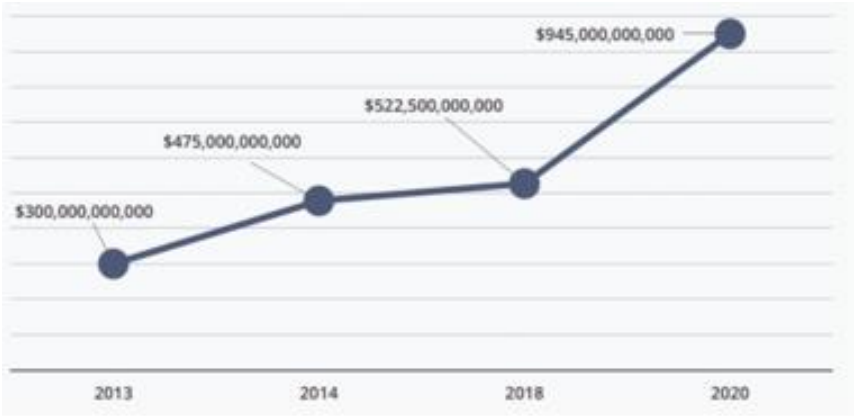
Slika 5: Postotak organizacija kompromitiranih barem jednim uspješnim kibernetičkim napadom

Izvor: ACSC Annual Cyber Threat Report https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (pristupio 4.6.2022)



Slika 6: Isplate otkupnine za kibernetičke napade po kvartalima

Izvor: ACSC Annual Cyber Threat Report https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (pristupio 4.6.2022)



Slika 7: Procijenjeni trošak kibernetičkih napada po godinama

Izvor: ACSC Annual Cyber Threat Report https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (pristupio 4.6.2022)

Pandemija COVID-19 je stvorila do sada neviđeni pritisak na tvrtke i zaposlenike kako bi promijenili način na koji rade i komuniciraju. Kompanije moraju brzo digitalizirati svoje poslovne modele, stvoriti fleksibilna radna mjesta i omogućiti rad na daljinu, naći nove klijente te upravljati sa zaposlenicima kroz digitalne kanale. Ovo stvara priliku za sektor kibernetičke sigurnosti koji se mora prilagoditi na sve veći broj kibernetičkih napada a isto tako na sve veći broj kompanija koje zahtijevaju usluge kibernetičke sigurnosti. Potražnja za adekvatnim kadrom je i prije pandemije COVID-19 bila visoka. U 2019. godini je procijenjeno da nedostaje

500,000 profesionalaca iz područja kibernetičke sigurnosti samo u USA nakon početka COVID-19 pandemije ta se brojka još više povećala a manjak adekvatnog kadra iz područja kibernetičke sigurnosti se osjetila pogotovo u područjima zdravstva, bankarstva i osiguranja. Kao rezultat ove krize pojavljuju se novi izazovi koji će biti stavljeni pred profesionalne kibernetičke sigurnosti. Dobivenim rezultatima ankete potvrđeno je da preko 80% profesionalca kibernetičke sigurnosti primijetilo promjene u svojim dnevnim aktivnostima radi COVID-19 pandemije. Više od pola ih je prešlo s tradicionalnih rola na pomaganje oko IT zadataka kao što su otklanjanje smetnji na računalima i mreži, instaliranje VPN mreža i pomoć službi za korisnike. Isto tako preko četvrtine profesionalaca kibernetičke sigurnosti je prijavilo da se broj intervencija po pitanju kibernetičke sigurnosti povećao od kada su prešli na udaljeni način rada. Prema dostupnim podacima COVID-19 pandemija je utjecala na rad profesionalaca kibernetičke sigurnosti na tri načina.

Vrsta napada se nije promijenila ali se promijenila njihova učestalost kao i broj kompanija i djelatnika koji su u opasnosti. Dok zaposlenici koji rade od kuće su sigurniji od izlaganja korona virusu, izlažu se većem riziku zaraze virtualnim virusom. Sve češće dolaze u kontakt s *malwareom, phishing-om* i ostalim vrstama napada koristeći osobne internetske mreže i uređaje. Kao rezultat toga stručnjaci kibernetičke sigurnosti sastavljaju infrastrukturu koja će pomoći organizacijama da se prilagode na sve veći broj sigurnosnih prijetnji koje uzrokuje rad na daljinu a što uključuje manje sigurne mreže, povećan broj cyber kriminalaca te povećanje broja *ransomeware* napada. Prema Dan-u Pattersonu iz CBS-a između siječnja i ožujka 2020. godine spam se povećao za 25%, *malware* za 35% i blokiranje loših URL-ova preko 55%. Povećano korištenje platformi za video konferencije između zaposlenika može dovesti kompaniju u rizik s obzirom da nisu sve platforme za komunikaciju sigurne i ne zahtijevaju da su sigurnosne funkcije omogućene.

Povećani broj kompanija koje traže *cybrsecurity* rješenja Prema Talent Trends, samo dvije od pet kompanija je prijavilo da su bile potpuno ili djelomično digitalne prije COVD-19 pandemije. Svjedočimo porastu korištenja VPN-a za 66% na kraju ožujka 2020.

Profesionalci za kibernetičku sigurnost pomažu i dalje će pomagati kompanijama u prijelazu na rad na daljinu na način da uspostave sigurnosne alate za rad na daljinu, *root acess to maschines* (glavni pristup strojevima) te da poboljšaju mrežne sposobnosti. Iako su neke tvrtke već imala ove sustave posložene, mnoge kompanije a posebno male tvrtke još nisu digitalizirale svoje poslovne modele. Dok su se mnoge kompanije oslanjale na fizičke zaštite podataka unutar ureda, prijelaz na rad na daljinu znači da se te kompanije više ne mogu oslanjati

na sigurna računala, mrežu, Internet i sigurnosne procedure unutar kompanije. Umjesto toga moraju se prilagoditi kako bi osigurali da svaki zaposlenik koji radi od kuće radi na siguran način te da se omogući siguran pristup podacima od bilo kuda. To može značiti da treba osigurati korištenje sigurnih mreža, VPN konekcija te da se prate sigurnosne procedure na ispravan način. Ako zaposlenici koriste svoja računala i uređaje, kompanije moraju omogućiti i „*bring your own device* (donošenje vlastitog uređaja)“ sigurnosne procedure koje će zaposlenici pratiti. To sve može biti vrlo izazovne za kompanije koje se nisu pripremile za tranziciju na digitalni način rada.

Povećana potražnja za sigurnosnim rješenjima određenih industrija

Sektor zdravstva je pod posebnim povećalom i pod sve većim brojem napada u vrijeme COVID-19 pandemije. Individualci traže on line platforme o medicinskim informacijama i uslugama. Iako neke zdravstvene ustanove već imaju napredne internetske servise i dalje su pod velikim rizikom jer su napadi prilagođeni vijestima o COVID-19 pandemiji. Te organizacije isto tako imaju povećani mrežni promet. Dodatno banke i osiguravajuće kuće će biti posebno ciljane jer se oslanjaju na starije tehnologije i infrastrukturu koja se ne može fizički premjestiti ili prebaciti na online način rada. Na primjer veliki broj osiguravajućih kuća rade na *main-fraimes* , što zahtjeva da zaposlenici rade u fizičkom uredu. U biti kompanije i zaposlenici se suočavaju sa strmom krivuljom učenja i nemaju puno prostora za pogreške koje mogu rezultirati sigurnosnim probojem. Kako sve veći broj tvrtki gleda na koji način što brže prijeći na udaljeni način rada, stručnjaci kibernetičke sigurnosti ne mogu pratiti te promjene dok se bave zaštitom sustava i educiranjem zaposlenika o važnosti praćenja sigurnosnih pravila. Poslovne organizacije koje uspostave rad na daljinu dugoročno mogu otkriti da im je taj model puno bolji.

Unatoč ovim nesigurnim vremenima COVOD-19 pandemija pruža priliku sektoru kibernetičke sigurnosti da ostvari rast radi sve veće potražnje za uslugama vezanim za kibernetičku sigurnost. Prelazak na rad na daljinu je pokazao da je *networking* (umrežavanje) ključan za tvrtke koje žele raditi udaljeno. Isto tako prelazak rada na *cloud* smanjuje troškove i smanjuje potrebu za fizičkom infrastrukturom. Oni koji planiraju tek sada ući u područje kibernetičke sigurnosti se trebaju fokusirati na konfiguraciju mreže jer će potreba za tim znanjima samo rasti i sve veći broj poslovnih organizacija će trebati te vještine. Nadalje stručnjaci za kibernetičku sigurnost će morati naučiti raditi pomoću udaljenog pristupa i u timskom okruženju. Prelazak na rad na daljinu zahtjeva da se i sektor kibernetičke sigurnosti prilagodi i pruži bolje alate za podršku na daljinu. Utjecaj COVID-19 pandemije zahtjeva da

profesionalci za kibernetičku sigurnost imaju šire vještine i kompetencije koja uključuje i efikasno i efektivno komuniciranje, strpljenje, upravljanje vremenom, agilnost, organizacija i rješavanje problema.

Cyber kriminalci su zatražili milione dolara od tvrtki za vrijeme COVID-19 pandemije koristeći najčešće napade kao što su *Phishing* i socijalni inženjering. Prema Danu Pattersonu iz CBS-a prosječni trošak proboja podataka poslovnih organizacija je iznosio 21.659 dolara po incidentu za vrijeme pandemije dok su se vrijednosti kretale od 800 dolara do 650.000 dolara. Samo 5 % uspješnih napada je koštalo kompanije 1 milion dolara ili više. Čak 85 % uspješnih proboja se odnosilo na prevaru djelatnika a ne na iskorištavanje mana unutar kompjuterskog koda. Iako specifične tehnike se razlikuju ovisno o industriji 61% svih proboja podataka su rezultati prevara koje pokušavaju prikupiti login podatke za pristup povjerljivim podacima kao što su *phishing* prevare.

Nekoliko ključnih faktora doprinose popularnosti *phishing i ransomware* napada. Mnoge kompanije koriste e-mail sigurnosne sustave kako bi uklonili količinu i učestalost *phishing* napadana način da skeniraju sumnjive linkove i privitke unutar mailova. Ali korporativni e-mail ostaje i dalje najčešći način napada kojim haker može dobiti nedozvoljeni pristup kompjuteru, mreži ili serveru kako bi lansirao cyber napad. U 2021. godini 36% uspješnih Cyber napada je uključivalo *phishing* napade što je povećanje od 11% u odnosnu na 2020. *Ransomware* je maliciozni software koji prijeti da će objaviti privatne podatke ukoliko se ne plati otkupnina je postao jako popularan među cyber kriminalcima jer nudi brzi način za zaradu. Mnogi *ransomware* alati su komercijalizirani i pojednostavnjeni. I dok su vještine programiranja samo bonus nisu više potrebne za izvršenje *ransomware* napada. Kao rezultat gore navedenog *ransomware as s Service* (otkupnina kao usluga) je u porastu.

Prije pandemije kriminalci su morali uložiti vrijeme i resurse u istraživanje mete. Danas oni mogu unajmiti *ransomware* uslugu na *dark webu (mračni web)* ili kupiti software koji im omogućava napad korištenjem maila. Za vrijeme COVID-a i udaljenog načina rada, vektori prijetnji su se prebacili na ciljanje zaposlenika mailovima vezanim za COVID kako bi kapitalizirali na stresu, strahu i tjeskobi za vrijeme pandemijske situacije. Zaposlenici u financijama, zdravstvu, javnoj administraciji i prodaji su se pokazali kao najbolje mete za prevarante. Financijske usluge i osiguranja su osjetila najveća povećanja u *ransomware* i *phishing* napadima u 2021.godini. Zdravstvo je isto tako pod povećanim brojem napada, a prema izvještajima ljudska pogreška je najčešći razlog incidenata. Socijalni inženjering i *phishing* iznosi 69% svih kibernetičkih napada koji ciljaju administratore. Nadalje kriminalci

najčešće napadaju djelatnike iz maloprodaje sa prevarama vezanim za prijenos novca. Najčešće taktike koriste *phising i pretexting*, oboje uključuju osmišljavanje priče koja će natjerati žrtvu da otkrije svoju lozinku ili neke druge osjetljive podatke. Isto tako prelaskom na cloud usluge porastao je broj napada na web aplikacije za 39%.

6.2. Rezultati ankete field-metoda

Socio-demografska struktura ispitanika ovog istraživanja prikazana je na slici 1. Uzorak su činili potrošači: muškarci (37,9%) i žene (62,1%); u dobi od 18 do 65 godina, pretežito visokoobrazovani (više od 60% ispitanika ima završen fakultet ili viši stupanj obrazovanja). Najveći broj ispitanika radi u ostalim društvenim, socijalnim i osobnim uslužnim djelatnostima (36%) a najmanje u prerađivačkoj, istraživanje i razvoj, poljoprivreda lov i šumarstvo (2%). Ovaj uzorak prikladan je za dobivanje indikativnih rezultata i donošenja općih zaključaka o utjecaju obrazovanja na znanje o kibernetičkoj sigurnosti.

Socio-demografska struktura	**n**	**%**
SPOL		
Muški	64	37.9%
Ženski	105	62.1%
Ukupno	169	100.0%
DOB		
18-26	19	11%
27-35	61	36%
36-44	72	43%
45-53	7	4%
54-65	10	6%
Ukupno	169	100%
ŠKOLSKA SPREMA		
Osnova škola	0	0%
Srednja škola	52	31%
Fakultet	59	35%
Magisterij	58	34%
Doktorat	0	0%
Ukupno	169	100%
VRSTA DJELATNOSTI		
Zdravstvena i socialna zaštita	9	5%
Ostale društvene, socijalne i osobne uslužne djelatnosti	60	36%
Poslovanje nekretninama, iznajmljivanje i poslovne usluge	3	2%
Trgovina na veliko i malo	42	25%
IT industrija	33	20%
Prerađivačka industrija	3	2%
Obrazovanje	9	5%
Istraživanje i razvoj	3	2%
Poljoprivreda lov i šumarstvo	3	2%
Građevinarstvo	4	2%
Ukupno	169	100%

Slika 8 : Rezultati demografskih pokazatelja

Izvor: izrada autora

Cronbach Alpha koeficijet u ovom zadatku mjeren je na 14 čestica na koje su ispitanici mogli dati odgovore . Koeficijent pouzdanosti koji je dobiven analizom jest 0,663 – što znači kako je dobra pouzdanost.

Case Processing Summary

		N	%
Cases	Valid	168	100.0
	Excluded[a]	0	.0
	Total	168	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.663	14

Slika 9: Prikaz rezultata Cronbach alpha

Izvor: IBM SPSS izrada autora

Prikazuje Anova analizu modela za testiranje hipoteze H1: Razina obrazovanja utječe na znanje o kibernetičkoj sigurnosti. Anova rezultati pokazuju da je značaj testa bio veći od 0,01 (0,297 i 0.304).

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Upoznat sam sa pojmom ransomweare.	Between Groups	0.611	2	0.305	1.224	0.297
	Within Groups	41.175	165	0.25		
	Total	41.786	167			
Najslabija karika u kiber2tičkoj sigurnosti su ljudi.	Between Groups	2.187	2	1.094	1.2	0.304
	Within Groups	150.331	165	0.911		
	Total	152.518	167			

Slika 10: prikaz rezultata Anove

Izvor: IBM SPSS izrada autora

Na temelju deskriptivne statistike dobiveni su slijedeći rezultati. Standardna devijacija na svim pitanjima se kreće između 0,9 i 1,4. Vidljivo je da je najviše ispitanika identificiralo da su ljudi najslabija karika u kibernetičkoj sigurnosti (Mean=4.05, σ = 0,956). Nadalje, vidljivo je da

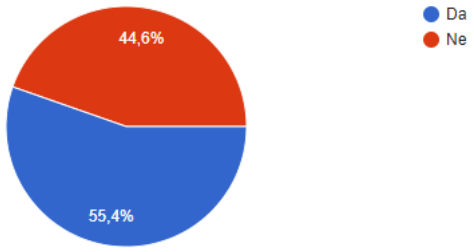
većina organizacija nije osigurala edukaciju za rad od kuće po pitanju kibernetičke sigurnosti (Mean=2,30, σ = 1,379).

Descriptive Statistics

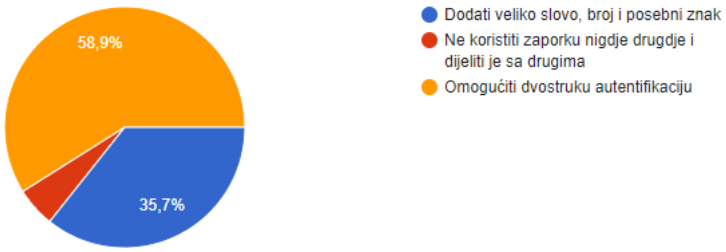
	N	Minimum	Maximum	Mean	Std. Deviation
ÄŠesto radim back-up po1taka.	168	1	5	3.02	1.412
Moja organizacija ulaže u edukaciju djelatnika po pitanju kiber2tičke sigurnosti.	168	1	5	2.43	1.391
Moja organizacija je osigurala edukacije za rad od doma po pitanju kiber2tičke sigurnosti.	168	1	5	2.30	1.379
Moja organizacija je osigurala podršku za vrijeme ra1 od doma po pitanju kiber2tičke sigurnosti.	168	1	5	2.57	1.442
U mojoj organizaciji je kiber2tička sigurnost na visokoj razini	168	1	5	3.21	1.389
Svoje znanje o kiber2tičkoj sigurnosti procjenjujem kao?	168	1	5	2.84	.981
Najslabija karika u kiber2tičkoj sigurnosti su ljudi.	168	1	5	4.05	.956
Valid N (listwise)	168				

Slika 11. prikaz rezultata deskriptivne statistike

Izvor: IBM SPSS izrada autora

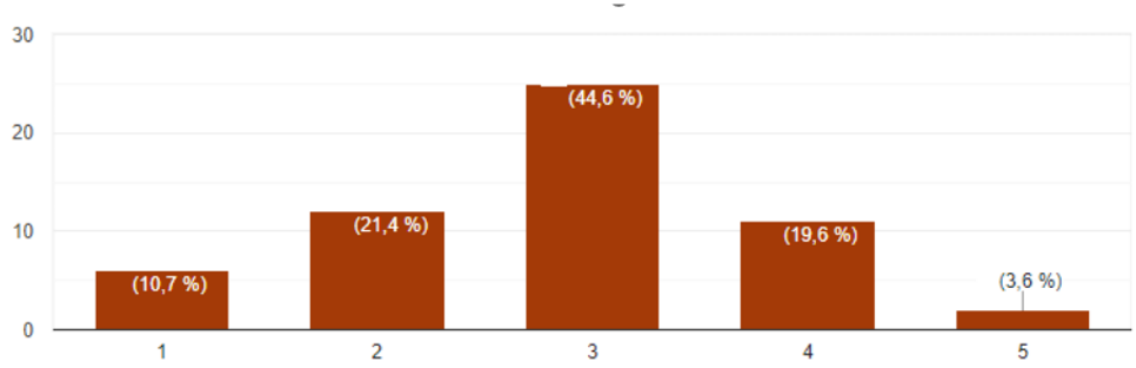


Slika 12: Grafički prikaz upoznatosti s pojmom dvostruke autentifikacije



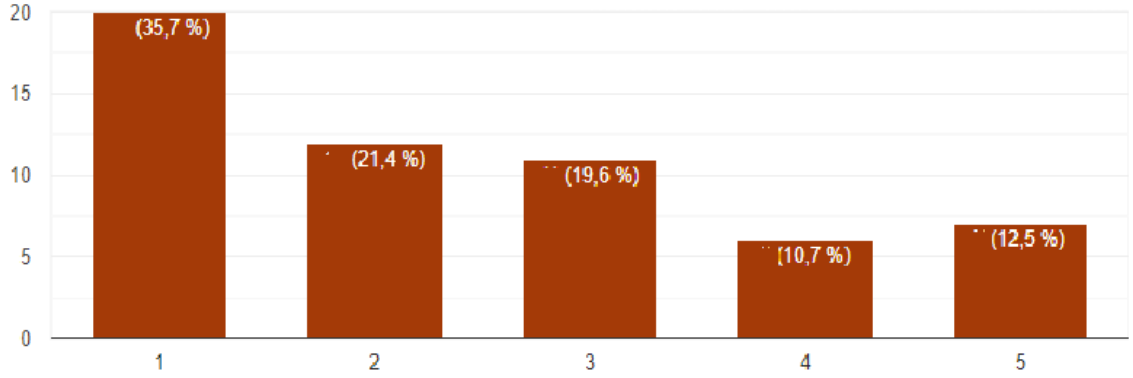
Slika 13: Grafički prikaz odgovora na pitanje koji je najbolji način za ojačati lozinku

Na Likertovoj ljestvici o vlastitoj procjeni znanja ispitanici su najviše odabrali odgovor 3. Što pokazuje da se većina ispitanika držala srednje vrijednosti, a vrlo mali broj ispitanika je dao odgovor 5 odnosno procijenio svoje znanje kao izvrsno.



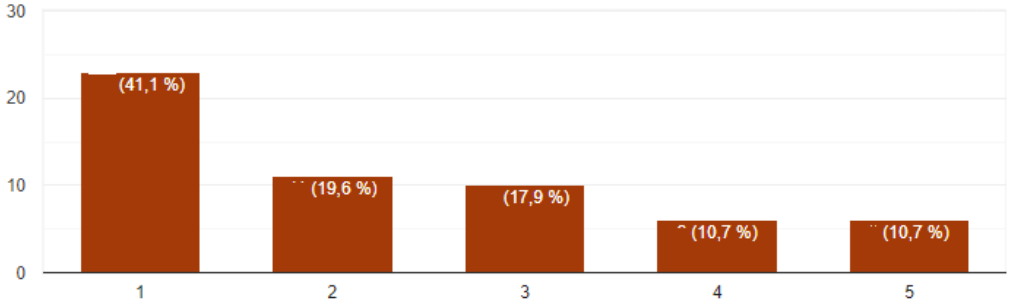
Slika 14: Grafički prikaz vlastite procjene znanja o kibernetičkoj sigurnosti ispitanika

Na Likertovoj ljestvici o tome ulaže li organizacija u edukaciju djelatnika po pitanju kibernetičke sigurnosti najveći broj odgovora je bio 1 što znači da kompanije ne ulažu u kibernetičku sigurnost.



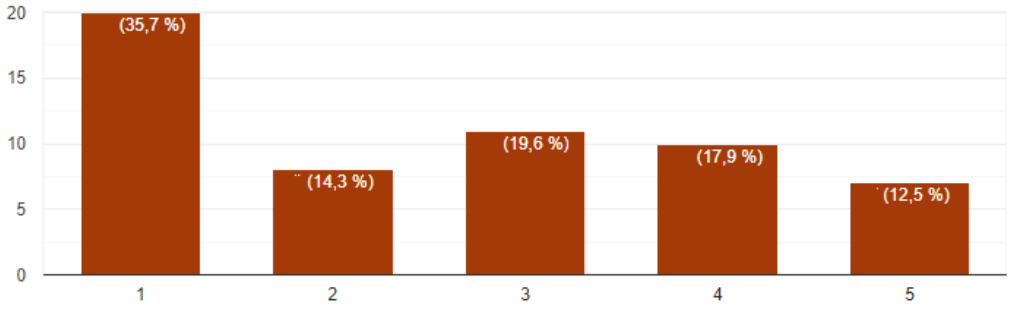
Slika 15: Grafički prikaz odgovora na pitanje „moja organizacija ulaže u edukaciju djelatnika po pitanju kibernetičke sigurnosti“

Na Likertovoj ljestvici o tome da li je poslovna organizacija osigurala edukacije za rad od kuće po pitanju kibernetičke sigurnosti najveći broj odgovora je bio 1 što znači da kompanije nisu osigurale potrebne edukacije za rad od kuće.



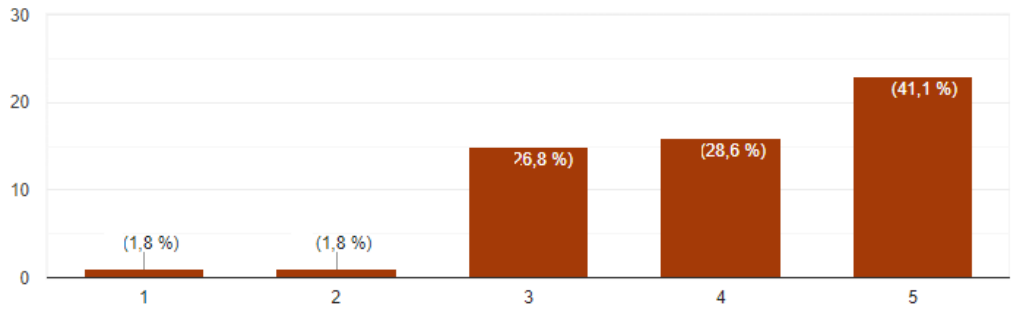
Slika 16: Grafički prikaz odgovora na pitanje „moja organizacija je osigurala edukacije za rad od kuće po pitanju kibernetičke sigurnosti“

Na Likertovoj ljestvici o tome da li je moja poslovna organizacija osigurala podršku za vrijeme rada od kuće po pitanju kibernetičke sigurnosti najveći broj odgovora je bio 1 što znači da kompanije nisu osigurale potrebnu podršku za rad od kuće.



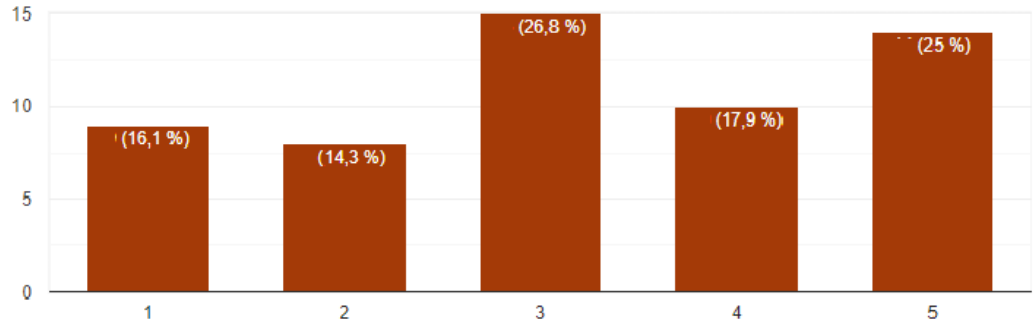
Slika 17: Grafički prikaz odgovora na pitanje „ moja organizacija je osigurala podršku za vrijeme rada od kuće po pitanju kibernetičke sigurnosti“

Na Likertovoj ljestvici o tome da li su najslabija karika u kibernetičkoj sigurnosti ljudi najveći broj odgovora je bio 5 što znači da su ispitanici svjesni ključne uloge djelatnika u sigurnosti.

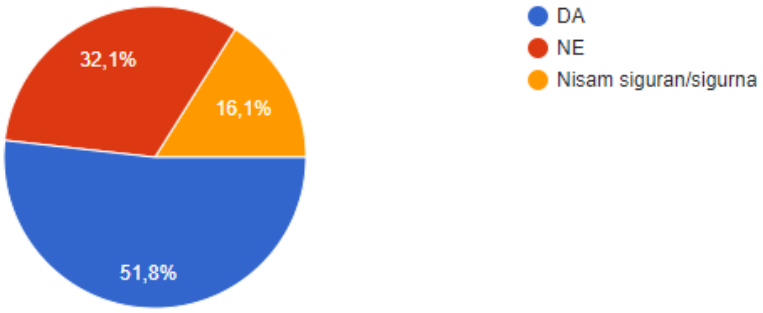


Slika 18: Grafički prikaz odgovora na pitanje „najslabija karika u kibernetičkoj sigurnosti su ljudi“

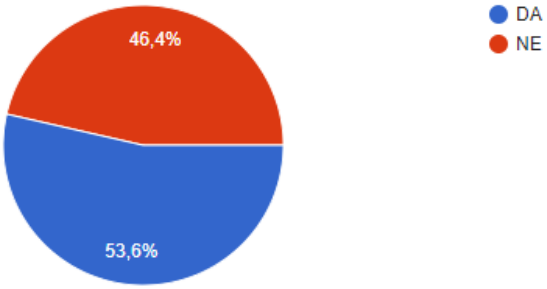
Na Likertovoj ljestvici o tome da li je u njihovoj organizaciji kibernetička sigurnost na visokoj razini ispitanici su dali različite odgovore što je i razumljivo s obzirom na različitost poslovnih organizacija.



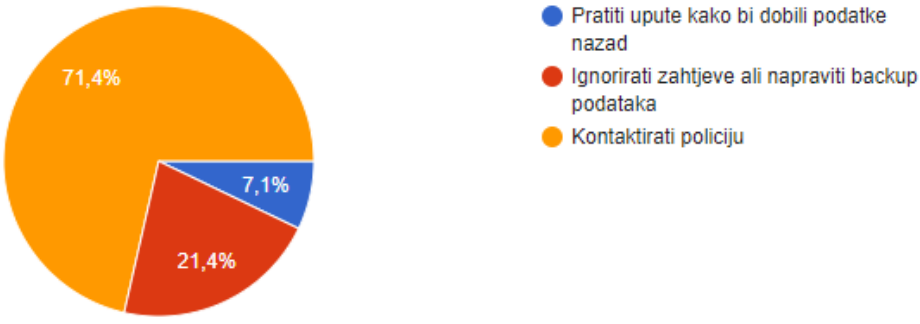
Slika 19: Grafički prikaz odgovora na pitanje „u mojoj organizaciji je kibernetička sigurnost na visokoj razini“



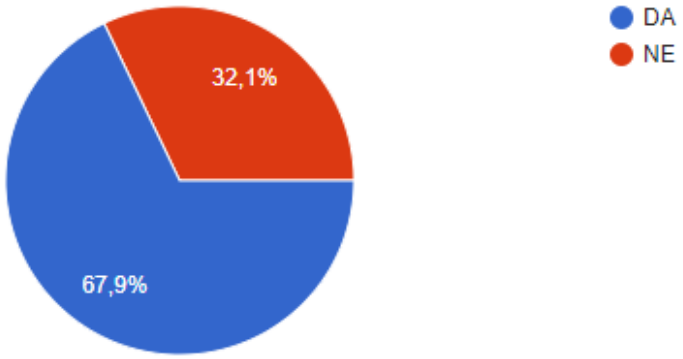
Slika 20: Grafički prikaz odgovora na pitanje „na poslu imamo pravila za kreiranje lozinki“



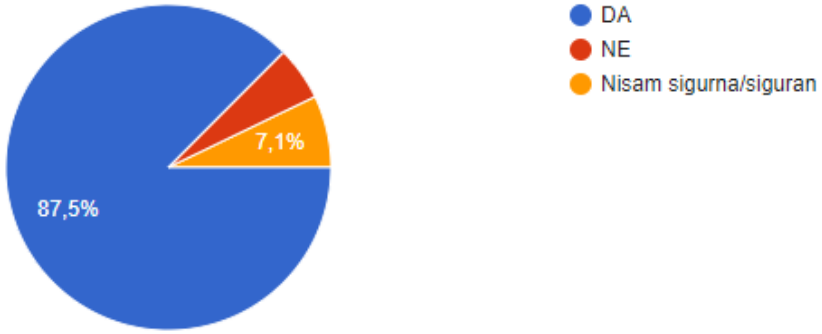
Slika 21: Grafički prikaz odgovora na pitanje „upoznat sam s pojmom ransomeware“



Slika 22: Grafički prikaz odgovora na pitanje „Što prvo trebate napraviti ako dođe do ransomeware napada“ ?



Slika 23: Grafički prikaz odgovora na pitanje „na poslu koristim i privatne uređaje“



Slika 24: Grafički prikaz odgovora na pitanje „na službenim računalima imamo instaliran antivirusni program“

7. Diskusija rezultata

Analizom odgovora dobivenih kroz provedenu anketu dobiven je uvid u odnos znanja i kibernetičke sigurnosti poslovne organizacije te je dobiven uvid o utjecaju COVID-19 pandemije na udaljeni rad i kibernetičku sigurnost kroz provedeno istraživanje.

7.1. Interpretacija rezultata istraživanja

Prema dobivenim rezultatima istraživanja provedenog desk metodom koje se odnosilo na povezanost COVID-19 pandemije i udaljenog rada na broj kibernetičkih napada može se jasno vidjeti vrlo uska povezanost. Veliki broj kompanija nije bio spreman za COVID-19 pandemiju koja ih je natjerala da ubrzaju svoju digitalnu transformaciju i omoguće svojim djelatnicima rad s udaljenim pristupom. Iako prelazak na rad od kuće nije značio samo ulaganje u infrastrukturu (hardver i softver) nego i u edukaciju djelatnika za novi način rada mnoge kompanije su upravo u tom segmentu napravile propust. Iz istraživanja se može vidjeti da je porastao broj hakerskih napada te je broj organizacija koje su napadnute s barem jednim kibernetičkim napadom porasla s 79% u 2019. godini na 86% u 2021. S obzirom da je najveći broj napada bio *ransomweare* broj isplaćenih otkupnina (ransome) je porastao s 100.000 dolara u 2019. godini na 250.000 dolara u 2021. godini. Ukupna prosječna vrijednost kibernetičkih napada je porasla s 522.500,000,000 dolara na 945.000,000,000 dolara. (https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 pristupio 15.6.2022).

Rezultati dobiveni istraživanjem provedenog field-metodom jasno daju do znanja kako je čovjek najslabija karika po pitanju kibernetičke sigurnosti (70% ispitanika se slaže s tom tvrdnjom). Isto tako moguće je vidjeti da kompanije nisu ulagale u edukaciju te osigurale podršku svojim zaposlenicima za vrijeme COVID-19 pandemije po pitanju kibernetičke sigurnosti jer je preko 50% ispitanika odgovorilo da nisu imali nikakvu edukaciju niti podršku. Isto tako 40% ispitanika se ocijenilo sa niskom ocjenom po pitanju znanja o kibernetičkoj sigurnosti što korelira s odgovorima na pitanja kao što su „upoznat sam sa pojmom *ransomeware*“ , „upoznat sam sa pojmom dvostruke autentifikacije“ i „ koji je najbolji način za ojačati lozinku“. Većina ispitanika je na ta pitanja odgovorila da nisu upoznati s navedenim pojmovima te nisu znali na koji način ojačati lozinku.

7.2. Elaboracija istraživačkog pitanja i hipoteza

Istraživačko pitanje: *Kakav utjecaj ima znanje na kibernetičku sigurnost poslovne organizacije?*

Istraživanje je pokazalo da znanje djelatnika ima direktan utjecaj na kibernetičku sigurnost poslovne organizacije te da ulaganje u edukacije djelatnika nisu na zadovoljavajućoj razini. Slijedom navedenog, odgovor na istraživačko pitanje je: **znanje ima bitan utjecaj na kibernetičku sigurnost poslovne organizacije.**

Hipoteze:

H1: Razina obrazovanja utječe na znanje o kibernetičkoj sigurnosti.

Primjenom field-metode kroz anketni upitnik i obradom dobivenih podataka IBM-ovim SPSS alatom rezultati Anove pokazuju da je značaj testa bio veći od 0,01 (0,297 i 0,304). Isto znači da stupanj obrazovanja i znanja ima direktan utjecaj na kibernetičku sigurnost poslovne organizacije što znači da je postavljena hipoteza **H1 prihvaćena.**

H2: Prelazak na udaljeni način rada uzrokovan COVID-19 pandemijom značajno je utjecao na povećani broj kibernetičkih napada.

Primjenom desk-metode te uzimajući u obzir podatke prikupljene u istraživanju koji ukazuju na trend većeg broja napada uslijed prelaska na udaljeni način rada uzrokovan COVID-19 pandemijom zaključuje se kako je hipoteza **H2 potvrđena.**

7.3. Primjena rezultata i preporuke

Vrlo mali broj zaposlenika ima razvijenu svijest o važnosti kibernetičke sigurnosti unutar poslovnih organizacija što je direktan utjecaj nedovoljnog ulaganja u educiranje djelatnika. Stoga je istraživanje u ovom radu bilo koncentrirano na samoprocjenu znanja o kibernetičkoj sigurnosti samih ispitanika te na njihovo poznavanje pojmova iz područja kibernetičke sigurnosti. Ono što je svakako potrebno naglasiti je da postoje ograničenja u provedbi anketnog upitnika koja se vežu uz poznavanje specifičnih znanja iz područja kibernetičke sigurnosti te zastupljenost ispitanika prema vrsti i sektoru zaposlenja, a ispitanici su bili pretežito visoko obrazovani.

Iz toga razloga potvrđivanje hipoteze o utjecaju znanja na kibernetičku sigurnost fokusirano je na odgovore vezane isključivo na pojmove kibernetičke sigurnosti te usporedba odgovora s razinom obrazovanja pojedinog ispitanika.

COVID-19 pandemija je ubrzala proces digitalne transformacije nekih poslovnih organizacija te je pritom omogućila hakerima veću površinu za napade (veći broj *endpointa*). Posebno su ciljani djelatnici medicinskih ustanova te osiguravajućih kompanija koji su za vrijeme COVID-19 pandemije bili najviše izloženi. Bez obzira na kvalitetu mrežne infrastrukture i jačinu zaštite ljudi su i dalje kritična točka svakog sustava.

Kako bi se uspješno zaštitili od hakerskih napada poslovne organizacije moraju razmišljati o nekoliko ključnih stavki. Razumijevanje prijetnji poslovnoj organizaciji je ključno kako bi se zaštitili najbitniji podaci. Potrebno je sastaviti jasne upute za sve zaposlenike i poticati komunikaciju i razmjenu informacija među zaposlenicima. Bitno je da su politike zaštite za vrijeme rada od kuće jasne i jednostavne za implementiranje što će omogućiti zaposlenicima da zadrže svoje okruženje za vrijeme rada od kuće sigurnim. Omogućavanjem dodatnih nivoa zaštite te korištenjem naprednih XDR (*Extended detection and response*) mogućnosti olakšava upravljanje ključnim resursima i njihovu kontrolu. S druge strane i djelatnici moraju sudjelovati i to na način da koriste kompleksne lozinke i dvostruku autentifikaciju gdje je to moguće. Također potrebno je redovno nadograđivati svoj sustav i softver instalacijom dostupnih ažuriranja. Koristeći VPN može se postići veza između zaposlenika i poslovnih organizacija koja će biti sigurna te na kraju podizanjem znanja djelatnika o potencijalnim prijetnjama i vrstama napada na koje trebaju obratiti pozornost za vrijeme rada od kuće kao što su *phishing* napadi.

Iz svega gore navedenog vidljivo je da je potrebno veliko ulaganje u znanje djelatnika i konstantna edukacija po pitanju važnosti kibernetičke sigurnosti, a ne samo ulaganje u infrastrukturna rješenja.

8. Zaključak

Neosporno je da je kibernetička sigurnost svake poslovne organizacije od neizmjerne važnosti za poslovanje te organizacije kako radi zaštite svojih sustava tako i nastanka velike financijske štete, a posebno u kontekstu sve većeg broja napada prelaskom na rad od kuće koji je uzrokovala COVID-19 pandemija.

Ono na što se poslovne organizacije trebaju fokusirati i dodatno unaprijediti je znanje zaposlenika i svijest o važnosti kibernetičke sigurnosti unutar organizacije. Polako, ali sigurno svijest o važnosti kibernetičke sigurnosti se podiže i u Hrvatskoj no nedovoljnom brzinom. Stoga je nužno da se na edukaciji radi i prije stupanja u radni odnos, odnosno u srednjim školama i fakultetima.

Ovaj rad referirao se na općeniti problem nedostatka znanja o kibernetičkoj sigurnosti, a ovo važno područje potrebno je dodatno istražiti, posebno uzimajući u obzir brzinu digitalne transformacije kompanija i sve veći broj kibernetičkih napada.

U godinama koje dolaze možemo očekivati dodatni razvoj digitalnih rješenja (razvoj cloud aplikacija) i Internet of Things koji će povezivati sve sustave te koji će predstavljati posebnu prijetnju kompanijama koje nemaju educirane i svjesne zaposlenike.

9. Popis literature

KNJIGE:

Donald I. pipkin 1992. – Halting the hacker ; A practiacl guide to computer security second edition , pub. Pearson Education, New Jersey

Elizabeth Hardcastle 2008.– Business information systems pub. Ventus Publishing, USA

Mark S. Kadrich 2007.- Endpoint security pub. Pearson education Inc., Boston

Petar Kim 2018. – The hacker Playbook 3; practical guide to penetration testing, pub. Secure Planet LLC, USA

ZNANSTVENI ČLANCI:

ACSC (2021)- Annual Cyber threat report URL: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Bolisani E. (2018) – the elusive definition of knowledge, URL: https://www.researchgate.net/publication/318235014_The_Elusive_Definition_of_Knowlede

Chang, S.; at al. (2022) – Hacker typs, motivations and strategies : A comprehensive framework, URL: https://www.sciencedirect.com/science/article/pii/S245195882200001X

Ibrahimova, A.N. (2020) – The definitions of infromation and security; history of information security development URL: https://www.zurnalai.vu.lt/open-series/article/view/22387/21645

Jennex, M. E. (2007)- What is Knowledge management URL: https://www.researchgate.net/publication/314500732_What_is_Knowledge_Management?

Muzer M. at al. (2014) – Upravljanje znanjem , priručnik za poduzeća URL: https://bib.irb.hr/datoteka/740473.KM_2.0_HR.pdf

Vrkić Dimić, J. (2014.) – Suvremeni oblici pismenosti URL: https://hrcak.srce.hr/clanak/200650

Witten, I.H. at al. (1990.) – Liveware: a new approach to sharing dana in social networks URL: https://prism.ucalgary.ca/bitstream/handle/1880/45931/1990-389-13.pdf?sequence=2&isAllowed=y

Zagzebski, L. (1996.) – Što je znanje?, URL : https://pdfcoffee.com/zagzebski-sto-je-znanje-pdf-free.html

INTERNET IZVORI:

Annual cyberthreat report; https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 pristupio 4.2022

Business Information System: Meaning, Features and Components (yourarticlelibrary.com) URL: https://www.yourarticlelibrary.com/management/information-system/business-information-system-meaning-features-and-components/70319 pristupio 10.6.2022

CROSBI;https://bib.irb.hr/datoteka/1027604.Klaic_Regulatorni_okvir_kiberneticke_sigurnosti_u_RH.pdf pristupio 24.6.2022

Core; https://core.ac.uk/download/pdf/212481485.pdf pristupio 24.6.2022

Cyber news; https://cybernews.com/security/looking-back-the-state-of-cybersecurity-in-2021/ pristupio 4.7.2022

Cyberattack and COVID-19; https://www.pcquest.com/cyberattack-another-pandemic-wake-covid-19/ pristupio 24.5.2022

History of cybercrime; https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/ pristupio 13.6.2022

HHS; https://www.hhs.gov/sites/default/files/covid-19-cyber-threats.pdf pristupio 2.7.2022

Hardware definition; https://www.techtarget.com/searchnetworking/definition/hardware pristupio 13.6.2022

Impact of COVID-19 on cyber security; https://www.apprenticeship.gov/sites/default/files/impact-of-covid-19-on-cyber-security-industry.pdf pristupio 24.5.2022

Leaf; https://leaf-it.com/10-ways-prevent-cyber-attacks/ pristupio 18.6.2022

National library of medicine; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/, pristupio 1.7.2022

Središnji državni ured za razvoj digitalnog društva; https://rdd.gov.hr/izdvojeno/kiberneticka-sigurnost-1436/zastita-racunalnih-mreza/1441 pristupio 21.6.2022

Typs of cyberattacks; https://www.dnsstuff.com/common-types-of-cyber-attacks pristupio 13.6.2022

Utarrakhand open university; https://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf pristupio 18.6.2022

Working from home; https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/ pristupio 24.5.2022

Popis ilustracija

Slika 1: Vrste znanja…….11

Slika 2 : Proces upravljanja znanjem……12

Slika 3 : Vrste Hakera i njihovi motivi…….20

Slika 4. Trend Micro Endpoint protection proces…….27

Slika 5: Postotak organizacija kompromitiranih barem jednim uspješnim kibernetičkim napadom……32

Slika 6: Isplate otkupnine za kibernetičke napade po kvartalima…….32

Slika 7: Procijenjeni trošak kibernetičkih napada po godinama……...33

Slika 8 : Rezultati demografskih pokazatelja……37

Slika 9: Prikaz reultata Cronbach alpha……38

Slika 10: prikaz rezultata Anove……...38

Slika 11. prikaz rezultata deskriptivne statistike……...39

Slika 12: Grafički prikaz upoznatosti sa pojmom dvostruke autentifikacije……39

Slika 13: Grafički prikaz odgovora na pitanje koji je najbolji način za ojačati lozinku……...39

Slika 14: Grafički prikaz vlastite procjene znanja o kibernetičkoj sigurnosti ispitanika……..40

Slika 15: Grafički prikaz odgovora na pitanje „moja organizacija ulaže u edukaciju djelatnika po pitanju kibernetičke sigurnost……..40

Slika 16: Grafički prikaz odgovora na pitanje „moja organizacija je osigurala edukacije za rad od kuće po pitanju kibernetičke sigurnosti“…….41

Slika 17: Grafički prikaz odgovora na pitanje „ moja organizacija je osigurala podršku za vrijeme rada od kuće po pitanju kibernetičke sigurnosti“……41

Slika 18: Grafički prikaz odgovora na pitanje „najslabija karika u kibernetičkoj sigurnosti su ljudi“…….42

Slika 19: Grafički prikaz odgovora na pitanje „u mojoj organizaciji je kibernetička sigurnost na visokoj razini“……..42

Slika 20: Grafički prikaz odgovora na pitanje „na poslu imamo pravila za kreiranje lozinki“.43

Slika 21: Grafički prikaz odgovora na pitanje „upoznat sam sa pojmom ransomeware“…….43

Slika 22: Grafički prikaz odgovora na pitanje „Što prvo trebate napraviti ako dođe do ransomeware napada“ ?.....43

Slika 23: Grafički prikaz odgovora na pitanje „na poslu koristim i privatne uređaje“…….44

Slika 24: Grafički prikaz odgovora na pitanje „na službenim računalima imamo instaliran antivirusni program“…….44

Prilog 1. Anketni upitnik

Utjecaj znanja djelatnika na kibernetičku sigurnost poslovne organizacije

Poštovani,

pred vama se nalazi anketa kojoj je osnovna svrha dobiti uvid u opće znanje zaposlenih po pitanju kibernetičke sigurnosti njihovih poslovnih organizacija.

Rezultati ankete koristiti će se za izradu diplomskog rada na Sveučilištu Sjever.

Anketa je anonimna, a osobni podaci koji se traže koriste se isključivo u statističke svrhe. Ukupno vrijeme potrebno za popunjavanje ankete je do 5 minuta.

Hvala vam na sudjelovanju.
Tomislav Bobić

Spol? *

- ◯ Muško
- ◯ Žensko

Vaša dob? *

- ◯ 18-26
- ◯ 27-35
- ◯ 36-44
- ◯ 45-53
- ◯ 54-65

Jeste li zaposleni? *

- ◯ DA
- ◯ NE

Razina Vašeg obrazovanja? *

- završena osnovna škola
- srednja stručna sprema
- prvostupnik (završen dvogodišnji ili trogodišnji studij)
- Magistar
- Doktorat

U kojoj djelatnosti radite? *

- Poljoprivreda, lov i šumarstvo
- Ribarstvo
- Rudarstvo
- Prerađivačka industrija
- Građevinarstvo
- Trgovina na veliko i malo
- Ugostiteljstvo
- Promet, skladištenje i veze
- Poslovanje nekretninama, iznajmljivanje i poslovne usluge
- Obrazovanje
- Zdravstvena i socijalna zaštita
- Ostale društvene, socijalne i osobne uslužne djelatnosti
- IT industrija
- Istraživanje i razvoj

6. Upoznat sam sa pojmom dvostruke autentifikacije (2FA)? *

- ◯ Da
- ◯ Ne

7. Što prvo trebate napraviti ako dođe do ransomeware napada (napadač traži otkupninu za podatke koje vam je ukrao)? *

- ◯ Pratiti upute kako bi dobili podatke nazad
- ◯ Ignorirati zahtjeve ali napraviti backup podataka
- ◯ Kontaktirati policiju

8. Koji je najbolji način za ojačati lozinku? *

- ◯ Dodati veliko slovo, broj i posebni znak
- ◯ Ne koristiti zaporku nigdje drugdje i dijeliti je sa drugima
- ◯ Omogućiti dvostruku autentifikaciju

10. U razdoblju od 2020-2022 sam radio/radila od doma? *

- ◯ Do tjedan dana
- ◯ Do mjesec dana
- ◯ Do 6.mjeseci
- ◯ Do godinu dana
- ◯ Preko godinu dana
- ◯ Nisam radila/radio od doma u tom periodu

U mojoj organizaciji je kibernetička sigurnost na visokoj razini *

	1	2	3	4	5	
Uopće se ne slažem	◯	◯	◯	◯	◯	Slažem se u potpunosti

Svoje znanje o kibernetičkoj sigurnosti procjenjujem kao? *

	1	2	3	4	5	
Vrlo loše	◯	◯	◯	◯	◯	Izvrsno

Moja organizacija ulaže u edukaciju djelatnika po pitanju kibernetičke sigurnosti. *

	1	2	3	4	5	
Uopće se ne slažem	○	○	○	○	○	Slažem se u potpunosti

Moja organizacija je osigurala edukacije za rad od doma po pitanju kibernetičke sigurnosti. *

	1	2	3	4	5	
Uopće se ne slažem	○	○	○	○	○	Slažem se u potpunosti

Moja organizacija je osigurala podršku za vrijeme rada od doma po pitanju kibernetičke sigurnosti. *

	1	2	3	4	5	
Uopće se ne slažem	○	○	○	○	○	Slažem se u potpunosti

Najslabija karika u kibernetičkoj sigurnosti su ljudi. *

	1	2	3	4	5	
Uopće se ne slažem	○	○	○	○	○	Slažem se u potpunosti

Često radim back-up podataka. *

	1	2	3	4	5	
Uopće se ne slažem	○	○	○	○	○	Slažem se u potpunosti

Na poslu koristim i privatne uređaje (mobitel, laptop...). *

- ○ DA
- ○ NE

Na poslu imamo pravila za kreiranje lozinki. *

- ○ DA
- ○ NE
- ○ Nisam siguran/sigurna

Na službenim računalima imamo instaliran antivirusni program. *

- ○ DA
- ○ NE
- ○ Nisam sigurna/siguran

Upoznat sam sa pojmom ransomweare. *

- ○ DA
- ○ NE

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, Tomislav Bobić pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog/seminarskog (obrisati nepotrebno) rada pod naslovom
„Utjecaj znanja na kibernetičku sigurnost poslovne organizacije" te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)
Tomislav Bobić
(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, Tomislav Bobić neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog rada pod naslovom „Utjecaj znanja na kibernetičku sigurnost poslovne organizacije" čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)
Tomislav Bobić
(vlastoručni potpis)