Informacijska sigurnost i zaštita poslovanja od kibernetičkog napada

Toth, Josip

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:756181

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-28**

Repository / Repozitorij:

University North Digital Repository

SVEUČILIŠTE SJEVER
SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 410/PE/2022

Informacijska sigurnost i zaštita poslovanja od kibernetičkog napada

Josip Toth

Varaždin, rujan 2022.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij: Poslovna ekonomija

DIPLOMSKI RAD br. 410/PE/2022

Informacijska sigurnost i zaštita poslovanja od kibernetičkog napada

Student:

Josip Toth, 0246006993

Mentor:

izv. prof. dr. sc. Ljerka Luić

Varaždin, rujan 2022.

PRIJAVA DIPLOMSKOG RADA

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 Josip Toth | MATIČNI BROJ 0246006993

DATUM 14. 9. 2022. | KOLEGIJ Informacijska sigurnost i zaštita podataka

NASLOV RADA Informacijska sigurnost i zaštita poslovanja od kibernetičkog napada

NASLOV RADA NA ENGL. JEZIKU Information security and business protection from cyberattack

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

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

Zadatak diplomskog rada

BROJ 410/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 informacijske sigurnosti i zaštite poslovanja od kibernetičkog napada; potom je potrebno (2) Sistematično prikazati upravljanje znanjem zaposlenika o informacijskoj sigurnosti i kibernetičkim prijetnjama kroz elaboraciju standarda i normi, a u nastavku rada zadanu temu obraditi kroz istraživačka pitanja: "Je li informacijska sigurnost u korelaciji s kibernetičkim napadom? Kako znanje zaposlenika utječe na pozitivan smjer korelacije?". U drugom dijelu rada potrebno je (3) Opisati materijal i metodologiju istraživanja, potom deskriptivno i vizualno (4) Prikazati rezultate istraživanja primjenom SPSS alata, te u okviru diskusije (5) Elaborirati odgovore na istraživačka pitanja i postavljene hipoteze i (6) Sistematizirati zaključke do kojih se došlo, ocijeniti ostvarenje cilja istraživanja i predložiti korake za podizanje znanja o informacijskoj sigurnosti unutar poslovnih organizacija.

ZADATAK URUČEN 16.09.2022 | POTPIS MENTORA

SVEUČILIŠTE SJEVER

SAŽETAK

Informacijska sigurnost je najvažniji zadatak svake poslovne organizacije zbog velike količine podataka koje posjeduje, od svojih zaposlenika pa sve do krajnjih korisnika. Ovaj diplomski rad daje objašnjenje osnovnih pojmova kao što su informacija i informacijski sustavi, objašnjena je važnost informacijske sigurnosti, prezentirana je mogućnost kibernetičkog napada na poslovnu organizaciju te aspekti zaštite i sigurnosti od kibernetičkih napada. Kroz provedeno istraživanje daje se odgovor na postavljenu hipotezu: „Zaposlenici su upoznati s osnovnim aspektima informacijske sigurnosti unutar poslovne organizacije“. Istraživanje je provedeno korištenjem primarnih i sekundarnih izvora, a analizom rezultata donesen je zaključak kojim se predlaže unapređenje zaštite od potencijalnih kibernetičkih napada unutar poslovne organizacije. Kibernetički napad može oštetiti ili čak uništiti poslovnu organizaciju, ovisno o cilju i ozbiljnosti napada. Posljedice takvih napada najčešće su financijska šteta, negativna reputacija i smanjeno povjerenje korisnika u integritet poslovne organizacije.

Ključne riječi: informacija, informacijska sigurnost, kibernetički napad, poslovna organizacija

SUMMARY

Information security is the most important task of every organization due to the large amount of data that they own, from their employees to the end users. This master thesis explains the basic definitions of information and information systems, as well as the importance of information security, the possibility of cybernetic attacks, and protection of said attacks. Through the conducted research it will answer the hypothesis “How well do employees know the information security in their business organization?”. After conducting the analysis of the research with primary and secondary sources, a conclusion has been reached, and a recommendation for enhancing the protection of cybernetic attacks in the organization. A Cyberattack, depending on his goal and severity can damage or even destroy an organization. The accumulated damage of this attacks is most commonly financial, but also in a reduced reputation and confidence of users.

Key words: information, information security, cyberattack, business organization

Popis korištenih kratica

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

COBIT - Control Objectives for Information and Related Technologies (standard kontrole za korporativno upravljanje informacijama i pripadajućim informacijskim procesima)

DNS – Domain Name System (domenski sustav imena)

DOS - Denial of service (odbijanje usluge)

DDOS - Distributed denial of service (distribuirano odbijanje usluge)

GDPR - General Data Protection Regulation (opća uredba o zaštiti podataka)

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

IEC - International Electrotechnical Commission (međunarodno elektroničko povjerenstvo)

ISM - Information Security Management (upravljanje sigurnošću informacija)

ISMS - Information Security Management System (sustav za upravljanje informacijskom sigurnošću)

ISO - International Organization for Standardization (međunarodna organizacija za normizaciju)

ITIL - Information Technology Infrastructure Library (knjižnica infrastrukture informacijske tehnologije)

WLA - World Lottery Association (svjetska lutrijska udruga)

WLA SCS - WLA Security Control Standard (WLA standard sigurnosne kontrole)

WLA SRMC - WLA Security and Risk Management Committee (WLA odbor za sigurnost i menadžment rizika)

SADRŽAJ

1. Uvod

U današnje vrijeme poslovne organizacije se sve više susreću s prijetnjama prilikom kibernetičkih napada, kako u svijetu tako i u Hrvatskoj, jer privatne i državne organizacije posjeduju velike količine povjerljivih informacija od zaposlenika i korisnika. Te informacije je potrebno adekvatno zaštititi kako bi se sačuvala njihova povjerljivost tako da se prepoznaje važnost ulaganja u informacijsku sigurnost. Informacija se danas smatra resursom te gubitkom povjerljivosti neke informacije to ima štetno djelovanje na samo poduzeće. Glavni cilj ovog rada je pokazati čvrstu vezu između poslovanja organizacije, zaposlenika i informacijske sigurnosti.

1.1. Predmet i cilj rada

Predmet rada je detektiranje uloge informacijske sigurnosti ili detektiranje značaja informacijske sigurnosti za poslovanje sagledane kroz prizmu percepcije zaposlenika. Cilj ovog rada je ukazati na važnost informacijske sigurnosti i zaštite poslovanja od kibernetičkog napada kao faktora stabilnosti poslovanja u digitalnom okruženju.

1.2. Izvori podataka i metode prikupljanja

Pri izradi diplomskog rada korištena je znanstvena i stručna literatura iz područja informacijske sigurnosti. Pri obradi teme su korišteni sekundarni podaci sa službenih internet stranica na kojima su objavljeni tekstovi i radovi koji se odnose na tematsko područje ovog diplomskog rada.

Za potrebe pisanja diplomskog rada provedeno je istraživanje pomoću anketnog upitnika. Rezultati dobiveni provedbom ankete analizirani su metodom deskriptivne statistike i na osnovu njih je izveden zaključak. Istraživanje je provedeno na uzorku zaposlenika odabrane poslovne organizacije pomoću online platforme „*Survey monkey*“ prema svim zaposlenicima.

1.3. Predmet i cilj istraživanja

Predmet istraživanja ovoga rada bile su metode rada, ISO standardi i norme, procedure koje se koriste u poslovnoj organizaciji, upute vezane za informacijsku sigurnost te razina znanja zaposlenika u poslovnoj organizaciji.

Cilj istraživanja bio je pokazati znanje i svjesnost zaposlenika o informacijskoj sigurnosti u poslovnoj organizaciji te njihova potreba za konstantnim edukacijama kako bi u svakom trenutku bili upoznati sa mogućim kibernetičkim napadima i zaštitama od istih.

1.4. Istraživačko pitanje i hipoteze rada

Iz predmeta i cilja istraživanja izvedeno je istraživačko pitanje i postavljene su hipoteze:

Istraživačko pitanje: Utječe li znanje zaposlenika o informacijskoj sigurnosti na razinu zaštite informacijskih sustava unutar poslovne organizacije?

H1: Zaposlenici su upoznati s osnovnim aspektima informacijske sigurnosti unutar poslovne organizacije.

H2: Stupanj obrazovanja zaposlenika utječe na razinu zaštite informacijskih sustava unutar poslovne organizacije.

1.5. Struktura rada

Ovaj diplomski rad podijeljen je u šest cjelina (poglavlja).

U prvom poglavlju objašnjeni su predmet i cilj rada, izvori podataka te istraživačko pitanje i hipoteza.

U drugom poglavlju objašnjeni su pojmovi vezani uz informacije, informacijske sustave i informacijsku sigurnost te se navode primjeri i vrste kibernetičkih napada.

U trećem poglavlju navedeni su i opisani modaliteti zaštite od mogućih kibernetičkih napada te norme/standardi iz serije ISO 27000 koje predstavljaju kvalitetan odgovor na potencijalne ugroze sigurnosti informacijskih sustava unutar bilo koje organizacije.

U četvrtom poglavlju, Provođenje internog audita, na primjeru poslovne organizacije objašnjen princip izvođenja internog audita, od pripreme, provođenja do završetka.

U petom poglavlju se iznose rezultati dobiveni kroz empirijsko istraživanje provedeno na temelju prethodno postavljene hipoteze.

U šestom poglavlju autor iznosi svoj zaključak na temu rada, koji se temelji na navedenim teorijama i samostalno provedenom istraživanju, tj. dobivenim rezultatima.

Nakon zaključka rada slijede: literatura, popis slika, tablica, mjerni instrumenti istraživanja i anketni prilog.

2. Informacijska sigurnost

Postoji dobar razlog zašto poslovne organizacije diljem svijeta daju mnogo pažnje za sigurnost informacijskih sustava, sigurnosne prijetnje dolaze iz više izvora poput špijunaže, prirodnih nepogoda, sabotaža i računalnog kriminala. Financijski pokazatelji upućuju na to da je šteta nanesena od strane računalnog kriminala sve veća što pa je bitno planirati, projektirati, definirati, implementirati, održavati i kontinuirano unaprjeđivati informacijsku sigurnost.

Ovo su područja informacijske sigurnosti u kojima se propisuju posebne mjere i standardi:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost informacijskog sustava,
- sigurnost podataka,
- sigurnost poslovne suradnje.

Zakon o informacijskoj sigurnosti, I. Osnovne odredbe, Članak 2. navodi:

Informacijska sigurnost je stanje cjelovitosti, povjerljivosti i raspoloživosti podataka, informacijska sigurnost se postiže organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda te njihovom primjenom. (Narodne novine, NN 79/07).

Informacijska sigurnost je osim zakona definirana i ISO 27001 standardom:

Informacijska sigurnost podrazumijeva očuvanje dostupnosti, integriteta i povjerljivosti informacije; mogu se uključiti i druga obilježja kao što su pouzdanost, odgovornost, vjerodostojnost i neporecivost. (Kostanjevec, 2014:2).

Informacijska sigurnost postaje sve važnija u modernom društvu. Moderni državni i gospodarski subjekti ovise o računalnoj i komunikacijskoj infrastrukturi. To omogućuje protok velike količine informacija među subjektima, ali ujedno izlaže informacije i njima pripadne informacijske sustave brojnim prijetnjama. Pod pojmom informacijske sigurnosti podrazumijeva se zaštita informacija od prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija. Informacijska sigurnost se postiže primjenom odgovarajućih kontrola, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkcije sklopovske i programske opreme. Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, pregledavati i poboljšavati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahtjeva organizacije. Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te radi sprječavanja gubitaka cjelovitosti ili raspoloživosti samih sustava. Sigurnosne mjere uključuju mehanizme i procedure koje trebaju biti implementirane u svrhu odvraćanja, prevencije, detektiranja i oporavka od utjecaja incidenata koji djeluju na povjerljivost, cjelovitost i raspoloživost podataka i pratećih sustavnih servisa i resursa, uključujući i izvještavanje o sigurnosnim incidentima. Definiranje, implementacija, održavanje i poboljšavanje informacijske sigurnosti može biti od presudne važnosti kako bi se ostvarila i zadržala konkurentnost, osigurao dotok novca i profitabilnost, kako bi se zadovoljile zakonske norme i osigurao poslovni ugled. Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, špijunaže, sabotaže, vandalizma, požara, poplave i sl. Šteta nanesena organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge je sve prisutnija pojava. Informacijska sigurnost je jednako važna javnim i privatnim organizacijama. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Upravljanje informacijskom sigurnošću zahtjeva sudjelovanje svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan granica organizacije. (http://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost pristupljeno 18.06.2022.)

2.1. Informacija

Informacija je resurs za rukovođenje, poput kapitala i rada, te predstavlja jednu od najznačajnijih upotreba informacijske tehnologije kao konkurentskog oružja. Kao resurs ima specifična obilježja jer za razliku od materije i energije ne troši se korištenjem, niti smanjuje raspodjelom. Ona se danas nalazi u središtu poslovanja i predstavlja njen centralni faktor. Dominacija informacijske funkcije ukazuje s jedne strane na potrebu informatizacije poslovanja unutar poslovnog sustava, a s druge strane na efikasno povezivanje s izvorima informacija iz njene okoline što tom okruženju osigurava uspješno poslovanje i izglednu budućnost. Jedino oni poslovni sustavi koji polažu dovoljno pažnje razvoju informacijskog sustava mogu se nositi sa složenim uvjetima svjetskog tržišta i konkurencije. (Luić, 2009:36)

2.2. Informacijski sustav

Informacijski sustav je skup dobro definiranih pravila, običaja i postupaka pomoću kojih ljudi, oprema ili jedno i drugo, rade na određenom inputu sa svrhom da dobiju informacije koje će zadovoljiti potrebe određenih pojedinaca u određenoj poslovnoj situaciji. (Šehanović et al., 2002:50)

Informacijski sustav poslovnog sustava izuzetno je značajan za njegovu opstojnost i poslovanje, stoga je njegovo strateško planiranje jednako važno koliko i strateško planiranje poslovnog sustava. Koji je u osnovi, temeljni cilj informacijskog sustava? Cilj je informacijskog sustava dostaviti pravu informaciju na pravo mjesto, u pravo vrijeme i uz minimalne troškove. Ali kako taj cilj ostvariti u praksi? Zasigurno ne tako lako. Osnovne zadaće informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje informacija na sve razine objektnog sustava, odnosno korisnicima. (Luić, 2009:36)

Informacijski sustavi izloženi su raznim vrstama prijetnji. Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti materijalna ili nematerijalna šteta te za poduzeće može značiti dugoročni oporavak. Informacijska obrana je mehanizam računalne mreže koji uključuje odgovore i zaštitu infrastrukture te osiguranje informacija za poslovne organizacije, državna tijela i druge poslovne mreže. Informacijska obrana usmjerena je na sprječavanje, otkrivanje i pružanje pravovremenih odgovora na napade ili prijetnje tako da nema promjene u infrastrukturi ili informaciji. (Galinec, Luić, 2020:495)

2.3. Razvoj informacijske sigurnosti

Informacijska sigurnost znači provođenje relevantnih mjera za zaštitu informacija pokrivenih informacijskim sustavima od preuzimanja bez dozvole, korištenja, uređivanja i štete. Nevezano uz činjenicu nalaze li se informacije na papiru ili u elektronskom obliku, potrebno ih je u svakom trenu zaštiti od strane osoba koje rukuju s tim informacijama. Razvojem digitalnih kanala komunikacije, problem sigurnog čuvanja, zaštite i korištenja informacija postao je učestala pojava za svakoga tko ima pristup informacijskim sustavima. Tranzicijom u informacijsko društvo i digitalizacijom svih procesa, informacijska sigurnost je dobila na većoj važnosti nego što je ranije imala.

Kako bi se što bolje shvatio koncept informacijske sigurnosti, prvo je potrebno razumjeti pojam informacija koje su osnova informacijskih i komunikacijskih tehnologija. Pa se tako pojam informacija može objasniti kao strukturirani i međusobno povezani podaci. Kako bi se mogli koristiti, podaci se moraju pretvoriti u informacije. Podaci sadržani u informacijskom sustavu mogu se onda prenijeti korisniku u obliku poruke.

Pojam sigurnosti u kojem su uključena računala, mreže, državne i korporativne označava cijeli koncept za informacijsku sigurnost te u širokom smislu pokriva informacijske sustave. Informacijski sustav na korporativnoj razini uključuje i software, korisnike kao treću stranu, te sustave tehničke podrške. Informacijska sigurnost garantira sigurno spremanje i procesiranje podataka bez da ih se izmijeni ili iskvari, te sprječava neovlašten pristup tim podacima u digitalnom okruženju. Kako bi se to garantiralo potrebno je definirati i postaviti relevantna sigurnosna pravila. Informacijski sustav je taktički, upravljajući i podržavajući sustav postavljen između korisnika i informacijskih tehnologija u dvosmjernoj interakciji. U tom smislu, informacijski sustav se ne može smatrati samo kao problem informacijskih i komunikacijskih tehnologija, već i kao način na koji se osobe odnose prema tehnologijama koje podržavaju i olakšavaju njihov način rada i njihove radne zadatke.

Svaka država ima svoj koncept informacijske infrastrukture unutar svojih zahtjeva i potreba. Uzimajući u obzir uobičajene zajedničke značajke, moguće je napraviti pregled mreža, sustav i struktura koje mogu imati negativni utjecaj na kontinuitet javnog reda ili na izvedbu javnih službi u slučaju da ne provode svoje uloge djelomično ili u potpunosti.

Održivost informacijskih infrastruktura i prilagodljivost na potrebe zajednice su od velike važnosti. Vanjski faktori poput pada električnih sustava u Americi 2003. godine ili nuklearno

curenje zbog Tsunamija u Japanu samo su neki od dokaza koliku važnost ima sigurnost infrastrukture u informacijskoj sigurnosti.

Svrha informacijske sigurnosti je pružati kontinuiranu, sigurnu i kvalitativnu uslugu prilikom implementacije aktivnosti informacijskih sustava. Održavanje profesionalnog imidža, zaštita podataka i sprječavanje neovlaštenog pristupa su također ključni ciljevi i prioriteti informacijske sigurnosti. Glavni problem na koji informacijska sigurnost cilja je sprječavanje svih napada na povjerljivost, integritet i korištenje informacijskih sustava, te eliminaciju svih slabosti koje bi te prijetnje mogle iskoristiti. Slijedom navedenog može se zaključiti kako je visoku razinu informacijske sigurnosti lako ostvariti, no zapravo je riječ o velikom izazovu uslijed sve učestalijih i jačih kibernetičkih napada. Poznavanje široke palete rizika i prijetnji koje postoje za informacijske sustave ključno je u postizanju visoke razine zaštite. Postoje brojne regulacije, smjernice i alati za održavanje informacijske sigurnosti. Među njima sljedeći se mogu smatrati najbitnijima: mrežna i računalna sigurnost, sustavi za menadžment informacijske sigurnosti, menadžment informacijske sigurnosti, kibernetička sigurnost, kriptologija, kibernetički zločini, zaštita i povjerljivost podataka, nacionalna sigurnost i međunarodni odnosi.

Kao rezultat primjene informacijske sigurnosti na računala i mreže, pojavio se koncept računalne i mrežne sigurnosti. Računalna i mrežna sigurnost je niz aktivnosti usmjerenih ka sprječavanju neovlaštenog pristupa mrežnoj opremi i programima koji povezuju računala, te modificiranju i brisanju sistemskih podataka. Računalna sigurnost je način kako osigurati podatke i pružiti siguran pristup informacijama zaštićenim u informacijskim sustavima u slučaju vanjskih faktora poput prirodnih katastrofa. Mrežna sigurnost se tehnički razlikuje od računalne sigurnosti. Računalna sigurnost štiti računalni informacijski sustav od prijetnji i napada, dok mrežna sigurnost štiti mrežu koju koristi više međusobno povezanih računala od potencijalnih napada. Mrežna sigurnost implementira otkrivanje prijetnji mreži i mehanizme koje bi iste mogli spriječiti, dok s druge strane omogućuje konstantno i kontinuirano sigurno pristupanje mreži. Potreba za omogućavanjem sigurnosti mrežnih tehnologija imala je velik utjecaj na promjenu s koncepta nacionalne informacijske sigurnosti na koncept nacionalne kibernetičke sigurnosti u procesu razvoja Internet tehnologija koje se naširoko koriste u mreži.

Iako je pojam informacijske sigurnosti postao puno popularniji od kada su računala postala sastavni dio naših života, poznato je da su informacije oduvijek bile korištene kao sredstvo društvene i ekonomske vrijednosti, te se oduvijek pokušavalo spriječiti da im pristup dobe osobe kojima one nisu bile namijenjene. Otkriće i razvoj pisma pomoglo je u spremanju

informacija, te njihovom prijenosu na druge u trenutku kada to bude potrebno. Prema nekim povjesničarima, starije civilizacije imale su svoje određene sustave kako informacije zadržati u određenom krugu ljudi, pa su tako koristili vrlo komplicirane abecede, te samo pismo nije bilo nešto s čim su bile upoznate široke mase. Primjerice, egipatski hijeroglifi su prvi puta rastumačeni tek 1820. godine te su do tada informacije koje su zabilježene u njima, bile nepoznate. Također, u stara vremena, povjerljivost informacija između ljudi na visokim položajima čuvala se pomoću posebnih oznaka i pečata na pismima, te se pomoću njih jasno znalo ako su informacije pročitane od strane nekoga kome nisu bile namijenjene. Isto tako, korišteno je i slanje poruka u šifriranim kutijicama, čiju kombinaciju bi znali samo oni među kojima se informacije i dijele. Industrijska revolucija te izumi koji su doveli do korištenja električne energije, rezultirali su prijenosom informacija na velikim udaljenostima te se pojavila potreba za novijim i adekvatnijim mjerama zaštite informacija. U tom periodu najčešće korišteni komunikacijski uređaji bili telegraf i radio, a prvi uspješan pokušaj hakiranja informacija dogodio se kada je John Ambrose Fleming hakirao Marconijevu demonstraciju putem radio odašiljača, kako bi komunicirao bezobrazne poruke prema auditoriju. Jedan od povijesno najvažnijih trenutaka koji je doveo do zaokreta u informacijskoj sigurnosti, je hakiranje Enigma sustava za enkripciju, od strane Poljskih kriptologa Rejewskog, Zygalskog i Rozyckog, što je odigralo ključnu ulogu u pobjedi nad Njemačkom. Enigma sustav je imao iznimno kompliciran način enkripcije za taj vremenski period. Prihvaćeno je da je to hakiranje, koje je dovelo do revolucije na polju enkripcije podataka, promijenilo slijed Drugog svjetskog rata. Znanstvenici poput Alana Turinga, koji se smatra jednim od osnivača računalne znanosti, te Thomas Flowers, izumitelj jednog od prvih računala koje je bilo moguće programirati, Colossusa, su bili poznati matematičari koju su bili dijelom tima koji je radio na hakiranju njemačkih poruka tijekom rata.

Nakon što su ti događaji doveli do većih spoznaja o informacijskoj sigurnosti, počelo je i doba informacija s uvođenjem računala u ljudsku svakodnevnicu. U početku su to bili samo produkti enkripcijske tehnologije, te nisu bili korišteni kao u današnje doba za spremanje i razmjenu velikih količina podataka putem interneta. Informacijska sigurnost u tom periodu može se opisati kao radnje koje bi spriječile napade na državu, poput špijunaže, krađe podataka i sabotaže. Također, širenjem računala u vojnim bazama, pojavila se i potreba za zaštitom svih podataka koje se na njima nalaze i koji se putem njih razmjenjuju te se informacijska sigurnost počela razvijati i u tom smjeru. Godine 1968. kreiran je prvi prototip interneta, nazvan ARPANET, kao proizvod američke vojske u svrhu slanja zaštićenih informacija. U početku se

smatralo vrlo sigurnim načinom komunikacije, no s vremenom su se pojavili problemi, a s njima i rješenja kako da se ti problemi uklone. U izvještaju, koji je nazvan „RAND report R-609-1“ detaljno je i po prvi put objašnjeno kako su svi informacijski sustavi sigurni kada djeluju sami za sebe, no kada se međusobno povezuju s drugim sustavima, mogu nastati određeni sigurnosni rizici. U 1990. godini, Tim Berners Lee implementirao je prvi *world wide web* (WWW) uz pomoć tima znanstvenika iz CERN-a. Taj projekt je omogućio osobnim računalima i informacijski sustavima diljem svijeta da međusobno kontaktiraju i ukratko, dovrše ono što danas nazivamo internetom. Komercijalizacijom i civilnim korištenjem interneta globalna razmjena informacija zakoračila je u novo doba. Širenjem korištenja interneta u 1990. godini opasnosti i rizici prilikom širenja informacija pojavile su se i na internetu. U istom periodu mnoge organizacije su primijetile koristi interneta te su ušle u borbu za dio tog novog tržišta. Popratni efekt tog tržišnog nadmetanja je u razvoju novih informacijskih tehnologija i sustava koji bi ih zaštitili i omogućili neometano poslovanje i razmjenu informacija putem novih kanala.

(https://www.zurnalai.vu.lt/open-series/article/view/22387/21645 pristupljeno 18.06.2022.)

2.4. Vrste kibernetičkih napada

Kibernetički napad, ovisno o svom cilju i ozbiljnosti može oštetiti ili čak uništiti tvrtku. Više od pola malih poslovnih organizacija koja su bila pod kibernetičkim napadima su prestala poslovati idućih šest mjeseci od napada. Osim financijske štete koje ovisno o veličini poduzeća budu poprilične, poduzeća izgube reputaciju te počinju gubiti svoje korisnike. Kako bi se poslovna organizacija zaštitila od potencijalnih napada potrebno je razviti sigurnosne mjere koje se poduzimaju za sprječavanje napada, kao i mjere za uklanjanje i ublažavanje nastale štete u slučaju da dođe do napada. Prema tome, informacijska sigurnost u današnje vrijeme predstavlja jedan od najvažnijih elemenata u poslovanju. Kako bi se razvila efikasna zaštita protiv napada, sigurnosni tim tvrtke mora znati koji su potencijalni ciljevi napadača kao i mete njihova napada. Informacije o razvoju proizvoda, listama dobavljača, podaci o potrošačima, financijski zapisi o prihodima, dobicima i porezima te velik broj ostalih informacija mogu biti štetne za poslovnu organizaciju ako dođu u krive ruke. Ponekad je cilj napada enkriptirati važne podatke sve dok poslovna organizacija ne plati određenu svotu novca. Bilo koja vrsta napada može imati ozbiljne posljedice koje uključuju i pad vrijednosti dionica na tržištu pa čak i tužbe od strane nezadovoljnih ili zabrinutih potrošača ili poslovnih partnera. Kako bi se tvrtka zaštitila

od svih navedenih (i nenavedenih) rizika, bitno ih je predvidjeti i razumjeti, kao i poznavati tehnologije korištene za napade i obranu od istih.

Zbog rasta broja i vrsti kibernetičkih prijetnji i napada, kibernetička odnosno računalna sigurnost postala je vrlo bitno pitanje u poslovanju poduzeća. Najnoviji trendovi i statistike kibernetičkih napada prikazuju velik porast napadnutih računalnih sustava i podatkovnih proboja putem uređaja koji su sve češći na radnim mjestima, poput mobilnih uređaja i interneta stvari (engl. Internet of Things - IOT). Uz to, nedavna sigurnosna istraživanja sugeriraju i da većina poduzeća ima nezaštićene podatke te čak i lošu praksu računalne sigurnosti, što ih čini ranjivima na potencijalne napade koji bi mogli rezultirati gubitkom podataka (https://www.idtheftcenter.org/post/what-the-new-2019-data-breach-report-means-for-your-identity/, pristupljeno 20.08.2022.). Kako bi se poduzeća uspješno borila protiv zlonamjernih kibernetičkih napada ili još bolje spriječila ih, nužno je imati svijest o računalnoj sigurnosti, prevenciji potencijalnih napada i najbitnije od svega, poznavati što točno podrazumijevaju pojmovi računalna sigurnost i kibernetički kriminal. Informatička sigurnost više nije dovoljna, postoji potreba za strategiju obrane, prevenciju i odgovoru. Ideja o otpornosti, u svom najosnovnijem obliku, je samo procjena onoga što se događalo prije, tijekom i nakon što digitalno umreženi sustav naiđe na prijetnju. Otpornost ne smije biti sinonim za oporavak te ju je potrebno uključiti u sveukupnu poslovnu ili organizacijsku strategiju zbog nemogućnosti rutinskog plana provedbe već dugoročnog povećanja. Informatička sigurnost ne napreduje dovoljno brzo tako je potrebno ozbiljno uzeti u obzir kibernetičku otpornost. Kada poslovne organizacije prihvate da će se u svoje vrijeme susresti sa kibernetičkim napadom mogu prijeći na sljedeći korak a to je implementacija kibernetičke otpornosti. (Galinec, Luić, 2019:110)

Za potrebe organiziranja napada većeg obujma, razlog za napad na računalne sustave može biti i uključivanje računala u DDoS napad (engl. Distributed Denial of Service - DDoS) (Khanse, 2020). Kibernetički kriminalci ponekad provode pomno isplanirane napade kako bi na velik broj računalnih sustava uspjeli podmetnuti zlonamjeran program koji će to računalo dodati u mrežu daljinski kontroliranih uređaja (engl. Botnet), u svrhu pokretanja kasnijih distribuiranih napada uskraćivanjem usluge. Primjerice, jedan veći distribuirani napad uskraćivanjem usluge usmjeren je na tvrtku Dyn, jednog od većih pružatelja DNS usluga (engl. Domain Name System), tijekom listopada 2016. godine, posljedično stvorivši smetnje na mnogim većim mrežnim stranicama, uključujući Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit i GitHub (Cloudflare). To je učinjeno pomoću zlonamjernog programa zvanog Mirai, koji služi za stvaranje mreža daljinski kontroliranih uređaja (engl. botnet) koristeći

internet stvari IOT (engl. Internet of Things), uređajima kao što su kamere, pametni televizori, radio, čak i monitori za bebe.

Zlonamjerni program (engl. malware, koji je skraćenica izraza engl. malicious software) opširni je pojam koji opisuje bilo koji zlonamjerni program ili kôd koji je štetan za računalne sustave, namjerno dizajniran kao nametljiv i neprijateljski nastrojen program kojem je cilj napasti, oštetiti ili onemogućiti normalan rad računala, računalnih sustava, računalnih mreža, tableta i mobilnih uređaja, primjerice preuzimanjem djelomične kontrole nad radom uređaja. Nadalje, postoje brojne različite kategorije zlonamjernih programa, uključujući crve, trojanske programe, špijunski softver i hvatače unosa podataka, a sve veći broj vrsta zlonamjernih programa može koristiti kombinaciju različitih tehnika zaraze i napada. Iako zlonamjerni programi najčešće ne mogu fizički oštetiti sustav ili mrežnu opremu, oni mogu krasti, šifrirati ili izbrisati podatke, izmijeniti ili otimati osnovne funkcije računala i špijunirati aktivnost računala bez korisnikovog znanja ili dopuštenja. (https://www.malwarebytes.com/malware pristupljeno 20.06.2022.)

Ucjenjivački zlonamjerni programi (engl. ransomware) su zlonamjerni programi koji korisnicima priječe pristup njihovom vlastitom računalnom sustavu ili osobnim datotekama ili programima te zauzvrat zahtijevaju plaćanje otkupnine u zamjenu za vraćanje pristupa zaključanim datotekama ili računalnom sustavu. (https://www.malwarebytes.com/ransomware pristupljeno 20.06.2022.)

Phishing je zločin zavaravanja ljudi kako bi ih se prijevarom uvjerilo u dijeljenje osjetljivih podataka poput lozinki, računa za elektroničku poštu, brojeva kreditnih kartica, brojeva telefona, broj socijalnog osiguranja (engl. Social Security Number - SSN), kućnu adresu, žrtvino ime i prezime i druge osobne podatke (Porter, 2020). Naziv phishing potječe od engleskog prijevoda riječi "pecanje" (engl. Fishing, a slovo f zamijenjeno je sa ph kao odavanje počasti prijašnjoj metodi hakiranja javnih telefona za besplatne pozive zvano Phreaking), aludirajući na metodu pripreme i postavljanja zamke, odnosno "mamca" te se napadač oslanja na vjerojatnost da će bar jedna žrtva "zagristi" i povjerovati lažnoj poruci i tako nesvjesno odati svoje osjetljive podatke napadačima (Kay, 2004). Žrtve najčešće primaju zlonamjernu elektroničku (engl. Malspam, od riječi engl. Malicious) ili tekstualnu poruku (SMS) koja oponaša neku osobu, organizaciju ili tvrtku kojoj žrtva vjeruje, poput suradnika, banke ili vladinog ureda s ciljem prijevare korisnika ili širenja zlonamjernih programa. Porter (2020) za Norton navodi primjer *phishinga* slanjem elektroničkih poruka u kojem se napadač predstavlja kao korisnikova banka. Kada žrtva otvori tu elektroničku poštu ili tekst, pronalaze poruku

napisanu s namjerom da čitatelja zastraši, primjerice tvrdeći da će bankovni račun korisnika biti ugašen radi neaktivnosti osim ako ne unesu svoje podatke na mrežnoj stranici kojoj mogu pristupiti preko poveznice koja se nalazi u toj poruci. Korisnik će, u nedostatku bolje prosudbe, pratiti upute u dobivenoj poruci te kao rezultat nesvjesno unijeti svoje podatke na lažnu mrežnu stranicu koja je dizajnirana kako bi što uvjerljivije izgledala kao primjerice mrežna stranica korisnikove banke kako bi korisniku dala lažan osjećaj sigurnosti. Sadržaj zlonamjernih neželjenih poruka uvijek je osmišljen s namjerom zastrašivanja koje treba prevladati žrtvinu bolju prosudbu ispunjavajući je strahom. (Porter, 2020. https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html pristupljeno 20.06.2022.)

Još jedna moguća prijetnja za računalne sustave je *rootkit*. *Rootkit* se definira kao zbirka računalnog softvera, tipično zlonamjernog, dizajnirana da omogući pristup računalu ili dijelu njegovog softvera kojem pristup inače nije dopušten i često prikriva njegovo postojanje ili postojanje drugih programa. Drugim riječima, *rootkit* je skup programa ili koda koji omogućuje neotkrivenu prisutnost na računalu.

2.5. Primjeri napada

Jedan od najvećih slučaja kibernetičkog napada na poslovnu organizaciju da se izravno tiče Hrvatske zasigurno je onaj o velikom hakerskom napadu na naftnu kompaniju INA-u. Još uvijek nepoznat napadač je uspio *ransomware-om* inficirati veći broj računala unutar INA-e, pa se privremeno njihovo poslovanje, osim maloprodaje, odvijalo bez interneta.

INA Grupa je objavila da se nalazi pod kibernetičkim napadom koji je započeo 14. veljače oko 22 sata a uzrokovao je povremene poteškoće koje utječu na normalan rad, na primjer, izdavanja elektroničkih vinjeta, bonova za mobitele, plaćanja komunalnih računa zbog poteškoća u radu pojedinih informatičkih sistema

Neslužbeno se moglo čuti da su napadači tražili 1.500 bitcoina, odnosno u nekim verzijama pedeset ili stotinu milijuna kuna otkupnine. Iz INA-e nisu isključili mogućnost da su razne hakerske skupine pokušale "preuzeti odgovornost" za ovaj napad i da su na taj način financijsku korist pokušali izvući i oni koji s napadom nemaju veze, što je česta pojava u svijetu kibernetičkih napada.

21
VELJ

Obavijest o kibernetičkom napadu

Poštovani,

INA Grupa u procesu je otklanjanja poteškoća u informatičkim sustavima na koje je utjecao kibernetički napad koji se dogodio krajem prošlog tjedna. Započeli smo s oporavkom sustava te radimo na ponovnoj uspostavi svih usluga koje povremeno nisu radile.

Kao što je ranije napomenuto, kibernetički napad prijavljen je mjerodavnim institucijama s kojima INA u potpunosti surađuje. Napad i mogući neovlašteni pristup podacima se istražuje. Kao i kod svakog kibernetičkog napada, u ovom trenutku ne možemo isključiti mogućnost da je došlo i do neovlaštenog pristupa osobnim podacima.

Napominjemo kako je opskrba tržišta sigurna, a prodaja goriva na našim maloprodajnim mjestima se nastavlja odvijati neometano. Također, provedba svih plaćanja je sigurna, neovisno o tome radi li se o gotovinskom plaćanju, INA kartici ili bankovnoj kartici.

Ispričavamo se našim kupcima i poslovnim partnerima za eventualne neugodnosti koje je ova situacija mogla prouzročiti. Cijenimo vašu kontinuiranu podršku i razumijevanje u ovoj situaciji.

Slika 1. Obavijest o kibernetičkom napadu INA

Izvor : https://www.ina.hr/obavijest-o-kibernetickom-napadu/ pristupljeno 15.07.2022.

Osim INA-e, kibernetički napad u Hrvatskoj zadesio je i Petrokemiju koja je uočila pokušaje neovlaštenog pristupa dijelu elektroničke komunikacije društva.

Iako se još ne piše dovoljno o kibernetičkim napadima u Hrvatskoj i postoji jako malo detaljnih informacija, hakerski napadi na poslovne subjekte se sve češće događaju u Hrvatskoj pa su tako unazad dvije godine napadnuti bili Pevex, Telemach i Overseas Express. https://www.vecernji.hr/vijesti/hakeri-napali-kutinsku-petrokemiju-otezana-elektronicka-komunikacija-1524004 pristupljeno 15.07.2022.

3. Zaštita i standardi

Unutar poslovnih organizacija raznih veličina još se predmnijeva da je dovoljno samo razviti strategiju za kibernetičku sigurnost i da je njezino postojanje te provođenje ispravnih poslovnih i sigurnosnih politika cjelovit odgovor na obranu i zaštitu od kibernetičkog kriminala (Grimes, 2017). Međutim, stvarnost je takva da je najčešće potrebno mnogo više za postizanje snažne zaštite protiv kibernetičkih napada u današnjem ranjivom digitalnom okruženju. Neki se podatkovni proboji lako mogu izbjeći, ali se oni često uspješno infiltriraju u računalne sustave i mreže zbog nedostatka znanja o računalnoj sigurnosti unutar poduzeća. Da bi postigle optimalnu razinu kibernetičke sigurnosti, tvrtke moraju osigurati ispravnu poslovnu politiku o primjeni sigurnosnih postupaka prilikom rada s računalnim i mrežnim sustavima te obrade podataka (Johns, 2020). Unatoč tome što se u obranu računalnih sustava poduzeća od napada ulaže mnogo resursa velik broj poduzeća i organizacija ipak ne provodi adekvatnu procjenu rizika od kibernetičkih napada ili pak nepravilno usklađuje mjere obrane s obzirom na prijetnje koje bi potencijalno mogle predstavljati najveći rizik za računalne sustave i mreže tog poduzeća ili organizacije.

Rastući i konstantno mijenjajući broj sigurnosnih prijetnji na internetu dodatno otežava pravilno suočavanje s rizikom i prepoznavanje razine prijetnje koju one predstavljaju te to može dovesti do loših ili samo djelomičnih odnosno neučinkovitih primjena sigurnosnih pravila tijekom rada na računalnim sustavima i mrežama u tom poduzeću ili organizaciji. Bitno je biti svjestan činjenice da je računalne sustave danas lako napasti ako oni na sebi imaju neredovito ažurirane programe. Iako se najčešće radilo o neažuriranim operacijskim sustavima, u novije vrijeme kibernetički kriminalci pronalaze načine za iskorištavanje sigurnosnih propusta i u ostalim programima i aplikacijama koje se mogu instalirati na računalo ili neki uređaj, primjerice internetski preglednici (Grimes, 2017).

Poduzeće koje je svjesno svih rizika kojima bi moglo biti podložno tijekom mrežnog poslovanja mora se pobrinuti da isplanira sigurnosne standarde i educira svoje zaposlenike o sigurnosnim postupcima i općenito sigurnom ponašanju prilikom korištenja mrežnih servisa i interneta (Honigman, 2015). Važnost toga posebice je velika za poduzeća koja osim svojih poslovnih podataka na svojim mrežnim poslužiteljima pohranjuju i osjetljive podatke svojih korisnika jer bi u slučaju kibernetičkog napada mnogobrojne privatne informacije mogle biti ukradene i iskorištene u zlonamjerne svrhe. Ali bez obzira na tu činjenicu poduzeća različitih veličina, a

pogotovo mala poduzeća, česta su meta kibernetičkih napada radi loše implementiranih ili čak nepostojećih sigurnosnih politika za obranu od kibernetičkih napada (Honigman, 2015).

Kako bi se zaštitila od kibernetičkih napada različitih vrsta, poduzeća bi morala osigurati bar neke navedene osnovne mjere sigurnosti u svojem poslovanju. Popat navodi da je jedan od najosnovnijih načina zaštite osjetljivih poslovnih podataka provedba zaštite računalne opreme i računalnih sustava u poduzeću implementacijom kompleksnih lozinki koje će znati samo korisnici tog računala ili profila, a sve djelatnike poduzeća ili korisnike usluga savjetovati da radije upamte lozinku umjesto da je zapisuju na papir ili tekstualne datoteke na koje bi bilo tko mogao naići. Osim toga, zaposlenici bi trebali proći osnovnu edukaciju o sigurnom korištenju interneta i opasnostima koje potencijalno predstavljaju neželjene elektroničke pošte, kako bi se spriječio bilo koji budući pokušaj *phishinga* na kojeg bi zaposlenici mogli nasjesti. Također, instalacija programa za geolokacijski pronalazak izgubljenog uređaja korisna je za pronalazak uređaja, računala, laptopa ili mobitela u slučaju fizičke krađe. Nadalje, enkripcija važnih i osjetljivih podataka, uključujući i podatke korisnika mrežnih usluga poduzeća, može osigurati da ti podaci ne budu ugroženi čak i ako dođe do kibernetičkog napada na mrežne sustave ili usluge poduzeća. Stvaranje sigurnosnih kopija koje će se pohranjivati na drugim lokacijama pak može uvelike pomoći poduzeću u slučaju kibernetičkih napada koji su rezultirali gubitkom podataka ili u slučaju napada ucjenjivačkim programima (engl. Ransomware), kako bi poduzeće uvijek bilo korak ispred kibernetičkih kriminalaca. Poduzeća bi trebala za svaki slučaj osigurati podatke tako da se u slučaju proboja podataka financijska šteta može bar do neke mjere ublažiti. (Popat, 2018)

Djelatnici poduzeća ipak su samo ljudi, i kao takvi podložni su ljudskim greškama koje bi mogle dovesti poduzeće u rizik od kibernetičkih napada. Rješenje za ovaj problem nije otpuštanje djelatnika sa slabijim poznavanjem računalne sigurnosti, već edukacija djelatnika o sigurnom korištenju interneta i njegovih usluga.

3.1. Upravljanje znanjem

Fizičke metode zaštite jedna su od ključnih komponenti u cjelokupnoj zaštiti informacijskog sustava. Fizička sigurnost informacijskog sustava ugrožava se u slučajevima elementarnih nepogoda te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost.

Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj. Cilj fizičke sigurnosti je spriječiti neautorizirane pristupe računalnom sustavu, zaštititi integritet podataka koji se pohranjuju na računalo, spriječiti oštećenje ili gubitak podataka u slučaju raznih nepogoda te spriječiti krađu podataka s računalnih sustava.

U programske metode zaštite ulazi zaštita na razini operacijskog sustava koji je osnovni stupanj zaštite. On uključuje administratore sustava i korisnike tj. zaposlenike u organizaciji. Administrator sustava ima pristup svim povlaštenim informacijama te dodjeljuje razinu ovlasti pojedinim korisnicima. Administrator svakom korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi imao pristup relevantnim informacijama i kako bi obavljao svoje radne zadatke. Svako računalo može imati više administratora te više korisnika.

Same lozinke ujedno mogu biti i slaba točka zaštite sustava, ali zbog ljudskog faktora. Ovo su osnovne greške koje ljudi rade u vezi s lozinkama:

1. Koriste se jednostavne ili slabe lozinke;
2. Ista lozinka se korisni na više računa;
3. Lozinke se pohranjuju na računala;
4. Lozinke se zapisuju na papiriće;
5. Lozinke se dijele s drugim korisnicima.

Kako bi spriječili ove pogreške, a s time i pad sigurnosti informacijskog sustava, postoji nekoliko pravila za lozinke:

- maksimalni vijek trajanja lozinke;
- minimalna duljina lozinke;
- potreba kompleksnosti;
- pregled povijesti lozinki.

Maksimalni vijek trajanja lozinke određuje da se lozinka mora mijenjati nakon određenog vremena. Minimalna duljina zahtijeva da lozinka ne bude kraća od zadanog broja znakova. Potreba kompleksnosti zahtjeva da se koristi kombinacija malih i velikih slova, brojeva i posebnih znakova, dok pregled povijesti lozinki onemogućava da postavimo istu lozinku, nego

zahtjeva njenu izmjenu. Pridržavanjem ova četiri pravila osigurat će se sigurnost korisničkih podataka, a time i informacijskog sustava.

U provedenom istraživanju o vrsti lozinke koju mladi u današnje vrijeme koriste, analizom dobivenih odgovora vidljivo je kako više od 50% ispitanika koristi 10-znakovnu lozinku koja sadrži kombinaciju slova, brojeva i specijalnog znaka dok 12% koristi lozinku sa više od 10 znakova. Više od trećine ispitanika (32%) koristi jednostavne lozinke kao što su osobna imena iz obiteljskog okruženja, uzastopne jednoznamenkaste brojeve ili riječi, te lozinke ne pružaju dobru zaštitu od kibernetičkog napada. (Luić et al., 2021:529)

Sljedeći korak u zaštiti informacijskih sustava je zaštita korisničkih programa. Nakon što pomoću korisničkog imena i lozinke se uđe u sustav tj. radnu površinu, pokreće se program kojim se obavlja određena aktivnost u informacijskom sustavu. Korisnički programi se štite na način da se pojedinim korisnicima dodaju ovlasti te tako određuju funkcije koje mogu obavljati u programu.

Postoje tri razine ovlasti:

Prva razina-samo čitanje iz baze podataka;

Druga razina-izmjena postojećih podataka u bazi i dodavanje novih podataka;

Treća razina-brisanje podataka iz baze.

Kako bi se poslovna organizacija zaštitila od zlonamjernog korištenja ovlasti radnika postoji još jedan korak povećanja sigurnosti informacijskog sustava. Naime, svi podaci koji se mijenjaju ili brišu spremaju se u posebne direktorije u sustavu kojima pristup ima samo administrator. Tek kada on odluči da podaci nisu potrebni oni se trajno brišu iz sustava.

Kako poslovne organizacije danas nisu centralizirane nego su prostorno dislocirane javlja se potreba za umrežavanjem računala kako bi se informacije mogle svugdje koristiti. Komunikacija između lokacija se odvija preko interneta, a to donosi nove prijetnje. U ovom procesu mora se osigurati jednoznačnost prijenosa i onemogućiti neautorizirano korištenje ili promjena podataka. Kako bi se omogućila sigurna komunikacija i promet podacima koristi se kriptiranje podataka tj. kriptografija. (Dujella, Maretić, 2007)

Antivirusni program je softverski alat koji je dizajniran za zaštitu računala i računalne mreže od računalnih virusa. Antivirus pregledava dolazni podatkovni promet i skenira sadržaj. U slučaju da primijeti prisutnost virusa odmah reagira upozoravajući korisnika te čeka upute za

daljnje radnje. Nakon otkrivanja virusa korisnik može zaraženu datoteku izbrisati, prebaciti u karantenu ili ignorirati upozorenje.

Antivirusni program funkcionira tako da uspoređuje dijelove koda dolaznog prometa tj. podataka s kodovima svih poznatih virusa iz njegove baze podataka. Svaki virus ima specifičan dio koda koji se u bazi podataka virusa naziva potpis.

Osim praćenja dolaznog prometa antivirusni program provjerava i sve datoteke koje korisnik otvara. Iako se otvaranje datoteka čini trenutačno ono to nije. Prije otvaranja datoteke antivirusni program uspoređuje njen kod s potpisima virusa u bazi podataka. U slučaju da se dio koda poklopi s potpisom virusa izdaje upozorenje korisniku.

Osim običnih i izvršnih datoteka antivirusni program provjerava i komprimirane datoteke jer je virus možda pohranjen u njima te word dokumente za mikro viruse. Također antivirusni programi imaju funkciju heurističkog skeniranja, što znači da osim uspoređivanja potpisa s bazom potpisa virusa oni provjeravaju programe po ponašanju, jer ako se program čudno ponaša postoji mogućnost zaraze.

Antivirusni programi se ažuriraju na dnevnoj bazi pa je važno omogućiti ažuriranja na računalu kako bi ono bilo zaštićeno od najnovijih virusa. On je barijera između korisnikove sigurne privatne mreže i nesigurnih mreža poput interneta.

Zaštitni zid je mrežni sigurnosni sistem koji kontrolira dolazni i odlazni promet po određenim sigurnosnim pravilima. Prema tim pravilima odlučuje dali će dopustiti podatkovni promet ili ga blokirati. On može biti softverskog ili hardverskog tipa. Zaštitni zid sprječava neželjeni pristup korisnikovom računalu na način da identificira i sprječava komunikaciju preko riskantnih portova. Portovi su komunikacijski kanali po kojima računalo komunicira s vanjskim mrežama. Računala komuniciraju preko mnogo poznatih portova i zaštitni zid dopušta tu komunikaciju bez korisnikovog znanja. Npr. internet stranice se otvaraju preko porta 80. Drugim riječima zadaća zaštitnog zida je identifikacija i blokiranje prometa po nesigurnim komunikacijskim kanalima.

Osim otkrivanja sigurnih komunikacijskih kanala zaštitni zid može otkriti čudna ponašanja u dolaznom prometu. Napadači se znaju koristiti sigurnim kanalima kako bi skenirali ranjive portove na korisnikovom računalu. Taj proces ima svoj uzorak koji zaštitni zid prepoznaje i odmah blokira komunikaciju.

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu. Postoji nekoliko razina informacijske sigurnosti. To su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te *outsourcing*. Svima je cilj zaštita informacijskog sustava. (Šehanović, Hutinski, Žugaj, 2002:237)

3.1.1. Institucije informacijske sigurnosti u RH

Uz zakone za informacijsku sigurnost u RH postoje i institucije koje provode te zakone. Četiri glavne institucije na području informacijske sigurnosti su:

1. Nacionalni CERT https://www.cert.hr/
2. Ured vijeća za nacionalnu sigurnost https://www.uvns.hr/hr
3. Zavod za sigurnost informacijskih sustava https://www.zsis.hr/
4. Agencija za zaštitu osobnih podataka https://azop.hr/

Nacionalni CERT je osnovan 2009. godine u skladu sa Zakonom o nacionalnoj sigurnosti. Zadaća mu je obrada incidenata na internetu, ali samo ako se jedna od strana nalazi u Hrvatskoj.

Nacionalni CERT provodi proaktivne i reaktivne mjere u okviru svog djelovanja. Proaktivne mjere su one kojima Nacionalni CERT djeluje prije događanja incidenta u svrhu njegovog sprječavanja ili ublažavanja. To su:

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti;

- kontinuirano praćenje računalno-sigurnosnih tehnologija;

- javno objavljivanje novih informacija u svrhu edukacije najšire javnosti;

- provođenje detaljne edukativne obuke za specifične grupe korisnika.

Reaktivne mjere su one kojima se djeluje na incident. To su:

- izrada i distribucija sigurnosnih upozorenja na osnovu prikupljenih saznanja;

- prikupljanje, obrada i priprema sigurnosnih preporuka o slabostima u informacijskim sustavima;

- koordinacija rješavanja značajnijih incidenata u koje je uključena barem jedna strana iz Republike Hrvatske.

Valja napomenuti da Nacionalni CERT iako je nadležan za sigurnost i zaštitu od incidenata nije nadležan za kažnjavanje i pokretanje kaznenih prijava. Nakon otkrivanja incidenta prijavu podnosi nadležnim tijelima u RH. (http://www.cert.hr/onama pristupljeno 15.06.2022.).

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Zavod obuhvaća sigurnosnu akreditaciju informacijskih sustava, standarde sigurnosti informacijskih sustava, koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava te upravljanje kripto materijalima koji se koriste u razmjeni klasificiranih podataka

Dokument u kojem se nalaze savjeti za zaštitu osobnih uređaja od kibernetičkih napada su zajedno izradili zavod za sigurnost i ured vijeća za nacionalnu sigurnost te se on odnosi na postupanje s osobnim uređajima (pametni telefoni, satovi, računala i sl.) koji se povezuju s internetom, a cilj je smanjenje rizika od kibernetičkog napada, također je izrađena i nova verzija dokumenta „Nacionalna taksonomija računalno-sigurnosnih incidenata“.

Zavod za sigurnost informacijskih sustava zadužen je za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava, sudjelovanjem u nacionalnoj normizaciji područja sigurnosti informacijskih sustava te donošenjem pravilnika i njihovim trajnim usklađivanjem s međunarodnim standardima i preporukama. (https://www.zsis.hr/ pristupljeno 15.06.2022.).

3.2. Ulaganje u informacijsku sigurnost

Ulaganje u informacijsku tehnologiju predstavlja sve veći dio investicija tvrtki. U razvijenim zemljama iznos ulaganja u IT je značajan, pogotovo kada su u pitanju uslužne tvrtke, jer priroda njihovih proizvoda ili učinaka su usluge i informacije. IT kapitalna ulaganja su se od 1980. godine gotovo udvostručila te se očekuje i njihov daljnji rast. U takvom ozračju ubrzanog rasta važnosti IT, logično je da ona predstavlja temu koja je izuzetno prisutna u suvremenom poslovanju i pridavanje sve veće važnosti načinu ulaganja u informacijsku tehnologiju u tvrtkama i upravljanju njome. Ulaganja u IT uzimaju sve veći postotak u ukupnim ulaganjima tvrtki i svi se zapravo pitaju koliko su ona opravdana, a s druge strane, upotrebom suvremene IT tvrtke mogu steći određene konkurentne prednosti kojima mogu potpuno potisnuti i marginalizirati konkurenciju na tržištu. (Mueller, 2001:587-612)

Prema Mukhopadhyay et al. (2005), ulaganje u sigurnost ne jamči potpuno sprječavanje utjecaj kibernetičkih rizika, stoga je korisno dio kibernetičkih rizika prenijeti na društva za osiguranje. Upravo Gordon et al. (2003) optimalno upravljanje kibernetičkim rizicima opisuju kao ono koje kombinira ulaganje u sigurnost i prijenos rizika na društva za osiguranje. Međusobnu povezanost metode fizičke kontrole, koja obuhvaća ulaganje u sigurnost, i metode financijske kontrole, koja obuhvaća prijenos rizika na društva za osiguranje istražuju Lelarge i Bolot (2008). Kombiniraju teoriju rizika i mrežnog modeliranja s ciljem razvoja modela očekivane korisnosti koja proizlazi iz odluke o prijenosu rizika. Prijenos rizika na društvo za osiguranje ističe se kao prikladno sredstvo za apsorbiranje financijskih gubitaka uzrokovanih kibernetičkim incidentom, a prema Böhme (2005) tržište osiguranja je poticajni čimbenik izgradnje sigurnog okružja.

Istraživanja u području kibernetičke sigurnosti mogu se razdijeliti prema kriteriju korištene metodologije u cilju optimizacije ulaganja u kibernetičku sigurnost u dva segmenta: Prvi segment pristupa analizi odluke o ulaganju u kibernetičku sigurnost temeljem teorije očekivane koristi što je tradicionalno prihvaćen model procjene ulaganja u kibernetičku sigurnost. Međutim, sigurnost poslovne organizacije ne ovisi samo o usvojenim mjerama i praksama sigurnosti, nego i o odlukama ulaganja drugih povezanih poslovnih organizacija. Stoga je sugestija da modeli ulaganja u sigurnost trebaju obuhvatiti stratešku interakciju između povezanih poslovnih organizacija, a upravo je teorija igara prikladna za modeliranje interakcija između poslovnih subjekata. Teorija igara je usmjerena na definiranje odluke o optimizaciji

ulaganju uvažavajući akcije i reakcije poslovnih organizacija koje pokušavaju zaštiti svoju informacijsku imovinu i napadača koji namjeravaju narušiti pretpostavke kibernetičke sigurnosti. Teorija igara korisna je u smislu razmatranju ishoda i koristi donesene odluke u području kibernetičke sigurnost s obzirom na djelovanje (odluke) svih prisutnih aktera. Nadalje, korisna je u mogućnosti postavljanja specifičnih obilježja prisutnih aktera što ostavlja prostor za nastavak primjene teorije igara u optimiziranju odluka o ulaganju. Slijedom navedenog za buduća istraživanja predložen je razvoj modela optimalnog ulaganja u kibernetičku sigurnost od strane Kovača koji pretpostavlja međusobnu povezanost više poslovnih organizacija, razmjenu informacija između napadača na informacijske sustave te definiranje poticajnih mehanizama kojima bi bilo moguće potaknuti poslovne organizacije na zajedničku odluku o koordiniranom ulaganju u sigurnost i razmjenu sigurnosnih podataka.

Upravljanje rizikom postaje presudan zadatak čijim se izvršenjem umanjuje negativan utjecaj rizika, realizacija kojih predstavlja opterećenje u odvijanju poslovnih procesa te ugrozu za poslovanje. Prevencija velikih gubitaka, koji se mogu dogoditi zbog kibernetičkog napada ili kvarova unutar informacijskog sustava, obično je povezana s kontinuiranim ulaganjem u različite sigurnosne mjere. Ulaganje u kibernetičku sigurnost iziskuje angažman resursa, koji je s ekonomskog gledišta nužno optimizirati. Međutim, bez obzira koliko iscrpan angažman resursa pretpostavili, u razvoj kibernetičke sigurnosti, apsolutnu sigurnost nije moguće postići. Stoga, metodu fizičke kontrole treba kombinirati s metodom financijske kontrole koja uključuje odluku o prijenosu rizika na društva za osiguranje. Kombiniranje navedenih metoda pruža rješenje u postizanju cilja, a riječ je o postignutoj kibernetičkoj sigurnosti. (Kovač, 2021:69-70)

3.3. ISO norme

Međunarodna organizacija za standardizaciju (ISO) nastala je kao savez nacionalnih organizacija za normizaciju a glavni zadatak je priprema normi, prihvaćanje, objavljivanje i briga o međunarodnim normama. Mrežu nacionalnih organizacija u sustavu ISO organizacije, po zadnjim podacima, čine članice 163 zemlje. Sa sjedištem u Ženevi kao nevladina organizacija, iz kojeg koordinira rad cjelokupnog sustava, organizacija predstavlja most između privatnog i javnog sektora te svojom ulogom ostvaruje konsenzus uslijed rješavanja problema u funkciji zadovoljstva svih zainteresiranih strana i društva u cjelini. ISO vodi brigu o međunarodnim standardima i normama iz svih područja tehnologije, tehnike i znanosti osim elektrotehnike i elektronike. Od 23.02.1947. godine od kad je službeno počela s radom,

međunarodna organizacija za standardizaciju (ISO) implementirala je i objavila više od 18.500 međunarodnih standarda i normi u različitim područjima i na različitim osnovama (komercijalne i industrijske). Svakako treba napomenuti da organizacija godišnje objavi otprilike 1.100 normi. Rad i upravljanje ISO organizacijom temelji se na strateškim planovima koji se donose svakih pet godina usvajanjem od strane punopravnih članica. (https://www.iso.org/home.html pristupljeno 10.06.2022.)

Druga međunarodna organizacija važna za sustav normizacije je Međunarodna elektrotehnička komisija (IEC), osnovana 26.06.1906. godine kao neprofitna, nevladina organizacija koja priprema i objavljuje međunarodne norme vezane uz područje električnih, elektronskih i ostalih tehnologija koje su u međusobnoj vezi (uključujući energetiku, elektroenergetiku, elektroakustiku…). Kroz svoje norme IEC je prva promovirala SI sustav jedinica (International System of Units). Osnovno cilj poslovanja IEC je razvoj međunarodne suradnje u svim pitanjima normizacije i pitanjima iz područja elektrotehnike u vezi s normizacijom i time poboljšanje međunarodnog razumijevanja tog područja. (Andrijanić et al., 2012.)

Norme iz serije ISO 27000 izrađene su tako da svaka od normi daje naglasak na nešto.

- ISO 27001 služi za postavljanje temelja informacijske sigurnosti i određivanje njezinih okvira

- ISO 27002 služi za implementaciju sigurnosnih mjera, sadrži najbolje prakse u uvođenju norme

- ISO 27003 pruža upute za implementaciju kao pomoć osobama koje implementiraju ISO 27000 standarde. U osnovi se bazira na smjernicama iz ISO 27001 standarda, te pruža vodstvo sve do pokretanja ISMS projekta

- ISO 27004 služi da pomogne organizacijama mjeriti, izvještavati i na temelju istoga sistematski poboljšavati kvalitetu ISMS (engl. Information Security Management System)

- ISO 27005 služi za provedbu procjene rizika

- ISO 27006 je akreditacijski standard koji vodi certificiranje kroz formalni proces certifikacije ISMS organizacija prema ISO 27001 standardu. U istome su navedene sve potrebe i upute kako izvesti certifikaciju i koje uvjete organizacija mora zadovoljiti. (Kostanjevec et al., 2014:28)

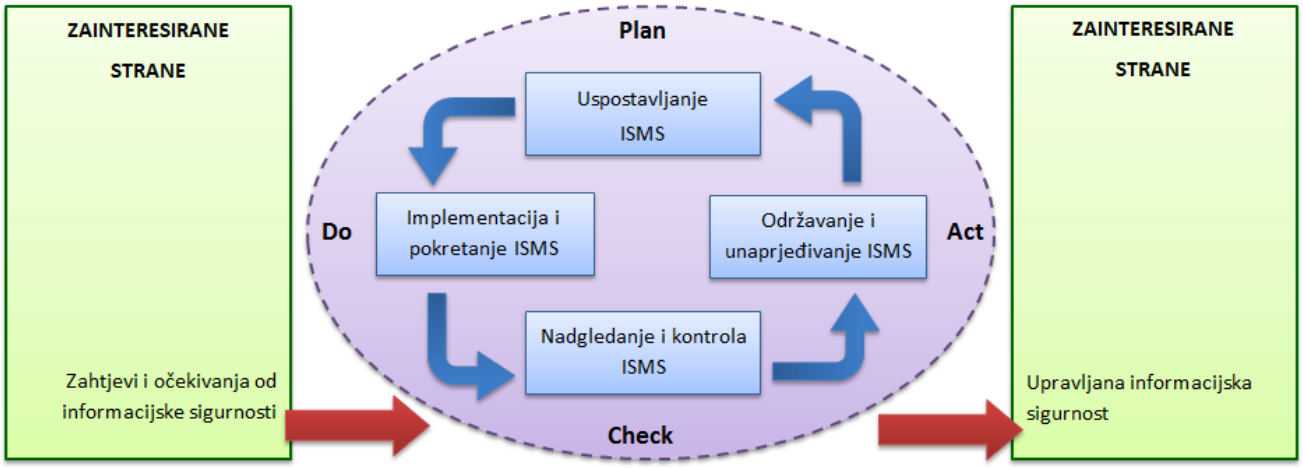
3.3.1. ISO/IEC 27001

Prije nastajanja ISO normi, postojala je BS 7799 norma (nastala pod okriljem British Standard Institute-BSI). Prvi put je izišla kao kodeks dobre prakse 1995. godine. Podijeljena je na dva dijela 1999. godine na BS 7799-1 i BS 7799-2. Nekoliko godina kasnije, normu BS 7799-1 preuzima ISO (Međunarodna organizacija za standardizaciju) i izdaje ju pod imenom ISO/IEC 17799. Kasnije je norma BS 7799-2 izdana kao ISO/IEC 27001:2005 u kojoj su opisani pojedini elementi sustava upravljanja sigurnošću informacija. Norma je napisana u obliku zahtjeva, koje sustav treba ispunjavati, a omogućava ocjenjivanje bilo interno ili vanjsko, od neovisne certifikacijske institucije.

ISO 27001 usvaja procesni pristup za: uspostavljanje, implementaciju, rad, nadziranje, provjeru, održavanje i unaprjeđivanje organizacijskog ISMS-a.

ISMS (eng. Information Security Management Systems) je sustav upravljanja informacijskom sigurnošću. Prema ISO 27001 normi, pruža sustavan pristup upravljanju osjetljivim informacijama kako bi ih zaštitio i obuhvaća sve što je unutar organizacije, a tiče se procesa, informacijske imovine i zaposlenika. ISMS je također moguće nazvati „sredstvo“ kojim uprava neke organizacije prati i nadzire sigurnost informacijskog sustava. Za izgradnju sustava upravljanja informacijskom sigurnošću potreban je PDCA model (spomenut u prethodnom poglavlju), koji se kontinuirano provodi. Izgradnja samog ISMS-a je iterativni proces koji se neprestano nadograđuje i poboljšava.

Organizacija treba identificirati i upravljati mnogim aktivnostima ukoliko želi učinkovito funkcionirati. Bitno je naglasiti kako ova međunarodna norma usvaja PDCA model.



Slika 2. PDCA model

Izvor : Kostanjevec et al. (2014)

3.3.2. ISO/IEC 27002

ISO 27002 je norma koja pobliže opisuje način na koji će se provesti mjere zaštite iz ISO 27001. Ova norma predstavlja međunarodnu osnovu za razumijevanje i upravljanje informacijskom sigurnošću, a sastavljena je od 11 domena koje opisuju sigurnosne kontrole. Navedene domene sastoje se od 39 kontrolnih ciljeva te 133 kontrola koje pomažu u identificiranju, upravljanju i reduciranju prijetnji kojima su informacije i informacijski sustavi svakodnevno izloženi. Zapravo, norma ISO 27002 do 1. srpnja 2007. g. nosila je naziv Norma ISO/IEC 17799 koja je preuzeta iz prvog dijela BS 7799 standarda "Code of Practice for Information Security Management". (Bogati, J., 2011., str. 112-117). Da bi se kontrole i kontrolni mehanizmi izradili u skladu s uputama ISO 27001, potrebne su smjernice koje nudi norma ISO 27002. Ovo zapravo nije upravljačka norma stoga se po njoj ne može certificirati.

Sigurnosne mjere u normi ISO 27002 nose iste nazive kao i one u Aneksu A norme ISO 27001 pa tako u normi ISO 27002 mjera 6.1.5 ima naslov Sporazumi o tajnosti, te u normi ISO 27001 pod istim imenom A.6.1.5 Sporazumi o tajnosti. Razlika između ove dvije norme, zapravo je u količini detalja koji su posvećeni određenoj sigurnosnoj mjeri. Tako je za istu sigurnosnu mjeru u normi ISO 27001 objašnjeno tek jednom rečenicom, dok je u normi ISO 27002 detaljnije objašnjena ta ista sigurnosna mjera; toliko detaljnije da je zauzeta gotovo cijela stranica.

Posljednja objavljena verzija standarda Sustava upravljanja informacijskom sigurnošću je - BS EN ISO / IEC 27001: 2017. Izdanje za 2017. nije utjecala na ISO verziju standarda (2013) i izmjene ne uvode nikakve nove zahtjeve.

3.4. ITIL

ITIL (eng. Information Technology Infrastructure Library) knjižnica infrastrukture informacijske tehnologije skup je detaljnih praksi za IT aktivnosti kao što su upravljanje IT uslugama i upravljanje IT imovinom koje su usmjerene na usklađivanje IT usluga s potrebama poslovanja. To je proces upravljanja informacijskom sigurnošću koji opisuje pristup i kontrolira mjeru IT sigurnosti unutar organizacije.

ITIL ISM proces je temelj procesa ITIL upravljanja sigurnošću. Primarni cilj upravljanja informacijskom sigurnošću, proces ITIL V3, je efikasna kontrola pristupa organizacijskim informacijama. ISM (eng. Information Security Management) ima snažan odnos s drugim ITIL procesima kao što su upravljanje dostupnosti i upravljanja kontinuitetom IT usluga za taj resurs i za nepredviđene planiranje.

Također, koordinira i upravljanjem rizika zbog provjere bilo kojeg narušavanja sigurnosti. Isto tako koordinira se s postupkom upravljanja promjenama radi provjere i potvrđivanja svih predloženih promjena iz točke sigurnosti organizacije.

Primarni cilj procesa upravljanja informacijskom sigurnošću ITIL-a (ITIL ISM) je uskladiti IT sigurnost s poslovnom sigurnošću i osigurati da se informacijskom sigurnošću učinkovito upravlja u svim uslugama i poslovima upravljanja IT uslugama. Osigurava povjerljivost, integritet, dostupnost sredstava, informacija, podataka i IT usluga.

Prema ITIL-u V3, ISM ima četiri pod procesa:

I. Dizajn sigurnosnih kontrola

Odgovoran je za osmišljavanje odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala povjerljivost, integritet, sigurnost i dostupnost imovine, informacija, podataka i usluga organizacije. Može se svrstati u administrativnu, logičku i fizičku kontrolu.

II. Provjera sigurnosti i testiranje

Odgovoran je za redovita ispitivanja i provjeru učinkovitosti aktivnosti i implementacije IT sigurnosti.

III. Upravljanje sigurnosnim prijetnjama

Otkrivanje i reakcije protiv sigurnosnih prijetnji odnosno minimiziranje štete nastale kršenjem sigurnosti.

IV. Kontrola

Preispitati jesu li mjere sigurnosti i postupci još uvijek u skladu s očekivanim rizicima poslovne strane, te provjeriti jesu li te mjere i postupci redovito održavani i testirani.

3.5. COBIT 5

COBIT 5 (eng. Control Objectives for Information and Related Technologies) je opće radni okvir za vladanje i upravljanje IT-em i jedini je poslovni okvir za upravljanje IT poduzeća. To je proizvod globalne radne skupine i razvojnog tima ISACA-e-neprofitne, neovisne udruge koji broji više od 140.000 profesionalaca u području upravljanja, sigurnosti, rizika i osiguranja u 187 zemalja. COBIT 5 uključuje najnovija razmišljanja u upravljanju tehnikama poduzeća koja pruža globalno prihvaćena načela, prakse, analitičke alate i modele koji pomažu u povećanju povjerenja u informacijske sustave i njihove vrijednosti.

COBIT 5 se gradi i proširuje na COBIT 4.1 integrirajući ostale glavne okvire, standarde i resurse, uključujući ISACA-in Val IT i Risk IT, informacijske tehnologije (ITIL) i srodne standarde Međunarodne organizacije za standardizaciju (ISO).

Svakodnevno se pojavljuju novi zahtjevi korisnika, specifični propisi i razni rizici. Maksimiziranje vrijednosti intelektualnog vlasništva, upravljanje rizikom i sigurnošću i osiguranje usklađenosti kroz učinkovito upravljanje informatičkim tehnologijama i upravljanje nikada nisu bili važniji.

Niti jedan drugi okvir fokusiran na IT poduzeća ne nudi širinu ili prednosti COBIT-a. Pomaže tvrtkama svih veličina u:

- Održavanju visokokvalitetne informacije za podršku poslovnim odlukama

- Postizanje strateških ciljeva kroz učinkovitu i inovativnu upotrebu IT-a

- Postizanje operativne izvrsnosti pouzdanom i učinkovitom primjenom tehnologije

- Održavanju rizika vezanog za IT na prihvatljivoj razini

- Optimizacija troškova IT usluga i tehnologije

- Podržavanje i poštivanje relevantnih zakona, propisa, ugovornih sporazuma i politika.

COBIT 5 je općenit i koristan za poduzeća svih veličina, bilo komercijalnih, neprofitnih ili u javnom sektoru. Koriste ga globalno oni koji imaju primarnu odgovornost za poslovne procese i tehnologiju, ovise o tehnologiji relevantnih i pouzdanih informacija i pružaju kvalitetu, pouzdanost i kontrolu informacija i srodne tehnologije. (www.isaca.org/cobit, pristupljeno 21.06.2022.)

Usporedba ISO/COBIT/ITIL

Svaki od okvira i standarda sustava može ponuditi različite snage i slabosti. Ako se odabere samo jedan od njih, moguće je propustiti neke dobre strane ovog drugog, a sustavu upravljanja nedostajati će neke važne karakteristike.

Na primjer, primjena ITIL-a pruža puno detaljnih smjernica o provedbi procesa, ali je prilično slaba u pogledu upravljanja i postavljanja ciljeva. S druge strane, COBIT 5 iako je vrlo jak u upravljanju i postavljanju ciljeva ne daje puno detalja o provedbi procesa; a ISO, koji pruža sažetu informaciju o tome što bi IT organizacija trebala raditi, nudi malo smjernica o tome kako zapravo raditi.

U praksi, bilo bi potrebno da se organizacija sagleda kroz nekoliko stajališta, a ne kroz samo jedan. U budućnosti će biti mnogo jednostavnije, tratiti će se manje vremena, a sama poslovna organizacija će biti učinkovitija kada zna u kojem se smjeru želi kretati, odnosno u kojim je područjima potrebno implementirati okvire i standarde.

Kako bi se pobliže shvatila i razumjela razlika između navedenih standarda, razlike su navedene u tablici ispod.

Tablica 1. Usporedba standarda COBIT, ISO, ITIL

	ITIL	COBIT	ISO
ŠTO JE?	Skup izdanja o najboljoj praksi za upravljanje IT uslugama	Poslovni okvir za upravljanje IT poduzećima	Međunarodni standard za zahtjeve sustava upravljanja IT uslugama
KOLIKO JE DUGAČKO?	5 temeljnih izdanja koje se sastoje od 1800 str. kompletnih izdanja	Temeljno izdanje sadrži 94 str + 230 str za omogućavanje procesa	1.dio ima 36 str; ima više nastavaka koji pokrivaju različita područja
KAKO IZGLEDA NA TRŽIŠTU?	ITIL se fokusira na internacionalne IT procese; u posljednjim izdanjima više se fokusira na vrijednosti i kupce	COBIT dolazi iz povijesti revizije i poštivanja pravila; najnovija verzija prešla je na upravljanje IT sustavima	ISO 27001 prikazuje primjernu upravljanja informacijskom sigurnošću
TKO GA KORISTI?	Sve organizacije koje pružaju IT usluge; najčešće u operativnom IT-u	Za velike IT organizacije; često ga koriste strateški timovi i ljudi odgovorni za reviziju i zakone	IT organizacije koje žele pokazati da ispunjavaju definirani standard
ZA ŠTO SE KORISTI?	Pomaže u definiranju operativnih procesa u pružanju IT usluga	Definiranje zahtjeva za revizijom i usklađivanje za IT	Pokazuje da IT organizacija ispunjava određeni standard

Izvor: izrada autora

3.6. World Lottery Association

Hrvatska Lutrija je članica Svjetske lutrijske organizacije (WLA-World Lottery Association) koja se bavi unapređivanjem interesa državnih lutrijskih organizacija te je u vlasništvu jedinog međunarodno priznatog sigurnosnog standarda u području poslovanja lutrijskih igara.

WLA-SCS definira standard za sigurnost, integritet i menadžment rizika koji koriste priređivači lutrijskih igara i igara klađenja, te je njena namjena biti središnja točka sektora za sve probleme sigurnosti i integriteta. Opisuje proces menadžmenta sigurnosti koji je poravnat s internacionalno prepoznatim standardima kao i osnovnom sigurnosnom podlogom koja predstavlja dobro poslovanje za priređivače lutrijskih igara i igara klađenja. Standard sadrži set kontrola i zahtjeva za priređivače i njihove dobavljače.

WLA-SCS se može smatrati temeljem za stvaranje odnosa povjerenja s dionicima industrije i regulatorima, u svrhu vođenja poslovanja u industriji igara na sreću, te igara koje se priređuju multi-teritorijalno. Također može biti od pomoći vrhu menadžmenta, pružajući samostalni

pregled kako bi se povećalo povjerenje u sigurnosne radnje priređivača lutrijskih igara i igara klađenja.

Posljednja verzija standarda, WLA-SCS:2020 uvela je certifikacijski okvir na dvije razine.

Usklađenost s WLA-SCS razinom 1 pruža osnovnu ali bitnu razinu informacijske sigurnosti za priređivače te pokazuje njihovu želju za ostvarenjem WLA-SCS razine 2, najveće razine certifikacije. WLA-SCS razina 1 pogodna je za one priređivače koji certificiranju žele pristupiti korak po korak.

Usklađenost s WLA-SCS razinom 2 dozvoljava članovima WLA da osiguraju integritet, dostupnost i povjerljivost usluga i informacija koji su ključni za njihovo sigurno upravljanje.

WLA-SCS razina 2 predstavlja najkompletniji i najobuhvatniji certifikacijski standard za priređivače lutrijskih igara i igara klađenja, te njihove dobavljače.

Usvajanje WLA-SCS je strateška odluka. Dizajn i implementacija sustava za menadžment za sigurnost i integritet u nekoj poslovnoj organizaciji, ovisi o utjecaju njihovih pojedinih potreba, ciljeva, rizika, procesa te veličine i strukture same organizacije. Ti faktori i potrebe mogu se mijenjati tijekom vremena, pa tako jednostavna organizacija treba jednostavna rješenja.

Usklađenje s WLA-SCS može se koristiti od strane zainteresiranih internih i eksternih stranka, kako bi se evaluirala sigurnost i integritet sustava neke lutrije, kao i njenih dobavljača. Uz ISO/IEC 27001, WLA-SCS je usklađena i s ISO 9001 kako bi se omogućila stalna integrirana implementacija i poslovanje s povezanim standardima menadžmenta. Pokriva sve vrste lutrijskih organizacija, uključujući trgovačka poduzeća, vladine ustanove i neprofitne organizacije.

WLA-SCS specificira zahtjeve za postavljanje, implementaciju, praćenje, pregledavanje, održavanje i unapređenje sistema za sigurnost i integritet, u kontekstu rizika neke organizacije. Sastoji od četiri dijela koji specificiraju minimum potrebnih kontrola za efikasni menadžment sigurnosti i integriteta u lutrijskim organizacijama i njihovim dobavljačima.

Prvi dio (aneks A – G) inkorporira ISO/IEC 27001 usklađenost u globalnom opsegu, s dodatno pridruženih 24 osnovnih WLA kontrola.

Drugi dio (Aneks B – L) uključuje dodatnih 64 kontrola za sigurnost i integritet specifičnih za igre unutar lutrijskih organizacija, a koje predstavljaju trenutno najbolje prakse.

Treći dio (Aneks C - S) sadrži 21 kontrolu koja se bazira na proizvodima i uslugama koje nude dobavljači za lutrijske igre i gire klađenja.

Četvrti dio (Aneks D – M) sadrži 11 kontrola koje su potrebne za sudjelovanje u igrama na sreću koje priređuje multi nacionalna lutrija Sjedinjenih država (MUSL).

Glavni cilj pristupa sigurnosti i integriteta za članove WLA je da osiguraju adekvatno poslovanje kao i povjerenje.

Povjerenje u poslu lutrijskih igara i igara klađenja je ključ za retenciju igrača i ostalih dionika. Prema tome, članovi WLA moraju razviti i održavati vidljivo i dokumentirano okruženje sigurnosti i integriteta. (https://www.world-lotteries.org/volumes/downloads/Download_Center/Security/WLA_SCS_2020/202012_EN_WLA-SCS-2020_Standard_V1-2.pdf pristupljeno 14.06.2022.)

3.7. General Data Protection Regulation

GDPR (eng. General Data Protection Regulation) je opća uredba o zaštiti podataka. Uredba Europske unije o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, poznatija pod akronimom GDPR, donesena je 27. travnja 2016. u Bruxellesu od strane Europskog parlamenta i Vijeća Europske unije, a stupila je na snagu dvadesetog dana od dana objave u Službenom listu Europske unije. Sukladno članku 99., stavku 2., Uredba se primjenjuje od 25. svibnja 2018. u svim državama članicama Europske unije. Razvoj novih tehnologija, a time i efikasnijeg, automatiziranog načina obrade podataka, omogućio je prikupljanje sve veće količine podataka, čime su osobni podaci postali dostupniji nego ikada prije.

Schepman et al. (2008) navode da su korisnici zbog toga sve više zabrinuti za svoju privatnost te da nisu uvijek informirani o načinu na koji se njihovi osobni podatci obrađuju.

Horvat (2002.) napominje da je identifikacija osobnim podatcima često neizbježna za dobivanje određene usluge ili obavljanja određenog posla. Također navodi i da su nove informacijske tehnologije omogućile i objedinjavanje osobnih podataka, te da se pojedinac „može s pravom bojati da bi mu neovlašteni uvid u njegove osobne podatke mogao onemogućiti dobivanje neke usluge, povlastice itd.” (Horvat, 2002:8-15).

U Priručniku se također navodi da je pojavom informacijske tehnologije 1960-ih rasla „potreba za detaljnijim propisima kojima bi se zaštitili (osobni) podaci pojedinaca“ jer su, kako objašnjava Horvat (2002), „države vrlo brzo shvatile opasnost zloporabe mogućnosti koje pruža nova informacijska tehnologija.” Slobodan protok informacija postao je bitna stavka europskoga tržišta, a kako se tehnologija za automatsku obradu i pohranu podataka razvijala istovremeno kada i Europska ekonomska zajednica (EEZ), ostvarena je i veća prekogranična razmjena podataka. Na temelju EEZ-a te Euratoma i Europske zajednice za ugljen i čelik nastala je Europska unija, koja je prepoznala potrebu za regulacijom protoka i obrade podataka te je doneseno više propisa s ciljem zaštite osobnih podataka.

Najrecentnija među njima je Opća uredba o zaštiti osobnih podataka, čiji se razlog donošenja navodi i u preambuli: „Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti osobnih podataka…Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i gospodarstvo i društveni život te bi trebala dalje olakšavati slobodan protok osobnih podataka u Uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visoku razinu zaštite osobnih podataka.“

(https://www.privacy-regulation.eu/hr/r6.htm pristupljeno 20.06.2022.)

4. Provođenje internog audita

Svrha i cilj provođenja internog audita je provjera ispunjavanja zahtjeva normi, zakonskih regulativa i internih dokumentiranih informacija.

Interni audit (revizija, procjena) je sustavan, neovisan i dokumentiran proces provjere postavljenih zahtjeva normi, zakonske regulative i internih dokumentiranih informacija kako bi se utvrdio opseg u kojem su ispunjeni kriteriji audita. Interni audit može biti redovni i izvanredni.

Redovni interni audit provodi se prema unaprijed planiranom planu internih audita, najmanje jednom godišnje. Godišnji plan internih audita definira koordinator internog audita do kraja prosinca tekuće godine za iduću godinu. Prilikom definiranja godišnjeg plana internih audita uzima se u obzir zadnja procjena rizika i rezultati internih i vanjskih audita iz prethodnih godina.

Izvanredni interni audit provodi se prema uočenoj potrebi koju utvrđuje Uprava ili koordinator internog audita.

U poslovnoj organizaciji potrebno je da interni audit provode radnici koji imaju dokazane osobne odlike i kompetentnosti za provođenje audita. U slučaju manjka kompetentnih radnika za pojedina područja ili u slučaju nedostatka resursa, interni audit može provesti vanjski ugovoreni partner.

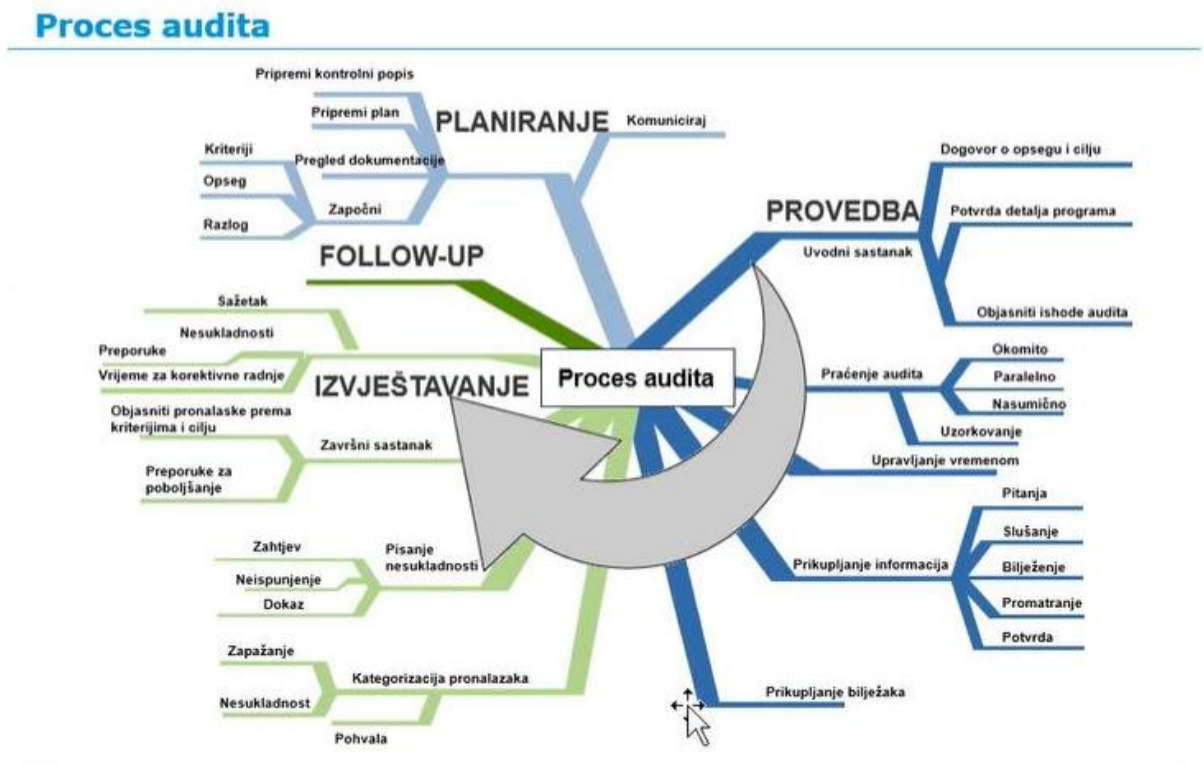
U slučaju da interni audit provodi vanjski ugovoreni partner, preporuča se postupanje po proceduri navedenoj u nastavku uz korištenje propisanih obrazaca.

Proces internog audita sastoji se od tri koraka:

1. priprema internog audita,

2. provođenje internog audita,

3. završetak internog audita.



Slika 3. Proces audita

Izvor: Det Norske Veritas (2013)

4.1. Priprema internog audita

Koordinator internog audita određuje točan termin izvođenja internog audita i članove audit tima, koji moraju biti neovisni o području auditiranja. Nakon toga koordinator internog audita izrađuje detaljni Izvedbeni plan internog audita po danima u dogovoru s predstavnicima auditiranog područja. Izvedbeni plan internog audita mora sadržavati i plan za dane u kojima se obavlja pregled dokumentacije auditiranog područja, u slučaju da audit to zahtijeva. Nakon definiranja Izvedbenog plana internog audita, koordinator internog audita obavještava voditelje organizacijskih jedinica iz kojih dolaze članovi audit tima o terminu izvođenja internog audita kako bi radnici u tom periodu u što većoj mjeri bili oslobođeni svojih standardnih poslova. Izuzev datuma navedenih u Izvedbenom planu internog audita, mora se uzeti u obzir i vrijeme koje je potrebno auditorima za pripremu za audit (izrada pripremnih materijala) i za izradu završnog izvještaja. Najmanje tjedan dana prije internog audita, koordinator internog audita mora poslati Izvedbeni plan internog audita svim članovima audit tima kako bi se isti upoznali

sa svrhom, opsegom i ciljevima planiranog internog audita i obavili potrebne pripreme za audit. Najmanje tjedan dana prije internog audita, koordinator internog audita mora poslati izvatke Izvedbenog plana internog audita predstavnicima auditiranog područja kako bi se isti mogli pripremiti za interni audit.

4.2. Provođenje internog audita

Provođenje internog audita sastoji se od pregleda dokumentacije auditiranog područja, ako to audit zahtijeva, prije samog razgovora s predstavnicima auditiranog područja i od razgovora s predstavnicima auditiranog područja.

Tijekom provođenja internog audita utvrđuje se stvarno stanje auditiranog područja, odnosno zadovoljava li auditirani sustav zahtjeve normi i zakonske regulative, provode li se aktivnosti i mjere koje su propisane internim dokumentiranim informacijama i je li sustav učinkovito proveden i održavan. Također, prilikom provođenja audita provjerava se status provedbe nesukladnosti i zapažanja s prethodnih audita (internih i eksternih). Članovi audit tima tijekom provođenja audita utvrđuju stanje kroz nalaze. Postoje četiri kategorije nalaza: nesukladnost, zapažanje, prilika za poboljšanje i pohvala. U nastavku su navedene definicije kategorija nalaza i akcije koje se poduzimaju za svaku kategoriju.

1. Nesukladnost

Nesukladnost predstavlja nalaz za područje koje nije usklađeno sa zahtjevima norme, zakonske regulative i internih dokumentiranih informacija ili kada predstavnici auditiranog područja ne mogu pokazati dokaze o usklađenosti. Nesukladnost mora imati jasan zahtjev koji nije ispunjen i moraju postojati jasni dokazi o neusklađenosti. Članovi audit tima zajedno s predstavnicima auditiranog područja definiraju popravne (korektivne) mjere za rješavanje nesukladnosti, odgovornu osobu za provođenje mjera i rok za provedbu.

2. Zapažanje

Zapažanje predstavlja nalaz za područje koje je trenutno usklađeno sa zahtjevima norme, zakonske regulative i internih dokumentiranih informacija, ali postoji mogućnost da postane nesukladno u budućnosti. Zapažanje se može shvatiti kao „nesreća koja čeka da se dogodi“. Članovi audit tima zajedno s predstavnicima auditiranog područja definiraju preventivne mjere

za zapažanje i odgovornu osobu za provođenje mjera. Kod zapažanja se ne definira rok za provedbu.

3. Prilika za poboljšanje

Prilika za poboljšanje predstavlja nalaz za područje koje nije nužno krivo ili ne udovoljava zahtjevima norme, zakonske regulative i propisanih internih dokumentiranih informacija, već predstavlja mogućnost poboljšanja učinkovitosti sustava. Prilika za poboljšanje nije „nesreća koja čega da se dogodi“ nego ukazuje na loše implementiranu praksu ili nedostatak iste. Priliku za poboljšanje članovi audit tima donose na temelju svoje stručnosti i proširenog pogleda na sustave upravljanja. Članovi audit tima zajedno s predstavnicima auditiranog područja definiraju osobu odgovornu za područje u kojem je uočena prilika za poboljšanje. Kod prilike za poboljšanje ne definira se rok za provedbu.

4. Pohvala

Pohvala predstavlja nalaz za područje za koje se smatra izvrsnim primjerom provedbe zahtjeva norme, zakonske regulative i internih dokumentiranih informacija. Pohvalom se također ukazuje na značajna poboljšanja u određenim područjima u odnosu na prethodne audite. Pohvale ne zahtijevaju nikakvu akciju nego služe za potrebe izvještavanja.

U slučaju da dođe do nemogućnosti usuglašavanja između članova audit tima i predstavnika auditiranih područja oko pronađenih nesukladnosti ili zapažanja, definiranja popravnih ili preventivnih mjera, definiranja odgovornih osoba ili rokova, članovi audit tima uključuju koordinatora internog audita koji donosi finalnu odluku u suradnji s rukovoditeljima auditiranih organizacijskih jedinica ili s Upravom. Provođenje internog audita završava nakon usuglašavanja oko pronađenih nesukladnosti ili zapažanja, definiranja popravnih ili preventivnih mjera i definiranja odgovornih osoba ili rokova.

4.3. Završetak internog audita

Nakon završetka provođenja internog audita članovi audit tima izrađuju Izvješće o internom auditu za auditirano područje te ga dostavljaju koordinatoru internog audita u roku od tjedan dana od završetka provođenja internog audita. Izvješće o internom auditu mora sadržavati popis svih nesukladnosti, zapažanja, prilika za poboljšanje i pohvala s definiranim akcijama (popisom dogovorenih mjera, rokova i odgovornih osoba) koje su definirane.

Nakon zaprimanja svih izvješća koordinator internog audita iste objedinjuje u jedinstveno Izvješće o internom auditu kojeg moraju potpisati članovi audit tima i sam koordinator internog audita.

Koordinator internog audita zadužen je za unos svih pronađenih nesukladnosti i zapažanja u Evidenciju nesukladnosti i zapažanja s internih audita. Nakon popisivanja svih nesukladnosti i zapažanja, koordinator internog audita zadužen je za slanje izvatka iz Evidencije odgovornim osobama definiranim na internom auditu kako bi iste bile upućene na popravne i preventivne mjere koje je potrebno provesti u definiranim rokovima. Revizija statusa otvorenih nesukladnosti i zapažanja obavlja se prema potrebi koju određuje koordinator internog audita, a najkasnije dva tjedna prije sljedećeg planiranog internog audita.

REFERENTNI DOKUMENTI

- Norma ISO/IEC 27001

- Norma ISO/IEC 27002

- Norma WLA SCS

- Politika informacijske sigurnosti

- Pravilnik o radu

5. Materijali i metode

U svrhu testiranja postavljenih hipoteza i odgovora na postavljeno istraživačko pitanje prikupljen je istraživački materijal iz znanstvenih i stručnih literatura koji se koristio pri izradi teorijskog dijela diplomskog rada.

5.1. Istraživački materijal

U diplomskom radu korišteni su primarni i sekundarni izvori podataka. Putem provedene online ankete koja je bila namijenjena svim zaposlenicima u poslovnoj organizaciji dobiveni su primarni podaci potrebni za analizu. Znanstveni radovi, časopisi, web izvori, knjige, stručne literature, zakoni, propisi i standardi su korišteni kao sekundarni izvori podataka.

5.2. Metode istraživanja

Istraživački dio diplomskog rada temeljen je na kvantitativnoj metodi istraživanja, odnosno anketnom upitniku. Metoda ispitivanja odnosno anketiranja provela se pomoću anketnog upitnika koji je kreiran na platformi *„Survey monkey“* te prikupljanjem i obradom empirijskih podataka su analizirani rezultati. Anketiranje je provedeno zbog mogućnosti kontakta sa što većim brojem zaposlenika unutar poslovne organizacije, upitnik se sastoji od 15 pitanja a u obzir se uzimaju odgovori zaposlenika u poslovnoj organizaciji.

5.3. Postupak provedbe istraživanja

Istraživanje je provedeno putem anonimne ankete koja je mailom poslana svim zaposlenicima unutar poslovne organizacije, rok za ispunjavanje ankete je bio mjesec dana.

Uzorak je prikladan za dobivanje indikativnih rezultata te donošenja općih zaključaka o utjecaju stupnja obrazovanja na razinu zaštite informacijskih sustava unutar poslovne organizacije.

Ograničenja koja su primijećena u provođenju ovog istraživanja su: ista poslovna organizacija, nejednaka zastupljenost ispitanika po sektoru poslovanja, uvjeti prilikom ispunjavanja anketnog upitnika te različito obrazovanje zaposlenika. Zaposlenici u poslovnoj organizaciji nemaju jednake kriterije prilikom procjenjivanja važnosti određenih faktora. Istraživanje je provedeno unutar poslovne organizacije, u online okruženju.

5.4. Metode obrade podataka

Obrada podataka dobivenih anketnim upitnikom obrađena je SPSS alatom sljedećim statističkim metodama: Anova (engl. Analysis of variance) test, cronbach alpha i deskriptivna statistika. Podaci koji su dobiveni iz ovog istraživanja pomoću anketnog upitnika prikazani su u tablicama i grafikonima uz kratki opis rezultata.

Anova test ili analiza varijance je statistički test koji traži značajne razlike između podataka. Postoje četiri pretpostavke nakon analize varijance: očekivane vrijednosti pogrešaka su nula, varijance svih pogrešaka u međusobno jednake, pogreške su međusobno povezane i pogreške se normalno distribuiraju.

Deskriptivna statistika organizira prikupljene podatke pomoću numeričkih i grafičkih prikaza.

Cronbach Alpha (α) je koeficijent koji se koristi za mjerenje pouzdanosti testa ili mjerne ljestvice. Pouzdanost testa ili mjerne ljestvice definira se kao mogućnost određenog produkta, usluga ili sistema koji na adekvatan način daje svoje funkcije u određenom vremenskom periodu, ili da u tom vremenskom periodu funkcionira bez greške. Prilikom mjerenja određenog procesa za koji se pretpostavlja konzistentnost u tom vremenu tada su i dobiveni rezultati konzistentni. Mjera koja određuje konzistentnost i kako je to u stvarnosti je pouzdanost testiranja i retestiranja. Cronbach alpha koeficijent se kreće od 0 do maksimalno 1. Što je koeficijent cronbach alphe bliže 1, stavke su međusobno usklađenije (također vrijedi obrnuto). S druge strane, uzima se u obzir dužina testa, što znači, duži test veća alpha.

Na primjeru testa koji ima pouzdanost od 0.80 varianca pogreške u tim podacima je 0.36 (0.80*0.80=0.64; 1-0.64= 0.36). Kako se povećava procjena pouzdanosti sukladno tome se smanjuje postotak variance pogreške. Ukoliko se neispravno koristi cronbach alpha dolazi do situacija u kojima test bude odbačen ili se karakterizira kao nepouzdan. Jednodimenzionalnost pomaže da izbjegnemo takve situacije te poboljšamo uporabu cronbach alphe.. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/, pristupio 10.07.2022)

6. Rezultati istraživanja

Anketa je sadržavala socio-demografska pitanja te se tražilo od zaposlenika da prikažu svoje poznavanje informacijske sigurnosti te procedure i ulaganja poslovne organizacije u informacijsku sigurnost.

Rezultate ankete sam analizirao pomoću ANOVA testa, deskriptivne statistike i Cronbach alpha koeficijenta. Pitanja su bila postavljena s mogućnošću jednog odgovora, više mogućih odgovora te Likertove skale. Zadnje pitanje je bilo opisnog karaktera u kojem su zaposlenici dali svoje mišljenje o dodatnom unapređenju informacijske sigurnosti u poslovnoj organizaciji.

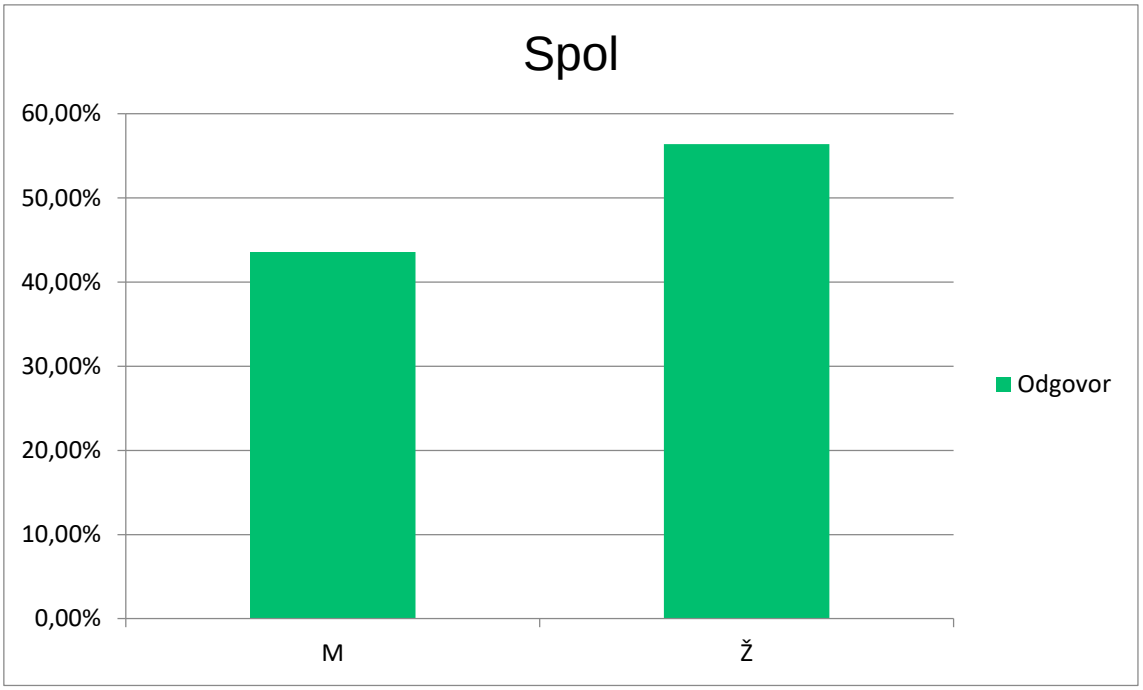
1. **Pitanje: Spol**

Prvo pitanje odnosilo se na spol ispitanika. Od 351 odgovora, njih 198 točnije 56,41% bilo je ženskog spola. 153 ispitanika bilo je muškog spola, što je iznosilo 43,59% od ukupnog broja ispitanika.

Tablica 2. Spol ispitanika

Ponuđeni odgovori	Odgovor	
M	43,59%	153
Ž	56,41%	198
	Odgovoreno	**351**

Izvor: izrada autora



Slika 4. Spol ispitanika

Izvor: izrada autora

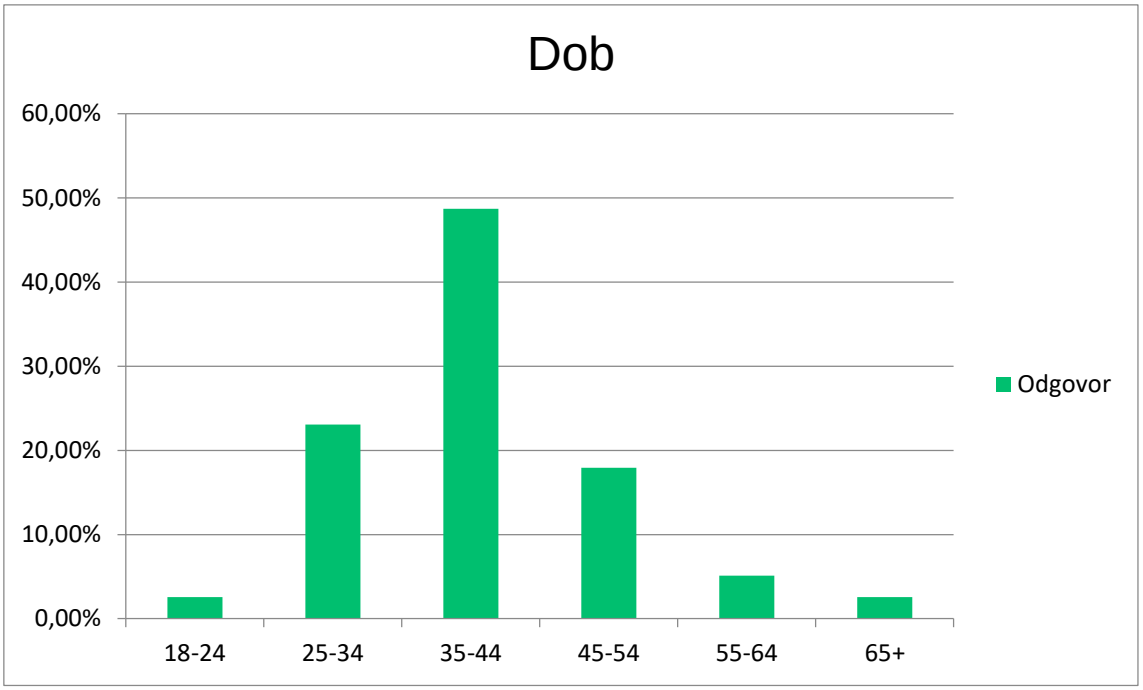
2. Pitanje: Dob

Drugo pitanje odnosilo se na dob ispitanika. Ponuđeni odgovori su bili od 18 do 24; od 25 do 34; od 35 do 44; od 45 do 54; od 55 do 64; i više od 65. Najviše ispitanika bilo je u dobi od 35 do 44 godina, njih 171 (48,72%). Najmanje ispitanika bilo je u skupini od 18 do 24 godine i više od 65 godina sa samo 9 ispitanika, odnosno 2,56% od ukupnog broja ispitanika.

Tablica 3. Dob ispitanika

Ponuđeni odgovori	Odgovor	
18-24	2,56%	9
25-34	23,08%	81
35-44	48,72%	171
45-54	17,95%	63
55-64	5,13%	18
65+	2,56%	9
	Odgovoreno	**351**

Izvor: izrada autora



Slika 5. Dob ispitanika

Izvor: izrada autora

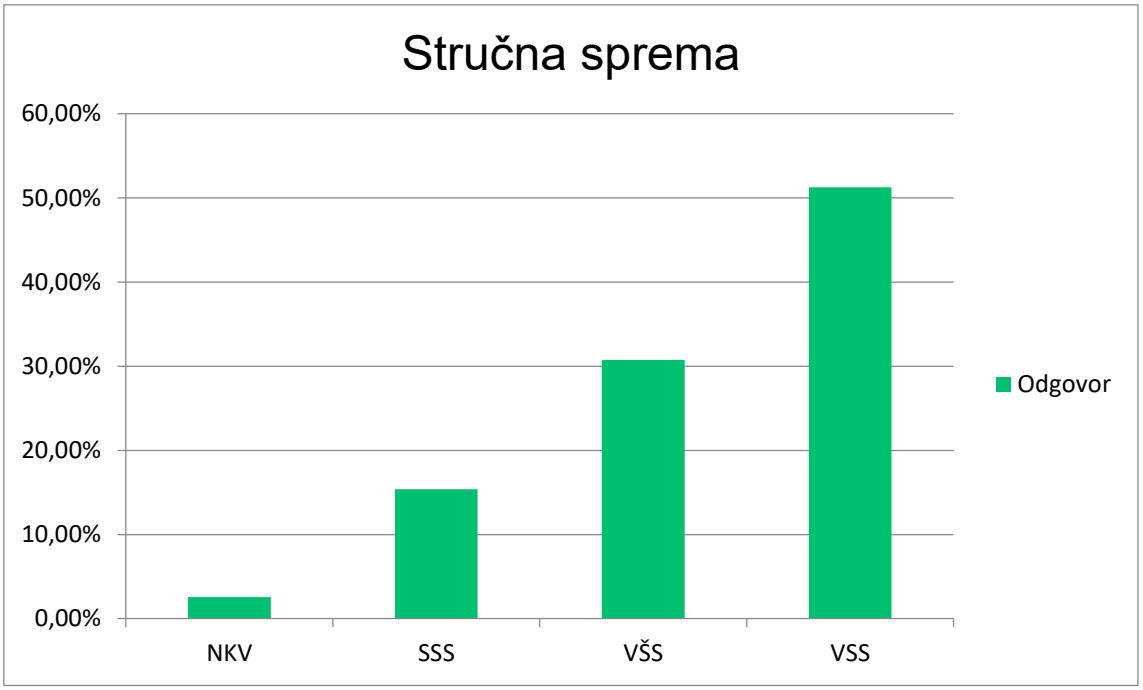
3. Pitanje: Stručna sprema

Treće pitanje se odnosilo na stručnu spremu ispitanika. Ponuđeni odgovori su bili NKV; SSS; VŠS; VSS. Višu stručnu spremu posjeduje 30% ispitanika, dok njih 51% ima visoku stručnu spremu, dok je samo 2% ispitanika nekvalificirano.

Tablica 4. Stručna sprema ispitanika

Ponuđeni odgovori	Odgovor	
NKV	2,56%	9
SSS	15,38%	54
VŠS	30,77%	108
VSS	51,28%	180
	Odgovoreno	**351**

Izvor: izrada autora



Slika 6. Stručna sprema ispitanika

Izvor: izrada autora

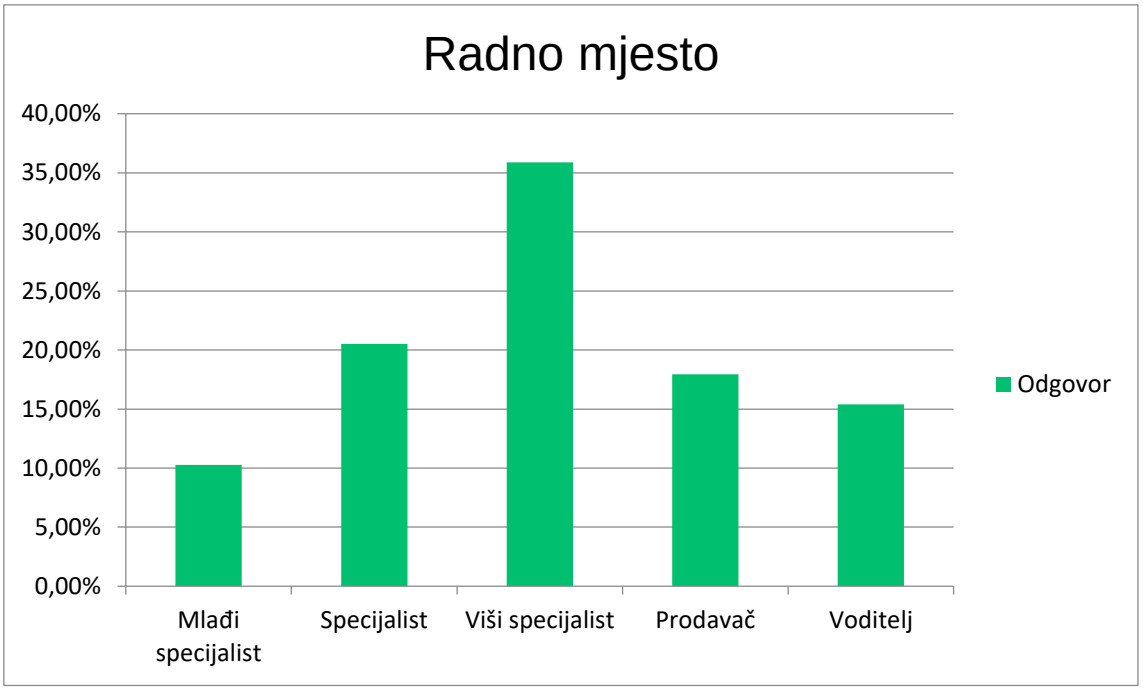
4. Pitanje: Radno mjesto

Četvrto pitanje se odnosilo na radno mjesto u poslovnoj organizaciji. Ponuđeni odgovori su bili Mlađi specijalist; Specijalist; Viši specijalist; Prodavač; Voditelj. Najviše ispitanika radi na poziciji Višeg specijalista 36%, dok funkciju mlađeg specijalista obavlja 10% ispitanika. S obzirom na opseg posla postoji mogućnost da prodavači nisu bili u mogućnosti popuniti anketu.

Tablica 5. Radno mjesto ispitanika

Ponuđeni odgovori	Odgovor	
Mlađi specijalist	10,26%	36
Specijalist	20,51%	72
Viši specijalist	35,90%	126
Prodavač	17,95%	63
Voditelj	15,38%	54
	Odgovoreno	**351**

Izvor: izrada autora



Slika 7. Radno mjesto ispitanika

Izvor: izrada autora

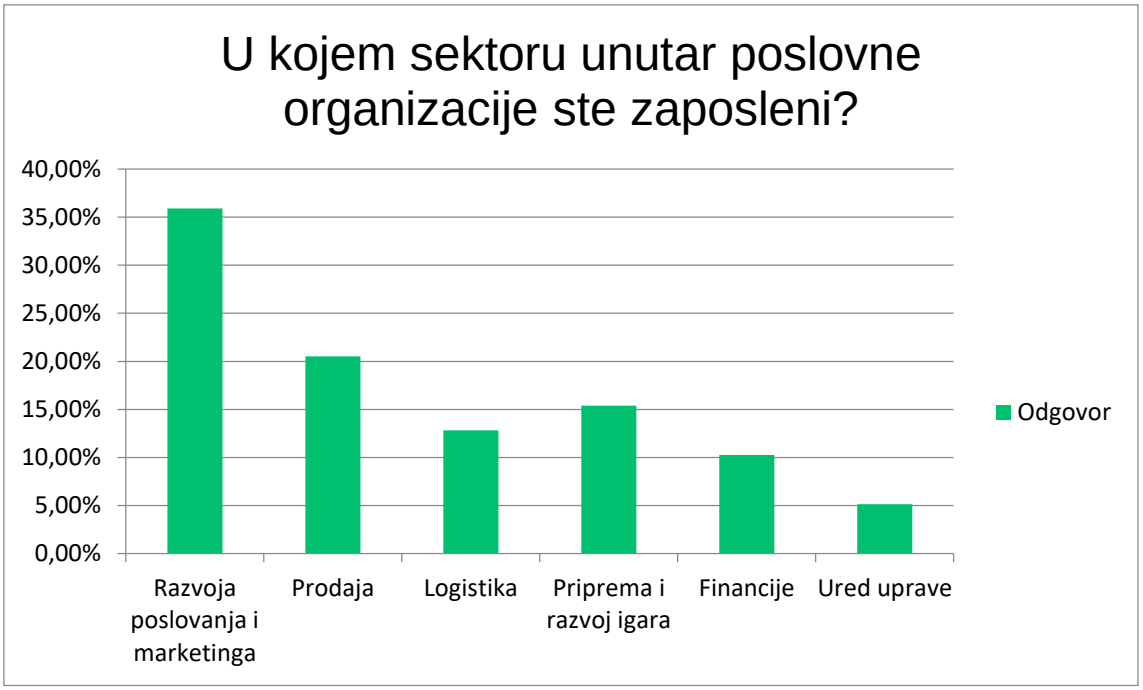
5. Pitanje: U kojem sektoru unutar poslovne organizacije ste zaposleni

Peto pitanje se odnosilo na sektor unutar organizacije zaposlenika. Ponuđeni odgovori su bili Razvoj poslovanja i marketinga; Prodaja; Logistika; Priprema i razvoj igara; Financije; Ured uprave. Najviše ispitanika radi u Sektoru razvoja poslovanja i marketinga, čak 36%, dok je najmanje ispitanika koji pripadaju uredu uprave, samo 5%.

Tablica 6. Sektor unutar organizacije ispitanika

Ponuđeni odgovori	Odgovor	
Razvoja poslovanja i marketinga	35,90%	126
Prodaja	20,51%	72
Logistika	12,82%	45
Priprema i razvoj igara	15,38%	54
Financije	10,26%	36
Ured uprave	5,13%	18
	Odgovoreno	**351**

Izvor: izrada autora



Slika 8. Sektor unutar organizacije ispitanika

Izvor: izrada autora

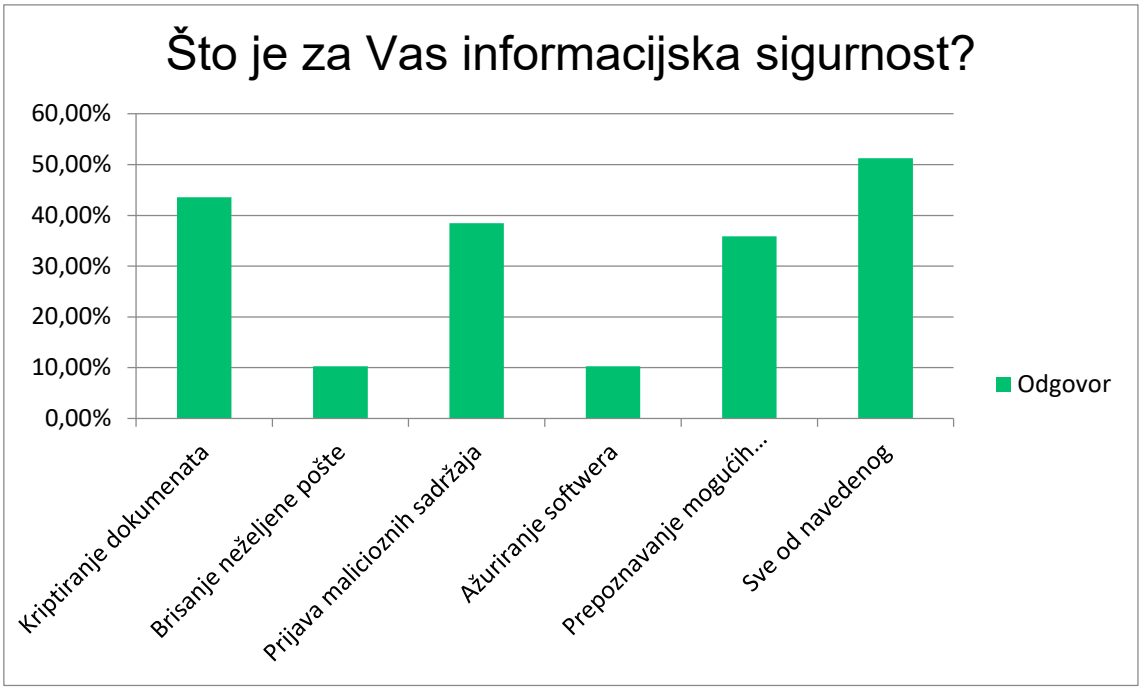
6. Pitanje: Što je za Vas informacijska sigurnost?

U šestom pitanju su ispitanici imali mogućnost odabrati više točnih odgovora. Najveći broj ispitanika je odabrao odgovor „sve od navedenog“, iz odgovora je vidljivo kako su zaposlenici upoznati sa pojmom informacijske sigurnosti te znaju koji su važni koraci za zaštitu.

Tablica 7. Mišljenje ispitanika o informacijskoj sigurnosti

Ponuđeni odgovori	Odgovor	
Kriptiranje dokumenata	43,59%	153
Brisanje neželjene pošte	10,26%	36
Prijava malicioznih sadržaja	38,46%	135
Ažuriranje software	10,26%	36
Prepoznavanje mogućih kibernetičkih napada	35,90%	126
Sve od navedenog	51,28%	180
	Odgovoreno	**351**

Izvor: izrada autora



Slika 9. Mišljenje ispitanika o informacijskoj sigurnosti

Izvor: izrada autora

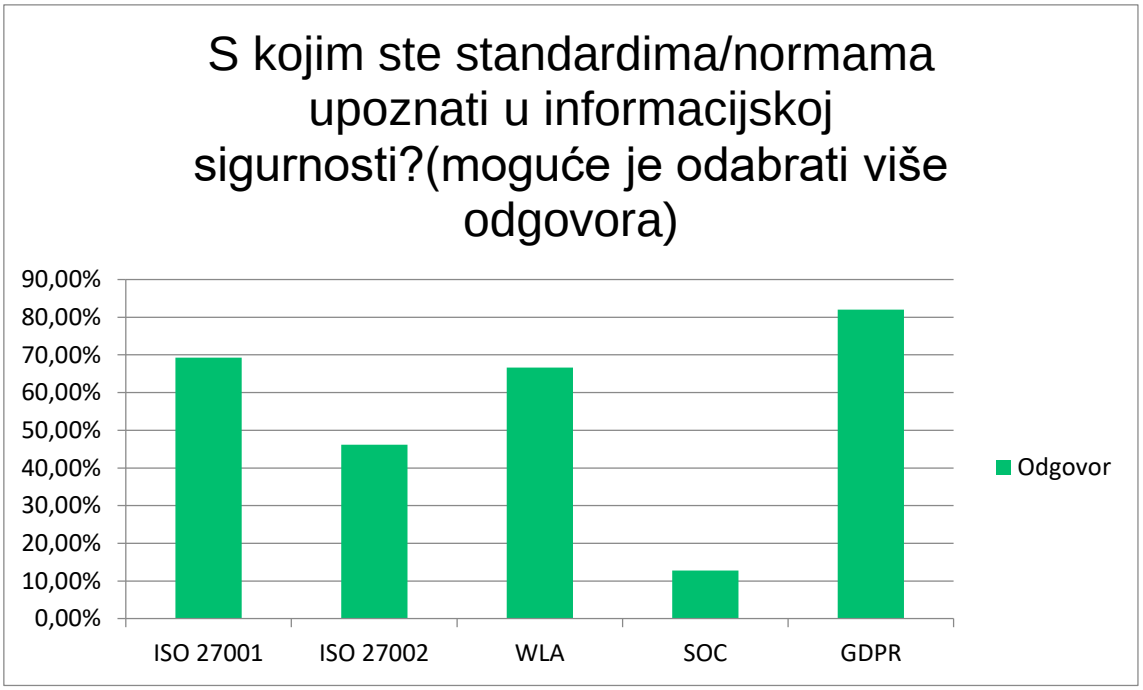
7. Pitanje: S kojim ste standardima/normama upoznati u informacijskoj sigurnosti?

Iz sedmog pitanja je vidljivo kako su zaposlenici upoznati sa standardima/normama poslovne organizacije. Čak 82% ispitanika je odgovorilo da je upoznato za uredbom o zaštiti podataka koja je jedna od najvažnijih u poslovnoj organizaciji.

Tablica 8. Standardi/norme s kojima su zaposlenici upoznati

Ponuđeni odgovori	Odgovor	
ISO 27001	69,23%	243
ISO 27002	46,15%	162
WLA	66,67%	234
SOC	12,82%	45
GDPR	82,05%	288
	Odgovoreno	**351**

Izvor: izrada autora



Slika 10. Standardi/norme s kojima su zaposlenici upoznati

Izvor: izrada autora

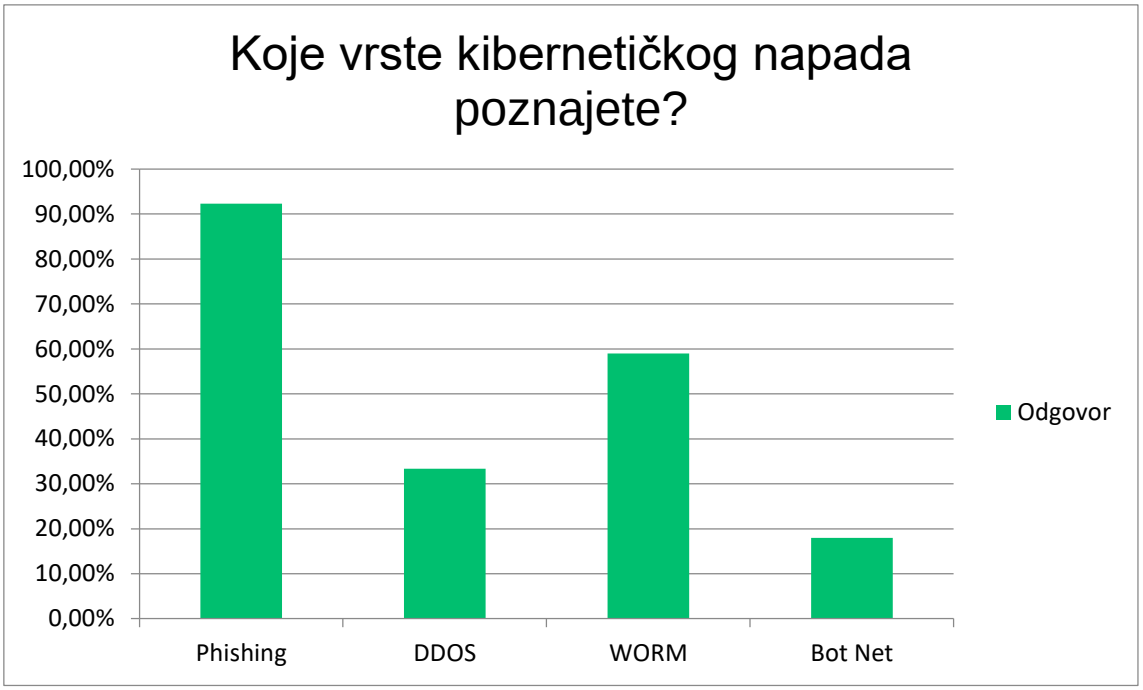
8. Pitanje: Koje vrste kibernetičkog napada poznajete?

U osmom pitanju su ispitanici potvrdili svoje poznavanje te je njih 92% odgovorilo da je upoznato sa *phishing* napadom koji je najučestaliji u velikim poslovnim organizacijama. Rezultat velikog postotka je nedavna edukacija vezana za informacijsku sigurnost.

Tablica 9. Poznavanje vrsta kibernetičkih napada zaposlenika

Ponuđeni odgovori	Odgovor	
Phishing	92,31%	324
DDOS	33,33%	117
WORM	58,97%	207
Bot Net	17,95%	63
	Odgovoreno	**351**

Izvor: izrada autora



Slika 11. Poznavanje vrsta kibernetičkih napada zaposlenika

Izvor: izrada autora

9. Pitanje: Znate li što je *phishing*?

U devetom pitanju su zaposlenici trebali prepoznati definiciju *phishing* napada te je veliki postotak ispitanika točno odgovorio na pitanje. Mali broj ispitanika, njih 5%, je odabralo pogrešan odgovor.

Tablica 10. Poznavanje značenja *Phishing*-a od strane zaposlenika

Ponuđeni odgovori	Odgovor	
Mrežna krađa identiteta	46,15%	162
Službena obavijest od strane odgovorne osobe	5,13%	18
Prijevara putem elektroničke pošte	79,49%	279
Računalni program koji umnožava sam sebe	25,64%	90
Sve od navedenog	5,13%	18
	Odgovoreno	**351**

Izvor: izrada autora

Slika 12. Poznavanje značenja Phishing-a od strane zaposlenika

Izvor: izrada autora

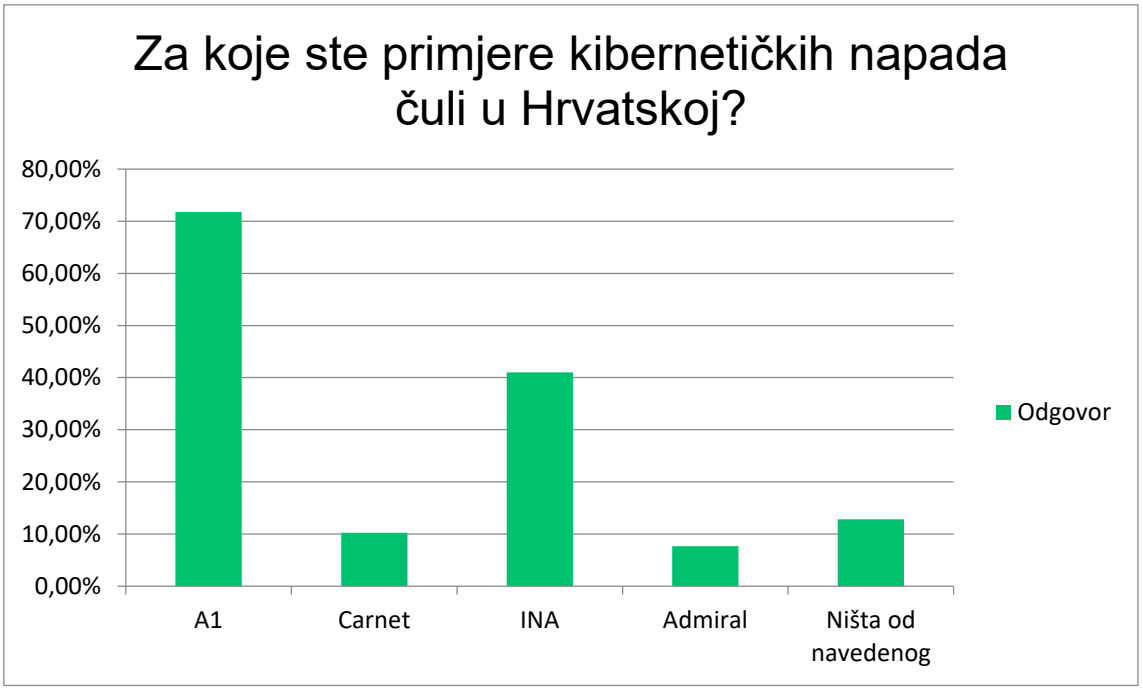
10. Pitanje: Za koje ste primjere kibernetičkih napada čuli u Hrvatskoj?

Ispitanici su naviše upoznati sa napadima na A1 (72%) i INA-u (41%) zbog nedavnih medijskih članaka vezanih za kibernetički napad, mali broj ispitanika (13%) nije upoznato sa primjerom kibernetičkog napada u Hrvatskoj.

Tablica 11. Poznavanje kibernetičkih napada u Hrvatskoj od strane zaposlenika

Ponuđeni odgovori	Odgovor	
A1	71,79%	252
Carnet	10,26%	36
INA	41,03%	144
Admiral	7,69%	27
Ništa od navedenog	12,82%	45
	Odgovoreno	**351**

Izvor: izrada autora



Slika 13. Poznavanje kibernetičkih napada u Hrvatskoj od strane zaposlenika

Izvor: izrada autora

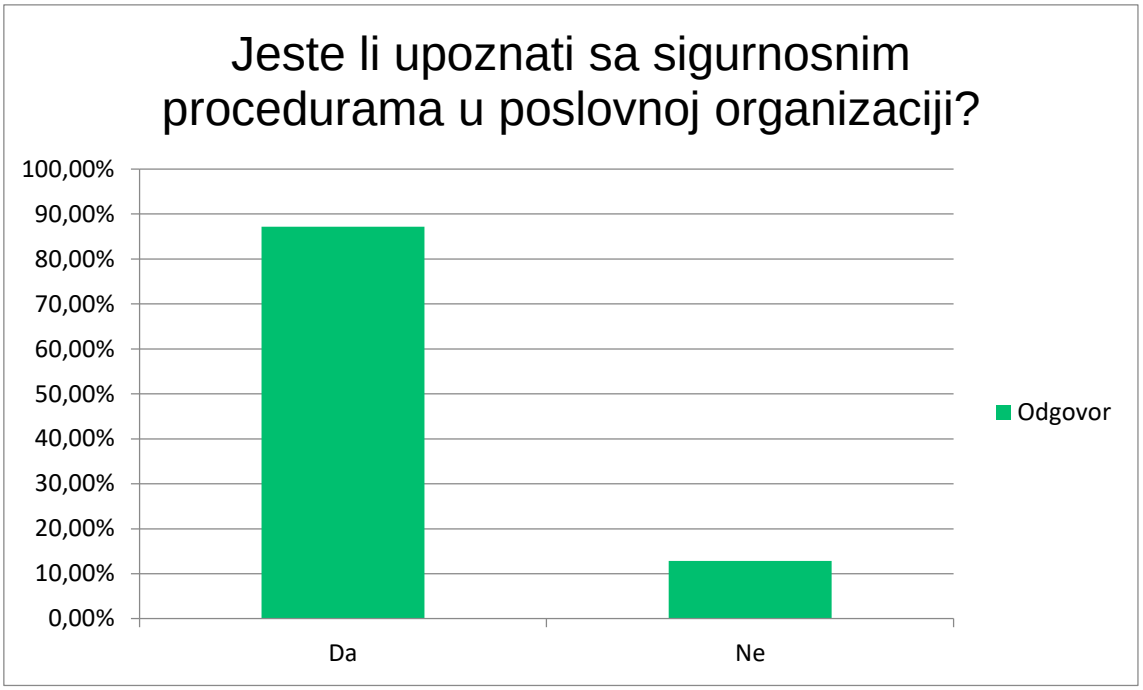
11. Pitanje: Jeste li upoznati sa sigurnosnim procedurama u poslovnoj organizaciji?

Na pitanje jesu li upoznati sa procedurama, 87% ispitanika je potvrdno odgovorilo dok je 13% odgovorili kako nisu upoznati sa sigurnosnim procedurama.

Tablica 12. Poznaju li zaposlenici sigurnosne procedure

Ponuđeni odgovori	Odgovor	
Da	87,18%	306
Ne	12,82%	45
	Odgovoreno	**351**

Izvor: izrada autora



Slika 14. Poznaju li zaposlenici sigurnosne procedure

Izvor: izrada autora

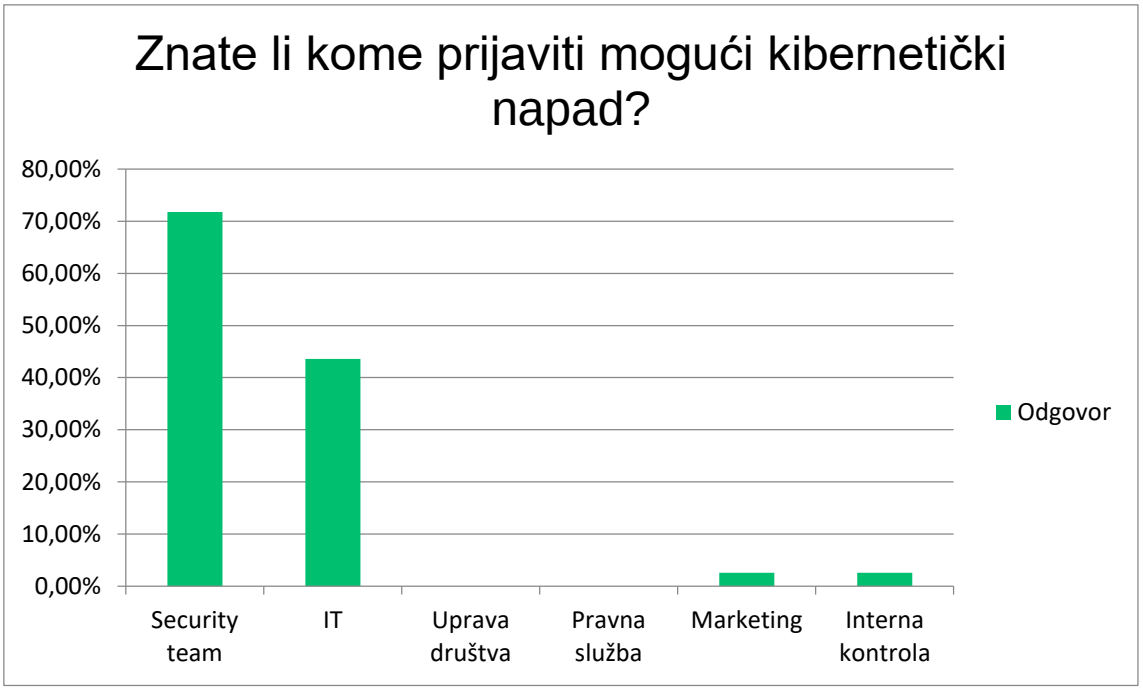
12. Pitanje: Znate li kome prijaviti mogući kibernetički napad?

U ovom pitanju je 72% zaposlenika bi kibernetički napad prijavilo Security timu, dok je 43% zaposlenika za prijavu kibernetičkog napada odabralo IT sektor. Nitko od ispitanika ne bi kibernetički napad prijavio upravi društva i pravnoj službi.

Tablica 13. Kome bi zaposlenici prijavili mogući kibernetički napad

Ponuđeni odgovori	Odgovor	
Security team	71,79%	252
IT	43,59%	153
Uprava društva	0,00%	0
Pravna služba	0,00%	0
Marketing	2,56%	9
Interna kontrola	2,56%	9
	Odgovoreno	**351**

Izvor: izrada autora



Slika 15. Kome bi zaposlenici prijavili mogući kibernetički napad

Izvor: izrada autora

13. Pitanje: Slažete li se da je sustav poslovne organizacije siguran/zaštićen?

Ispitanici su odgovorili kako je regularnost izvlačenja najsigurniji/najzaštićeniji sustav u poslovnoj organizaciji, nakon toga su financijski podaci i intranet, dok su mobilne aplikacije najmanje zaštićene.

Tablica 14. Mišljenje zaposlenika o sigurnosti/zaštićenosti sustava

Ponuđeni odgovori	Srednja ocjena
Intranet	4,11
Outlook	4
Financijski podaci	4,11
Regularnost izvlačenja	4,39
Web stranica	3,78
Mobilne aplikacije	3,59
Odgovoreno	**351**

Izvor: izrada autora

Slika 16. Mišljenje zaposlenika o sigurnosti/zaštićenosti sustava

Izvor: izrada autora

14. **Pitanje: Mislite li da poslovna organizacija dovoljno ulaže u informacijsku sigurnost?**

Po mišljenju ispitanika, poslovna organizacija naviše ulaže u *auditing*, dok se najmanje ulaže u kriptiranje.

Tablica 15. Mišljenje zaposlenika o ulaganju u informacijsku sigurnost

Ponuđeni odgovori	Srednja ocjena
Interna kontrola	3,54
Kriptiranje	3,3
Vanjska kontrola	3,38
Auditing	3,89
Ažuriranje verzija softwera	3,47
Zaštita softwera	3,5
Odgovoreno	**351**

Izvor: izrada autora

Slika 17. Mišljenje zaposlenika o ulaganju u informacijsku sigurnost

Izvor: izrada autora

15. Pitanje: Na koji način bi vaša poslovna organizacija mogla unaprijediti svoj sustav informacijske sigurnosti?

Najčešći odgovori :

- više testnih *phishing* mailova;
- više ulaganja u informacijsku sigurnost;
- više ulagati u edukacije o informacijskoj sigurnosti;
- potrebno je više provjera, edukacija i općenito ulaganja u informacijsku sigurnost;
- edukacijom zaposlenika;
- Ulaganje u nove alate vezano za *security*, specijalizirane edukacije za *security* i IT tim vezano za informacijsku sigurnost, certificiranje *security* tima vezano za informacijsku i kibernetičku sigurnost, generalne edukacije za sve zaposlenike vezano za podizanje svijesti o informacijskoj sigurnosti;
- približiti zaposlenicima načine zaštite od mogućih napada;
- boljim nadzorom postojećeg sustava i učestalijim kontrolama istog;

- za početak zaposliti vodećeg stručnjaka za informacijsku sigurnost, a kasnije eventulano i proširiti tim koji se bavi ovom problematikom kako bi sva područja njihovog rada bila adekvatno pokrivena;
- ulaganjem u pravovremeno ažuriranje software-a kako bi se spriječili kibernetički napadi, te zaštitili osjetljivi podaci.

U istraživanju je prikazana socio-demografska struktura ispitanika u tablici 16. Uzorak su činili zaposlenici: muškarci (43,6%) i žene (56,4%); najčešća dob zaposlenika je 35-44 godine, a zaposlenici su uglavnom visokoobrazovani (više od 80% ispitanika ima višu ili visoku stručnu spremu). Uzorak istraživanja je prikladan za dobivanje indikativnih rezultata, analizu te donošenja zaključaka vezanih za informacijsku sigurnost u poslovnoj organizaciji.

Tablica 16. Opis uzorka istraživanja (n = 351)

Socio-demografska struktura	**n**	**%**
SPOL		
Muški	153	43.6
Ženski	198	56.4
Ukupno	351	100
DOB		
18-24	9	2.6
25-34	81	23.1
35-44	171	48.7
45-54	63	17.9
55-64	18	5.1
65+	9	2.6
Ukupno	351	100
STRUČNA SPREMA		
NKV	9	2.6
SSS	54	15.4
VŠS	108	30.8
VSS	180	51.3
Ukupno	351	100
RADNO MJESTO		
Mlađi specijalist	36	10.3
Specijalist	72	20.5
Viši specijalist	126	35.9
Prodavač	63	17.9
Voditelj	54	15.4
Ukupno	351	100

Izvor: izrada autora

Cronbach Alpha koeficijent za anketu korištenu u ovom istraživanju. Cronbach Alpha koeficijent je mjera unutarnje dosljednosti skupa tvrdnji, a može poprimiti vrijednost između 0 i 1; što je bliže vrijednosti 1, to je mjerna ljestvica pouzdanija.

Kriteriji pouzdanosti mjernih ljestvica:

- vrijednost oko 0,9, pouzdanost se može smatrati izvrsnom
- vrijednost oko 0,8, pouzdanost se može smatrati vrlo dobrom
- vrijednosti oko 0,7, pouzdanost može smatrati prihvatljivom
- koeficijent pouzdanosti manji od 0,5 ukazuje na činjenicu da bi više od polovice opažene varijance moglo biti posljedicom slučajne pogreške, mjerne ljestvice s tako niskim koeficijentom pouzdanosti ne mogu se smatrati pouzdanima, te ih ne treba primjenjivati u daljnjoj analizi

U ovom istraživanju je Cronbach Alpha koeficijet mjeren na 6 čestica u kojima su ispitanici dali odgovore. Analizom je dobiven koeficijent pouzdanosti koji iznosi 0,844 što znači kako je vrlo dobra pouzdanost, a taj rezultat ukazuje na činjenicu da ispitanici (84 od 100) imaju isto mišljenje te su upoznati s ulaganjima poslovne organizacije u informacijsku sigurnost.

Tablica 17. Cronbach Alpha

Reliability Statistics

Cronbach's Alpha	N of Items
,844	6

Izvor: izrada autora

Tablica 17. deskriptivne metode donosi prikaz zaštite i brige o informacijskoj sigurnosti u poslovnoj organizaciji. Pojedine karakteristike bilo je moguće ocijeniti prema važnosti na ljestvici od 1 do 5. Pritom ocjena jedan (1) znači da je karakteristika manje važna, a ocjena pet (5) da je karakteristika vrlo važna. Standardna devijacija na svim pitanjima se kreće između 0,820 i 0,984. Stupac „Mean“ označava vrijednost aritmetičke sredine pojedinog elementa. Kod pitanja vezanog za brigu poslovne organizacije o informacijskoj sigurnosti je vidljivo da su zaposlenici podijeljenog mišljenja a većina ispitanika kao najveću brigu je odgovorila za auditing koji se provodi interno a zaposlenici su nedavno prolazili edukaciju te sudjeluju u internom auditu (Mean=3,89, σ = 0,969). Zaposlenici misle da je najmanja briga vezana za

kriptiranje podataka (Mean=3,30, σ = 0,984), a to proizlazi zbog nedovoljne provjere i prijava nekriptiranih mailova.

Tablica 18. Deskriptivna statistika

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Mislite li da se poslovna organizacija brine/ulaže u informacijsku sigurnost? Interna kontrola	333	2	5	3,54	,920
Kriptiranje	333	1	5	3,30	,984
Vanjska kontrola	333	1	5	3,38	,970
Auditing	342	1	5	3,89	,969
Ažuriranje verzija softwera	342	1	5	3,47	,820
Zaštita softwera	342	1	5	3,50	,912

Izvor: izrada autora

ANOVA testom i provedenom analizom varijance koja je manja od 0,05 (0,001) te standardnom devijacijom koja je u razini 1,666-1,949, rezultati analize ukazuju na to da ispitanici/zaposlenici upoznati s osnovnim aspektima informacijske sigurnosti i smatraju kako poslovna organizacija brine i ulaže podizanje razine zaštite.

Tablica 19. Anova test

Descriptive Statistics of Within-Subject Factor Levels

Dependent Variables	Mean	Std. Deviation	N	Min	Max
Kriptiranje	3,43	1,949	333	1	5
Vanjska kontrola	3,45	1,895	333	1	5
Auditing	3,95	1,890	333	1	5
Ažuriranje verzija softwera	3,55	1,666	333	1	5
Zaštita softwera	3,56	1,836	333	1	5

Izvor: izrada autora

Bayesian Estimates of Group Means[a]

		Posterior		95% Credible Interval	
Dependent Variables	Mode	Mean	Variance	Lower Bound	Upper Bound
Kriptiranje	3,43	3,43	,001	3,37	3,48
Vanjska kontrola	3,45	3,45	,001	3,39	3,51
Auditing	3,95	3,95	,001	3,90	4,01
Ažuriranje verzija softwera	3,55	3,55	,001	3,49	3,61
Zaštita softwera	3,56	3,56	,001	3,50	3,61

Izvor: izrada autora

7. Diskusija rezultata

Analizom odgovora dobivenih kroz provedenu anketu stečen je uvid u poznavanje zaposlenika s osnovnim aspektima informacijske sigurnosti te odnos stupnja obrazovanja i razine zaštite informacijskih sustava unutar poslovne organizacije, te su dani odgovori na istraživačko pitanje i hipoteze.

7.1. Interpretacija rezultata istraživanja

Analizom istraživanja potvrđene su obje postavljene hipoteze, da su zaposlenici poslovne organizacije upoznati s osnovnim aspektima informacijske sigurnosti, te da stupanj njihovog obrazovanja utječe na razinu zaštite informacijskih sustava unutar poslovne organizacije. Veliki broj ispitanika je upoznat, pored osnovnih pojmova informacijske sigurnosti, sa standardima/normama poslovne organizacije i znaju kome je potrebno prijaviti potencijalni kibernetički napad. Zaposlenici su visoko ocijenili sigurnost svih sustava poslovne organizacije i procijenili da se dovoljno ulaže u informacijsku sigurnost, te smatraju kako je i dalje potrebno primjenjivati utvrđene metode u svakodnevnom radu jer samo jedna neopreznost može rezultirati kibernetičkim probojem.

7.2. Elaboracija istraživačkog pitanja i hipoteza

Istraživačko pitanje: Utječe li znanje zaposlenika o informacijskoj sigurnosti na razinu zaštite informacijskih sustava unutar poslovne organizacije?

Analizom prikupljenih podataka potvrđeno je da zaposlenici poslovne organizacije koji posjeduju znanje o informacijskoj sigurnosti znaju kako prepoznati pokušaj kibernetičkog napada, zaštititi podatke poslovne organizacije i kojim odjelima prijaviti sumnju u kibernetički napad te tako prevenirati napad. Slijedom navedenog, odgovor na istraživačko pitanje je: Znanje zaposlenika o informacijskoj sigurnosti utječe na razinu zaštite informacijskih sustava unutar poslovne organizacije.

Hipoteze:

H1: Zaposlenici su upoznati s osnovnim aspektima informacijske sigurnosti unutar poslovne organizacije.

Primjenom alata poslovne inteligencije kroz anketni upitnik i obradom prikupljenih podataka IBM-ovim SPSS alatom dobiveni su rezultati koji potvrđuju da su zaposlenici upoznati s osnovnim aspektima informacijske sigurnost ponajprije zbog internog audita u kojem sami sudjeluju, te kroz odgovore koji ukazuju na poznavanje metoda zaštite informacijskih sustava unutar poslovne organizacije. Slijedom navedenog, postavljena hipoteza H1 potvrđena.

H2: Stupanj obrazovanja zaposlenika utječe na razinu zaštite informacijskih sustava unutar poslovne organizacije

Primjenom alata poslovne inteligencije kroz anketni upitnik i obradom prikupljenih podataka IBM-ovim SPSS alatom dobiveni su rezultati koji potvrđuju da ispitanici s većim stupnjem obrazovanja imaju više znanja o informacijskoj sigurnosti od ispitanika s nižim stupnjem obrazovanja. Također možemo utvrditi da razina znanja kod visokoobrazovanih ispitanika nadmašuje razinu poznavanja osnovnih aspekata informacijske sigurnosti. Slijedom navedenog, postavljena hipoteza H1 potvrđena.

7.3. Primjena rezultata i preporuke

Istraživanjem je utvrđeno kako je veliki broj zaposlenika unutar poslovne organizacije upoznat s osnovama informacijske sigurnosti i ima razvijenu svijest o važnosti zaštite informacija, što je direktan utjecaj efektivnog ulaganja u educiranje djelatnika. Istraživanje u ovom radu bilo je koncentrirano na procjenu znanja zaposlenika o osnovnim aspektima informacijske sigurnosti te utvrđivanje korelacije između stupnja obrazovanja zaposlenika i njihovog poznavanja metoda zaštite informacijskih sustava.

Preporuka ne temelju dobivenih rezultata glasi kako bi poslovna organizacija trebala uključiti što više zaposlenika u provođenje internog audita, te kontinuirano ulagati u obrazovanje zaposlenika o informacijskoj sigurnosti kroz interne ili vanjske edukacije od strane certificiranih osoba.

Sigurnost informacijskog sustava bi se trebala periodično kontrolirati, poslovna organizacija bi trebala tražiti načine kako sustav učiniti još sigurnijim, otpornijim te implementirati dodatne sigurnosne kontrole koje savjetuju stručnjaci za informacijsku sigurnost.

Poslovne organizacije trebaju razmišljati o više ključnih stavki ukoliko se žele uspješno zaštititi od kibernetičkih napada i prijetnji. Sastavljanje jasnih uputa svim zaposlenicima, poticanje na međusobnu komunikaciju te dijeljenje informacija u poslovnoj organizaciji od iznimne je važnosti. Zaposlenici trebaju sudjelovati korištenjem kompleksnih lozinki te dvostrukom autentifikacijom. Redovito ažuriranje i nadograđivanje informacijskih sustava.

8. Zaključak

U današnjem poslovanju informacijski sustavi se smatraju jako važnim dijelom poslovanja jer se svaki poslovni sustav sastoji od skupa povjerljivih informacija kojima upravlja informacijski sustav. Prikupljanjem i obradom tih informacija postiže se temelj za donošenje odluka koji utječu na cjelokupno poslovanje. Jedan od najvažnijih ciljeva svake organizacije je osiguranje neprekinutosti odnosno kontinuiteta poslovanja. Kontinuitet poslovanja u današnje vrijeme ovisi o faktorima koji na njega utječu, jedan od tih faktora dakako je informacijska sigurnost tj. zaštita podataka i ostalih resursa u poslovanju. Informacijska sigurnost je proces, što znači da se neprekidno razvijaju i unaprjeđuju novi sustavi zaštite informacijskog sustava.

U ovom diplomskom radu su prikazane osnove za uspostavu i zaštitu informacijskog sustava od mogućih kibernetički napada na organizaciju. Činjenica je da postoji određena razina opasnosti za sustav pogotovo u suvremenom poslovanju pa organizacije moraju biti toga svjesne i biti spremne na reakciju protiv mogućih prijetnji. Odabirom pravog i odgovarajućeg informacijskog sustava za poslovanje te briga i zaštita informacijskog sustava bitno utječe na cjelokupno poslovanje neke organizacije, ali je potrebno konstantno provjeravati rad sustava radi održavanja uz prihvatljive razine rizika. Modernizacijom i informatizacijom poslovanja sigurnosni rizik se povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi konkurentnost poslovne organizacije. Ukoliko se zanemari sustav informacijske sigurnosti te ukoliko poduzeće nije u mogućnosti kontrolirati problem sigurnosti, vrlo lako može postati žrtva napada.

Pošto poslovne organizacije, kao i društvo općenito, uvelike ovise o modernim tehnologijama i internetu za potrebe svog poslovanja, potrebno je unaprijed isplanirati zaštitu računalnih sustava i mreža poduzeća kako bi se smanjio rizik od gubitka ili kompromitiranja osjetljivih poslovnih ili korisničkih informacija.

9. Popis literature

1. Aytakin Nazim Ibrahimova : The definitions of information and security ; History of information security development, Baku State University 2020; https://www.zurnalai.vu.lt/open-series/article/view/22387/21645 pristupljeno 18.06.2022.
2. Andrijanić, I. Buntak, K., Bošnjak, M. : Upravljanje kvalitetom s poznavanjem robe, Visoka poslovna škola Libertas, Zagreb, 2012.
3. Bogati, J., NORME INFORMACIJSKE SIGURNOSTI ISO/IEC 27K ,Praktični menadžment, Vol. II, br. 3, 2011.
4. Böhme, R. : Cyber-Insurance Revisited, Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA, 2005.
5. CRN, australski web portal; https://www.crn.com.au/news/10-reasons-why-iso-27001-makes-a-better-is-security-professional-152262, pristupljeno 20.06.2022.
6. COBIT - www.isaca.org/cobit, pristupljeno 21.06.2022.
7. Det Norske Veritas : Priručnik za polaznike ISO 27001 Seminar za interne auditore ver 6.1 © 2013 DNVGL Business Assurance
8. Dujella A., Maretić M. : Kriptografija, Element, Zagreb, 2007.
9. Galinec, D., Luić, Lj. : Design of Conceptual Model for Raising Awareness of Digital Threats, WSEAS transactions on environment and development, 2020.
10. Galinec, D., Luić, Lj. : Digital Security Perspectives and Engagement for Resilience in Information-Communication Environment, Proceedings 2019 3rd European Conference on Electrical Engineering & Computer Science (EECS), 2019.
11. GDPR - EU Opća uredba o zaštiti podataka, https://www.privacy-regulation.eu/hr/r6.htm, pristupljeno 20.06.2022.
12. Gordon, L. A., Loeb, M. P. i Sohail, T. : A framework for using insurance for cyber-risk management, Communications of the ACM, God. 46., Br. 3, 2003.
13. Grimes, R, A. : Fixing the #1 Problem in Computer Security: A Data-Driven Defense, Independently Published, 2017.
14. Hoglund, G. & Butler, J. : Rootkits: Subverting the Windows Kernel. NJ, Addison-Wesley Professional, 2006.
15. Honigman, B. : 4 Ways Your Small Business Can Better Prevent Cyber Crime, 2015. https://www.entrepreneur.com/article/245102, pristupljeno 25.06.2022.

16. Horvat, A. : Javno i tajno u knjižničarskoj struci. Arhivi, knjižnice, muzeji: mogućnosti suradnje u okruženju globalne informacijske infrastrukture: zbornik radova, 2002.
17. Identity Theft Resource Center - https://www.idtheftcenter.org/post/what-the-new-2019-data-breach-report-means-for-your-identity/, pristupljeno 20.08.2022.
18. INA – https://www.ina.hr/obavijest-o-kibernetickom-napadu/, pristupljeno 15.07.2022.
19. Johns, E. : Cyber Security Breaches Survey, London: Department for Digital, Culture, Media & Sport, 2020.
20. Khanse, A. : Why would someone want to hack my computer? 2017. https://www.thewindowsclub.com/why-someone-want-hack-computer pristupljeno 20.06.2022.
21. Kostanjevec A. et al.: Sigurnost informacijskih sustava, Varaždin 2014.
22. Kovač, D. : Ulaganje u kibernetičku sigurnost, Zbornik radova Veleučilišta u Šibeniku, Vol. 15(1-2), pp. 61-73, 2021.
23. Krakar Zdravko i suradnici; Korporativna informacijska sigurnost, Fakultet organizacije i informatike Varaždin 2014.
24. Lelarge, M. i Bolot, J. : A local mean fi eld analysis of security investments in networks. In Proceedings of the 3rd international workshop on Economics of networked systems, 2008.
25. Luić Lj.: Informacijski sustavi, Veleučilište u Karlovcu, Karlovac 2009.
26. Luić, Lj., Švelec-Juričić, D., Mišević, P. : The Impact of Knowledge of the Issue of Identification and Authentication on the Information Security of Adolescents in the Virtual Space , WSEAS Transactions on Systems and Control, 2021.
27. Malwarebytes. (n.d.). Malware. https://www.malwarebytes.com/malware pristupljeno 20.06.2022.
28. Malwarebytes. (n.d.). Ransomware. https://www.malwarebytes.com/ransomware pristupljeno 20.06.2022.
29. Malwarebytes. (n.d.). What is phishing? https://www.malwarebytes.com/phishing pristupljeno 20.06.2022.
30. Međunarodna organizacija za standardizaciju (ISO), https://www.iso.org/home.html pristupljeno 10.06.2022.,

31. Mueller J. : Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija, Ekonomski pregled, Vol. 52, 2001.
32. Mukhopadhyay, A.; Saha, D., Chakrabarti, B. B., Mahanti, A., i Podder, A. Insurance for cyber-risk: A Utility Model. Decision, God. 32., Br. 1, 2005.
33. Nacionalni CERT, pristupljeno 15.06.2022., http://www.cert.hr/onama
34. Narodne novine, Zakon o informacijskoj sigurnosti, NN 79/07, https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html pristupljeno : 18.06.2022.
35. National Library of Medicine - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/, pristupio 10.07.2022.
36. Porter, K. : What is phishing? How to recognize and avoid phishing scams, 2020. https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html pristupljeno 20.06.2022.
37. Popat, A. : Five Ways To Protect Your Company Against Cyber Attacks, 2018. pristupljeno 25.06.2022., https://www.entrepreneur.com/article/316886
38. Schepman, T., Koren, M., Horvat, A., Kurtovic, D., Grgić, I. H. (2008). Access With(out) Anonymity. U 16th BOBCATSSS Symposium 2008.
39. Šehanović J. et al.: Informatika za ekonomiste, Sveučilište u Rijeci, Pula 2002.
40. The Future Decade of the EU Law, 8th International Conference of PhD Students and Young Researchers, 2020.
41. Ured vijeća za nacionalnu sigurnost, http://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost pristupljeno 18.06.2022.
42. Večernji list, https://www.vecernji.hr/vijesti/hakeri-napali-kutinsku-petrokemiju-otezana-elektronicka-komunikacija-1524004 pristupljeno 01.07.2022.
43. Zavod za sigurnost informacijskih sustava, https://www.zsis.hr/, pristupljeno 15.06.2022.
44. WLA-SCS:2020 – © WLA 2020 – Publication: October 2020, Version 1.1 (Revised: December 10, 2020) https://www.world-lotteries.org/volumes/downloads/Download_Center/Security/WLA_SCS_2020/202012_EN_WLA-SCS-2020_Standard_V1-2.pdf, pristupljeno 14.06.2022.

POPIS SLIKA

POPIS TABLICA

MJERNI INSTRUMENT

Mjerni instrument na temelju kojeg je provedeno istraživanje :

Upitnik - anketna pitanja

1. Pitanje : Spol
2. Pitanje : Dob
3. Pitanje : Stručna sprema
4. Pitanje : Radno mjesto
5. Pitanje : U kojem sektoru unutar organizacija ste zaposleni?
6. Pitanje : Što je za Vas informacijska sigurnost?
7. Pitanje : S kojim ste standardima/normama upoznati u informacijskoj sigurnosti?
8. Pitanje : Koje vrste kibernetičkog napada poznajete?
9. Pitanje : Znate li što je *phishing*?
10. Pitanje : Za koje ste primjere kibernetičkih napada čuli u Hrvatskoj?
11. Pitanje : Jeste li upoznati sa sigurnosnim procedurama Hrvatske Lutrije?
12. Pitanje : Znate li kome prijaviti mogući kibernetički napad?
13. Pitanje : Slažete li se da je sustav Hrvatske Lutrije siguran/zaštićen?
14. Pitanje : Mislite li da se Hrvatska Lutrija dovoljno brine/ulaže u informacijsku sigurnost?
15. Pitanje : Na koji način bi Hrvatska Lutrija mogla unaprijediti svoj sustav informacijske sigurnosti?

Prilog 1. Anketni upitnik

Poznavanje informacijske sigurnosti u poslovnoj organizaciji

1. Spol

- M
- Ž

2. Dob

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

3. Stručna sprema

- NKV
- SSS
- VŠS
- VSS

4. Radno mjesto

- Mlađi specijalist
- Specijalist
- Viši specijalist
- Prodavač
- Voditelj

5. U kojem sektoru unutar poslove organizacije ste zaposleni?

- Razvoja poslovanja i marketinga
- Prodaja
- Logistika
- Priprema i razvoj igara
- Financije
- Ured uprave

6. Što je za Vas informacijska sigurnost?

- [ ] Kriptiranje dokumenata
- [ ] Brisanje neželjene pošte
- [ ] Prijava malicioznih sadržaja
- [ ] Ažuriranje softwera
- [ ] Prepoznavanje mogućih kibernetičkih napada
- [ ] Sve od navedenog

7. S kojim ste standardima/normama upoznati u informacijskoj sigurnosti? (moguće je odabrati više odgovora)

- [ ] ISO 27001
- [ ] ISO 27002
- [ ] WLA
- [ ] SOC
- [ ] GDPR

8. Koje vrste kibernetičkog napada poznajete?

- [ ] Phishing
- [ ] DDOS
- [ ] WORM
- [ ] Bot Net

9. Znate li što je phishing?

- [ ] Mrežna krađa identiteta
- [ ] Službena obavijest od strane odgovorne osobe
- [ ] Prijevara putem elektroničke pošte
- [ ] Računalni program koji umnožava sam sebe
- [ ] Sve od navedenog

10. Za koje ste primjere kibernetičkih napada čuli u Hrvatskoj?

- [ ] A1
- [ ] Carnet
- [ ] INA
- [ ] Admiral
- [ ] Ništa od navedenog

11. Jeste li upoznati sa sigurnosnim procedurama u poslovnoj organizaciji?

- ( ) Da
- ( ) Ne

12. Znate li kome prijaviti mogući kibernetički napad?

- [ ] Security team
- [ ] IT
- [ ] Uprava društva
- [ ] Pravna služba
- [ ] Marketing
- [ ] Interna kontrola

13. Slažete li se da je sustav poslovne organizacije siguran/zaštićen?

	1 (U potpunosti se ne slažem)	2	3	4	5 (U potpunosti se slažem)
Intranet	○	○	○	○	○
Outlook	○	○	○	○	○
Financijski podaci	○	○	○	○	○
Regularnost izvlačenja	○	○	○	○	○
Web stranica	○	○	○	○	○
Mobilne aplikacije	○	○	○	○	○

14. Mislite li da poslovna organizacija dovoljno ulaže u informacijsku sigurnost?

	1 (U potpunosti se ne slažem)	2	3	4	5 (U potpunosti se slažem)
Interna kontrola	○	○	○	○	○
Financiranje projekata	○	○	○	○	○
Vanjska kontrola	○	○	○	○	○
Auditing	○	○	○	○	○
Ažuriranje verzija softwera	○	○	○	○	○
Zaštita softwera	○	○	○	○	○

15. Na koji način bi vaša poslovna organizacija mogla unaprijediti svoj sustav Informacijske sigurnosti?

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, JOSIP TOTH *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom INFORMACIJSKA SIGURNOST I ZAŠTITA OD KIBERNETIČKOG NAPADA *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

Josip Toth
(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, JOSIP TOTH *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom INFORMACIJSKA SIGURNOST I ZAŠTITA OD KIBERNETIČKOG NAPADA *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)

Josip Toth
(vlastoručni potpis)