Cyber sigurnost u poslovnim informacijskim sustavima

Bubnjić, Jelena

Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni prijediplomski studij *(Ekonomija i poslovna ekonomija)*

Jelena Bubnjić

CYBER SIGURNOST U POSLOVNIM INFORMACIJSKIM SUSTAVIMA

Završni rad

Osijek, 2024.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni prijediplomski studij *(Ekonomija i poslovna ekonomija)*

Jelena Bubnjić

CYBER SIGURNOST U POSLOVNIM INFORMACIJSKIM SUSTAVIMA

Završni rad

Kolegij: Poslovni informacijski sustavi

JMBAG: 0010236211

e-mail: jbubnjic@efos.hr

Mentor: Prof.dr.sc., Jerko Glavaš

Komentor: Bruno Mandić, mag.oec.

Osijek, 2024.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
Undergraduate Study *(Economics and business economics)*

Jelena Bubnjić

CYBER SECURITY IN BUSINESS INFORMATION SYSTEMS

Final paper

Osijek, 2024.

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je ZAVRŠNI RAD (navesti vrstu rada: završni/diplomski/specijalistički/doktorski) rad isključivo rezultat osobnoga rada koji se temelji na vlastitim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska.* (cc) BY-NC-SA
3. Kojom izjavljujem da sam suglasan/suglasna trajnom pohranjivanju i objavljivanju mog rada u Institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, Repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom Repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).
4. Izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan s dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Jelena Bubnjić

JMBAG: 0010236211

OIB: 65839802092

e-mail za kontakt: jelena.bubnjic123@gmail.com

Naziv studija: Ekonomija i poslovna ekonomija

Naslov rada: Cyber sigurnost u poslovnim informacijskim sustavima

Mentor/mentorica rada: Prof.dr.sc., Jerko Glavaš

U Osijeku, 06. rujna 2024. godine

Potpis Jelena Bubnjić

Cyber sigurnost u poslovnim informacijskim sustavima

SAŽETAK

Poslovni informacijski sustavi u današnjem vremenu su u većem dijelu digitalizirani, te samim time podatci koji se nalaze u računalnim sustavima mogu biti izloženi riziku za nekom od vrsta *cyber* napada. Ti podatci su važni pri donošenju odluka koje će usmjeravati poslovni subjekt prema njihovoj budućnosti na tržištu. Sigurnost poslovnih informacijskih sustava je važna iz više aspekata, kako za zaposlenike u vidu očuvanju njihove sigurnosti, tako i za osiguranje povjerljivosti i sigurnosti podataka korisnika odnosno potrošača. Cilj rada je istraživanje koliko su sigurni poslovni sustavi, te koje prijetnje se nadziru u poslovanju s velikim brojem važnih podataka. Teorijska podloga završnog rada je proizašla iz informacija različitih vrsta znanstvene i stručne literature, te knjiga i internetskih izvora. Kroz analizu i sintezu, usporedbu različitih izvora, dedukcije donošenja zaključaka rada, vidljivo je kako cyber napadi predstavljaju prijetnju poslovanju. Neke od nedostataka kod narušavanja *cyber* sigurnosti su potencijalni financijski gubitci i narušavanje ugleda same tvrtke. Kroz provedene analize važno je naglasiti kako je edukacija zaposlenika od iznimne važnosti i jedna od stavki u koju se isplati i mora ulagati. Povećanje svijesti edukacijom zaposlenika je jedna od prednosti same edukacije, ali i sigurnost kod zaposlenika prilikom rada. Ovaj rad može biti koristan svim zainteresiranim osobama u području zaštite poslovnih informacijskih sustava.

Ključne riječi: sigurnost, poslovni informacijski sustavi, zaposlenici, edukacija, cyber napadi i rizik.

Cyber Security in Business Information Systems

ABSTRACT

Business information systems today are largely digitalized, making the data stored within these systems susceptible to various types of cyber attacks. This data is crucial for decision-making processes that guide the future direction of a business in the market. The security of business information systems is important from multiple perspectives, including protecting employees and ensuring the confidentiality and security of user and consumer data. This paper aims to investigate the security of business systems and identify the threats present in operations involving significant amounts of important data. The theoretical basis of the thesis is derived from a variety of scientific and professional literature, as well as books and online sources. Through analysis and synthesis, comparison of different sources, and deductive reasoning, it is evident that cyber attacks pose a threat to business operations. Some of the negative consequences of compromised cyber security include potential financial losses and damage to the company's reputation. The conducted analyses highlight the importance of employee education as a critical area of investment. Increasing awareness through employee education is a key advantage, providing security for employees during their work. This paper can be useful to anyone interested in the field of business information systems security.

Keywords: security, business information systems, employees, education, cyber-attacks and risk.

SADRŽAJ:

1. UVOD

Poslovni informacijski sustavi su od velike važnosti za tvrtke. Zaštita podataka ima ključnu ulogu u osiguranju integriteta poslovanja i lojalnosti koju potrošači imaju prema toj organizaciji. Rad ima za cilj istražiti područje prijetnji u poslovnim informacijskim sustavima. Informacije su ključne za donošenje odluka u tvrtkama, te njihova zaštita je od velike važnosti za nastavak neometanog poslovanja i sprječavanja velikih financijskih gubitaka, ali i gubitaka povjerenja klijenata i naposljetku samog ugleda tvrtke.

U samom radu istražuju se i identificiraju *cyber* napadi, pod kojim sve vrstama je moguće uočiti ovakvu vrstu napada, koje posljedice se odražavaju na samu tvrtku, te metode primjene u zaštiti poslovnog sustava. Svrha rada je pružiti detaljan pregled prijetnji koje ugrožavaju poslovanje, te koje mogu oštetiti tvrtku privremeno ili trajno, ovisno o samoj vrsti napada. Nadalje je potrebno naglasiti važnost koje imaju metode i strategije kojima se štite sustavi. Kroz analizu različitih metoda zaštite, radom se želi povećati svijest o važnosti informacijske sigurnosti među zaposlenicima u poslovnom okruženju, te potaknuti važnost edukacije u razdoblju kada digitalizacija sve više napreduje.

2. METODOLOGIJA RADA

Svrha završnog rada je proučavanje *cyber* sigurnosti u poslovnim informacijskim sustavima. U samom postupku izrade rada korištena je literatura koja je sadržavala znanstvene i stručne akademske članke, knjige, službene internetske izvore, izvještaje stručnjaka iz područja poslovne informacijske sigurnosti, te Zakon o kibernetičkoj sigurnosti. Korištene metode u radu su bile metoda analize i sinteze autora kako bi se razumjela složenost i važnost teme, te objedinile informacije o *cyber* sigurnosti u poslovnim informacijskim sustavima. Korištene metode su i metoda usporedbe različitih autora, kako bi se vidjele sličnosti i razlike u temi. Metoda dedukcije s kojom se dolazilo do razumijevanja problema te donošenja zaključaka. Jedna od korištenih metoda je i analiza učinka koju edukacija ima na zaposlenike u razvijanju njihove svijesti i vještina. Cilj rada se definira kroz objašnjenje koliko je poslovanje u riziku od *cyber* napada, te da je vrlo bitan potencijalni problem u digitalnom svijetu osim *cyber* napada i zaposlenici koji moraju biti educiraniji, kako bi sustav poslovanja bio siguran.

3. POSLOVNI INFORMACIJSKI SUSTAVI

Poduzeća u današnje vrijeme donose jako puno promjena sa sobom. Svaka tvrtka ima svoj informacijski sustav koji im omogućuje pohranu, analizu i korištenje jako velikog broja informacija. Informacijski sustav tvrtke omogućava bolju produktivnost rada i bržu integraciju podataka. Prema Garača (2008). na temelju tih podataka, osigurava se temelj za buduće donošenje poslovnih odluka.

Hardcastle (2008). opisuje ulogu informacijskog sustava kao pružatelja informacija menadžmentu organizacije s pomoću kojih će donositi odluke neophodne za nastavak poslovanja i kontrolu nad tvrtkom. Poslovni informacijski sustavi se mogu opisati kao skup međusobno povezanih elemenata koji obavljaju razne zadaće u koje su uključene prikupljanje, obrada, pohrana, izlaz te kontrola podataka. Cilj poslovnog informacijskog sustava je da sve te neobrađene informacije pretvori u korisne podatke koji će biti važni za organizaciju.

Garača (2008). objašnjava da je upravljanje sustavom poslovanja povezano sa:

- planiranjem – u ovom procesu važno je definirati ciljeve, odnosno koje zadaće će tvrtka poduzeti kako bi ostvarila svoje potrebe.
- Organiziranjem – u procesu ostvarivanja cilja svake tvrtke potrebno je propisati i ispuniti određena pravila, odnosno na koji način i uz koja sredstva doći do cilja.
- Kontroliranjem – vrlo bitna stavka u ostvarenju cilja, jest da se pravovremenim kontrolama smanji i u potpunosti otkloni mogućnost nastanka problema.

Poslovni informacijski sustavi koriste informacijsku tehnologiju kao što su računala. Hardcastle (2008). objašnjava da iza toga stoje valjani razlozi poput točnosti podataka, brzina u prijenosu informacija te vjerodostojnost istih. Ove tri odlike su jednako važne kao i zapošljavanje osoba koje su sigurne i pouzdane. Zaposlenici tvrtke koji rade s vrlo značajnim podatcima obvezni su te podatke i čuvati, gdje je u praksi postojao slučaj gdje su organizacije manipulirale svojim resursima kako bi istražile više o svojim konkurentima u poslovnom svijetu, odnosno uhodile druge organizacije.

Dvije glavne funkcije poslovnih informacijskih sustava koje navodi Štefanić (2021). su:

- operativne funkcije,
- informacijske funkcije.

Operativne funkcije su usmjerene ka izvršenju bolje učinkovitosti sustava PIS-a, njihov cilj je kada operativne funkcije budu uspješno izvršene, one će olakšati zaposlenicima da obave posao na precizan način. S druge strane informacijske funkcije preuzimaju ulogu pohrane podataka, lakši pristup podatcima te generiranje izvještaja koji su potrebni.

3.1. Vrste poslovnih informacijskih sustava

Autori Srića i Spremić (2000). u svojoj knjizi podijelili su poslovne informacijske sustave na sljedeći način:

- klasični,
- sustav za potporu odlučivanja,
- ekspertni sustav.

Garača (2008). opisuje ekspertni sustav kao softverski sustav čija je ideja jednostavna. U ekspertnom sustavu postoje zaposlenici čije je znanje stečeno kroz godine, odnosno obrazovanjem, zatim znanje koje je zaposlenik stekao prilikom svog poslovanja, te proceduralno znanje. Glavna zamisao ekspertnih sustava jest da se sve znanje preuzme od eksperata, prenese ga u softver i pohrani u računalu, gdje ga kasnije mogu zaposlenici rabiti i analizirati te pomagati u rješavanju problema. Ćurko (2001). navodi kako je glavna uloga sustava potpore odlučivanju da osigura visokokvalitetne informacije koje će kasnije poslužiti menadžmentu u donošenju odluka. Klasični sustav još se naziva i transakcijski informacijski sustav. Vidaković (2021). u svom završnom radu objašnjava da je transakcijski sustav ključni dio organizacije koji se odnosi na operativni menadžment. Transakcijski sustav se može opisati kao voditelj evidencije o poslovnim aktivnostima.

Sve tri komponente čine jedan cjelovit poslovni sustav i mogu se poistovjetiti s razinama menadžmenta, po hijerarhiji. Klasični informacijski sustavi bi bila operativna razina menadžmenta, sustav za potporu odlučivanja bi bila taktička razina menadžmenta, dok bi ekspertni sustav bio najviša razina menadžmenta, a to je strateški menadžment.

Ove vrste poslovnih informacijskih sustava zahtijevaju plan i razvoj sigurnosnih mjera kako bi se zaštitili podatci, osigurao integritet, odnosno točnost te dostupnost podataka od *cyber* napada ili prijetnji. Neadekvatna, odnosno nedovoljno dobra zaštita sustava može dovesti do stvarnih oštećenja tvrtke, njezine reputacije i ugleda te gubitka povjerenja njenih klijenata.

3.2. Dijelovi poslovnih informacijskih sustava

Dijelovi jednog poslovnog informacijskog sustava koje navodi Hardcastle (2008). su sljedeće:

- *hardware*,
- *software*,
- *lifeware*,
- *netware*,
- *orgware*.

Hardware predstavlja materijalni dio informacijskih sustava. Postoji pet grupa prema kojima se dijeli *hardware.* Garača (2008). dijeli komponente na centralnu jedinicu, u koju se svrstavaju procesor, memorija i drugi. Nakon toga opisuje ulaznu jedinicu gdje se svrstavaju skeneri, miš, tipkovnica kojima se koriste zaposlenici za unošenje potrebnih podataka u računala. Izlazne jedinice jesu one s pomoću kojih dobijemo podatke na uvid, a u koje se ubraja ekran i printer. Vanjska memorija podrazumijeva magnetski disk. U zadnju komponentu, koja se naziva mrežna komponenta, ubrajaju se modemi, koncentratori i drugo.

Software nije materijalna komponenta, jer sadrži prema Garača (2008). znanje ljudi kojima će pomoći u rješavanju složenih programskih problema. Postoje dvije vrste *software*-a koje je Hardcastle (2008). podijelila na: sistemski i aplikacijski. Sistemski *software* nadgleda rad računalnog sustava prilikom izvršavanja zadataka koje mu postavi zaposlenik. Aplikacijski *software* čini sveukupnost programa koji omogućavaju rješavanje problema poslovnih sustava.

Lifeware se može opisati kao vrsta poslovnog informacijskog sustava koju čini čovjek. Galičić i Ivanović (2008). opisuju lifeware kao sastavnicu svih ljudi, odnosno zaposlenika u organizacijama koji sudjeluju u rabljenju informacija. *Netware* predstavlja telekomunikacijski sustav s pomoću kojeg se dalje prenose bitne informacije. Osim toga vrlo je bitno naglasiti kako je on sastavnica *hardware*-a i *software*-a, te čini mogućom komunikaciju i razmjenu podataka unutar mreže.

Orgware je ključna organizacijska komponenta, koja obuhvaća sve dijelove kojima se upravljaju procesi i ljudi unutar jedne organizacije. Galičić i Ivanović (2008). objašnjavaju kako on sadrži potrebne metode koje se koriste za koordinaciju *hardware*-a, *software*-a i drugih podataka, kako bi se zaokružila cjelina koja će podržati sve ciljeve i procese koje ima organizacija. Glavna zadaća *orgware*-a je ta da se iskoristi potencijal informacijskih tehnologija, te pomogne u izvršavanju zadaća kako bi se postigli ciljevi poslovanja.

3.3. Razvoj poslovnih informacijskih sustava

Poslovni informacijski sustavi nisu važni samo za zaposlenike, već i za menadžere. Kako se svijet razvija, tako se i sustav poslovanja mijenja, danas se ne može zamisliti poslovanje bez korištenja informacijskih sustava. Težak (2002). objašnjava kako je zapravo dvadeseto stoljeće bila prekretnica, gdje su ljudi morali prihvatiti i početi se prilagođavati na novim situacijama. U današnje doba važno je i potrebno za zaposlenike da budu informacijski pismeni. Važno je naglasiti kako Težak (2002). odvaja pojmove informacijska pismenost i tehnologija. Informacijska pismenost se može okarakterizirati prema Vrkić Dimić (2014). kao širi pojam vezan uz pristup, interpretiranje i korištenje informacija, dok Galičić i Ivanović (2008). objašnjavaju informacijsku tehnologiju kao ne samo alat, već glavni čimbenik kojim se oblikuje organizacijska kultura. Za uspješno i sigurno poslovanje potrebno je biti informacijski pismen, znati iskorištavati podatke i s pomoću njih rješavati zadatke, i imati kvalitetnu podlogu tehnologija, koje će pomoći u brzom i točnom rješavanju. Razvoj informacijskih sustava prema Hardcastle (2008). je sljedeći:

- faza inicijacije – utvrđuje se prilikom prvog koraka je li novi informacijski sustav potreban, ali i isplativ kako bi ga se uspješno provelo.
- Procjena izvedivosti – na početku je također bitno utvrditi ekonomsku i tehničku izvedivost projekta razvoja informacijskih sustava. Tehnička izvedivost odgovara na pitanje podržava li tehnologija sustav koji se želi razviti, dok ekonomska odgovara na pitanje koliko novca će se potrošiti.
- Analiza sustava – procjenjuju se zahtjevi koju korisnici imaju za sustav, nakon što su prethodne dvije faze provedene, odnosno definira se što se želi ugraditi u sustav.
- Dizajn sustava – odnosi se na sve ono što će sustav isporučiti krajnjem korisniku u smislu njegovih zahtjeva, te kako će sučelje izgledati.
- Izgradnja sustava – ova faza uključuje programiranje i stvaranje *softwarea* od strane programera te testiranje njegovog rada.
- Implementacija sustava – predstavlja promjenu sustava, odnosno faza u kojoj se želi vidjeti postoji li greška kako bi se pravovremeno otklonila.
- Pregled i održavanje sustava – kako bi se prilagodio na poslovni sistem, sustav će se s vremena na vrijeme morati održavati i ažurirati, gdje će sustav dobiti nove značajke koje će pomoći u sigurnom poslovanju.

Tehnologija koje je u razvoju, a koja se bazira na smanjenje nepodudarnosti na tržištu je *blockchain*, kako navodi Lozić i suradnici (2023). ta vrsta tehnologije omogućava odvijanje, razmjenu informacija bez potrebe za posrednicima na tržištu. *Blockchain* je u svojim početcima bio vezan uz kriptovalute, a najpoznatiji je bio po *Bitcoinu*, no prema mišljenu Lozića i suradnika (2023). kako je vrijeme prolazilo tako je postojala potreba da se tehnologija proširi, odnosno da se iskoristi potencijal koji donosi *blockchain* u poslovanju.

Prema Harvard *Business Review* (2022). rad *blockchaina* se temelji na:

- distribuiranoj bazi podataka – u poslovnom procesu svi imaju priliku vidjeti bazu podataka kao i povijest podataka. Svaka strana može provjeriti podatke i transakcije, ali ih nitko ne smije kontrolirati i mijenjati.
- *Peer-to-peer* prijenosu – u komunikaciji i prijenosu podataka postoji čvor, putem kojega se prosljeđuju informacije njihovim primateljima.
- Transparentnosti pseudonima – korisnici i čvorovi na *blockchain* adresi mogu ostati anonimni ili mogu odati svoj identitet, a te transakcije se odvijaju putem *blockchain* adrese.
- Nepovratnosti zapisa – nakon što se unese transakcija u bazu podataka, zapisi se ne mogu mijenjati. Razlog tomu je što je svaki zapis povezan s prethodnim, na taj način se sprječava manipulacija ili izmjena podataka, čime se sigurnost podataka stavlja na primarno mjesto.
- Računskom logikom – brz način upisa podataka kroz korištenje algoritama, odnosno programiranjem može se postići automatska transakcija.

Poslovni informacijski sustavi ključni su za uspješno poslovanje u modernom svijetu, informacijska pismenost je glavna vještina koju moraju usavršiti zaposlenici u tvrtkama. *Blockchain* tehnologija se i dalje razvija, a na putu je poboljšanju sigurnosti, transparentnosti i učinkovitosti u poslovanju. Najvažnije je zaštititi podatke od neželjenih pogleda, svaka neželjena izloženost podataka, mora se umanjiti i potpuno ukloniti. Kako se svijet sve više modernizira, poslovanje koje se odvija preko mreža može biti na udaru od *cyber* napada, koji su najčešće greška nedovoljno educiranih zaposlenika. Iz tog razloga osim razvijanja sigurnosti sustava potrebno je razvijati informacijsku pismenost.

4. PRIJETNJE U POSLOVNIM INFORMACIJSKIM SUSTAVIMA

Informacije su ključ za donošenje poslovnih odluka u tvrtkama, a iz toga proizlazi glavna misao zaštite informacijskih sustava. Krakar i suradnici (2014). naglašavaju kako je najbitnija stavka u razvoju informacijske sigurnosti veza između zainteresiranih strana tvrtke, a to su unutarnji i vanjski dionici. Na taj način se pokreće strategija u poslovnim sustavima gdje će se povezati osobe zainteresirane za informacijsku sigurnost.

Škanata (2022). navodi kako su *cyber* prijetnje nastale davnih godina prošlog stoljeća kroz pojavu računalnih virusa. Važno je naglasiti kako prijetnja može biti izazvana stvarnom namjerom da se ugrozi nečiji poslovni sustav, ili se može dogoditi slučajno. Škanata (2022). naglašava kako postoji sve veći broj *cyber* prijetnji te da se ne može osigurati potpuna zaštita informacijskog sustava. Prilikom građenja snažnog sustava koji će se boriti protiv *cyber* napada, potrebno je shvatiti razloge nastanka napada, odnosno kada su poslovni informacijski sustavi pod prijetnjom. Kako objašnjava Janczewski i suradnici (2007). glavni razlozi su svrstani u tri kategorije:

- strah,
- spektakularnost,
- ranjivost.

Cilj je stvoriti pomutnju kod ljudi, iskoristiti njihove slabosti i strahove znajući kako će to ići u napadačevu korist. Kroz ove tri kategorije pokazuju svoju nadmoć nad žrtvama napada. Posljedica napada na poslovne sustave može se pretvoriti u ozbiljne financijske, ali i informacijske gubitke. Napadi u informacijskim sustavima također ima svoje korake, koje su objasnili Janczewski i suradnici (2007). dijele se na pet faza:

- izviđanje,
- ulazak,
- širenje,
- krađa informacija,
- brisanje tragova.

Svaki napad kreće prvo od izviđanja svoje žrtve odnosno sustava u koji želi ući, u toj fazi napadači prikupljaju sve informacije koje će biti korisne tijekom napada. Nakon što prikupi dovoljan broj informacija, napadač ruši obrambeni sustav te se širi dalje. Nakon toga uzima sve podatke iz sustava i u posljednjoj fazi briše svoje tragove da mu se kasnije ne uđe u trag.

4.1. Vrste *cyber* napada

Najčešći uzrok nastanka greške u poslovnim informacijskim sustavima je pogreška ljudske nemarnosti ili nedovoljne pažnje i neznanja. Prema Hardcastle (2008). postoji nekoliko načina kako se mogu izgubiti podatci. Prvi način je netočan unos podataka, gdje se samo jednim krivim brojem ili slovom se može učiniti da poslije toga ništa više nije točno. Drugi način je taj da se zaposlenicima dodijeli posao koji u tom trenutku nije u razini s njihovim sposobnostima. Postoji još nekoliko nastalih grešaka, a to je djelovanje na vlastitu odgovornost i inicijativu te neprovođenje sigurnosnog kopiranja. Glavna stavka svakog *cyber* napada je ljudsko neznanje, te je vrlo bitno provesti edukaciju zaposlenika, kako bi shvatili što, te u kojim okolnostima je potrebno da naprave potrebni korak.

Jedna od vrsta *cyber* napada mogu biti i prirodne katastrofe. Sicard (2019). objašnjava kako bilo da je riječ o ljudskoj pogrešci ili prirodnoj nepogodi koja može imati negativan utjecaj na poslovanje važno je pripremiti sustav. Naglasak je na izradi plana koji će planirati oporavak sustava poslovanja nakon jakih vremenskih napada, u Republici Hrvatskoj u zadnjih deset godina bilo je prilika za vidjeti i potrese i poplave. To govori kako s prirodom se nikad ne zna i ne može se očekivati samo najbolje, već se pripremiti i za loše situacije.

Postoji nekoliko vrsta *cyber* napada u obliku aplikacija, Bundi i suradnici (2019). naglašavaju sljedeće:

- virus,
- *adware*,
- *spyware,*
- *ransomware*.

Zajednička stavka svim nabrojanim vrstama koje prijete poslovnim informacijskim sustavima je ta da su to zlonamjerni programi. Svi oni imaju isti cilj, ali posljedice koje ostave na poslovne sustave mogu se razlikovati. Bundi i suradnici (2019). naglašavaju kako *adware* može prevariti korisnike na način tako da se klikne na njihovu reklamu i tada nastaje šteta. Kod *spywarea* je drugačija situacija jer se on zapravo predstavlja kao legalna aplikacija, gdje koristi razne informacije o korisnicima te ih negativno iskorištava, a da oni to niti ne znaju. Virus je također negativan jer on usporava rad sustava, te mu čini štetu. *Ransomware* je od svih ovih programa najokrutniji, jer on može staviti lozinku na podatke korisnika, te tražiti za uzvrat otkupninu prilikom koje će vratiti podatke vlasniku. U situaciji gdje se ne dobije tražena otkupnina podatci se gube trajno.

Sabotaža i vandalizam se također ubrajaju u *cyber* napade na poslovni sustav tvrtke. Hardcastle (2008). objašnjava kako sabotaža može biti prouzrokovana s namjerom da se učini šteta ili može biti sasvim slučajna. Ona uvijek dolazi od zaposlenika koji nisu zadovoljni, a glavni cilj je nanijeti štetu u financijskom smislu, prilikom prekida ugovora o poslovanju odnosno, odlaska iz tvrtke, dok se vandalizam smatra namjernim. Bundi i suradnici (2019). uzimaju u obzir sljedeće moguće napade na *cyber* sustav:

- *phishing* - James (2005). objašnjava *phishing* kao napad na poslovni sustav nekog poduzeća koji krade informacije putem lažnog e-*maila* ili putem internetskih stranica.
- Krivotvorenje – prema SecureFlag (n.d.) krivotvorenje zapisa se smatra manipulacijom od strane napadača, gdje se želi narušiti vjerodostojnosti podataka u tvrtkama.
- Napad na lozinke – Raza i suradnici (2012). predstavljaju napad na korisničke račune, putem krađe lozinke koje su pohranjene u operativnom sustavu.
- *Man-in-the-middle* – Mallik (2019). opisuje ovu vrstu napada na poslovni sustav kao upad treće osobe u komunikaciju između pošiljatelja i primatelja poruke, gdje napadač može mijenjati smjer komunikacije. U tom trenutku može doći do potpunog nezadovoljstva sa obje strane, bez da su oni svjesni stvarne situacije.
- *Snooping* – Floehlick (n.d.) objašnjava kako *snooping* predstavlja pregledavanje elektroničke pošte, a to mogu čak raditi i velike tvrtke kako bi provjerile produktivnost svojih zaposlenika.
- *Spoofing* – Forcepoint (2018). govori o *spoofingu* kao obliku prijevare u kojem komunikacija poput elektroničke pošte naizgled dolazi iz pouzdanog izvora, a zapravo je zlonamjerni sadržaj.
- Otimanje sesije - također jedan od napada na sigurnost u poslovnom informacijskom sustavu. Imperva (n.d.) opisuje otimanje sesije kao otimanje kontrole nad nekom internetskom stranicom, gdje se napadač da dođe do cilja, koristi podatcima od korisnika.

4.2. Posljedice napada na poslovne informacijske sustave

Posljedica napada na poslovne informacijske sustave može ostaviti velike gubitke na samu tvrtku koja je žrtva tog napada. Šimundić i Franjić (2009). objašnjavaju kako u trenutku kada se događa napad na *cyber* sustav potrebno je da se ostane pri sebi kako u trenutku panike s kojom se suočava zaposlenik ne bi dogodilo najgore. Nakon toga važno je promatrati kako, u koliko sati i što se događa u tom trenutku na računalu, te je potrebno i ispisati dokumente. Najvažnija stavka kod zaposlenika je da se bude u pripravnosti i da ima na svijesti da se napad može dogoditi. Ovisno o tome koja vrsta *cyber* napada se dogodi nekoj tvrtki, Kala (2023). navodi sljedeće moguće posljedice koje će snositi poslovni informacijski sustav:

- gubitak u novcu,
- zastoj ili nemogućnost daljnjeg poslovanja,
- nove poslovne prakse koje će morati primijeniti,
- gubitak povjerenja klijenata,
- narušavanje ugleda tvrtke.

Nemoguće je procijeniti koja od navedenih posljedica je teža, svaka od njih povlači za sobom drugu posljedicu. Kada se dogodi gubitak u financijskom smislu, tada će se vrlo vjerojatno dogoditi zastoj samog poslovanja iz čega će proizaći, ako se ne riješi brzo problem, nemogućnost isplate plaća i daljnjeg poslovanja. Huang i suradnici (2023). objašnjavaju kako financijski gubitak može znatno utjecati na neku tvrtku u vidu njezinih dionica, gdje se povratak na razdoblje prije napada, ne mora trajati dugo, ako nije u pitanju znatno drastičan novčani gubitak. Važno je naglasiti kako banke takve tvrtke smatraju manje pouzdanim za posudbu novca, što takvim tvrtkama dodatno otežava tijek poslovanja.

Mass (2018). naglašava kako posljedice koje ostavi *cyber* napad je povećanje opreznosti kako se ona više ne bi ponovila, no uz to dolazi i novi sustav koji će činiti odbor ljudi kako bi nadzirali rizik, uspostavljanje poslovne prakse koja će biti poboljšana zbog iskustva. Postoji nekoliko stavki koje će biti trajne posljedice za tvrtku, a to je sam ugled i reputacija na tržištu te gubitak klijenata, koji će biti oprezniji u vremenu koje stoji pred njima. Bendovschi (2015). pridodaje na važnosti tome da se upravljanjem sigurnosti poslovanja razmišlja i pri tom djeluje na globalnoj razini. Odgovornost nije samo na tvrtkama, već i na pojedincu, ali i vlasti kako bi se razvijao sustav sigurnosti, te da je pravo svake osobe da razmisli i donese odluku o tome kako će upravljati, čuvati i kome će podijeliti svoje podatke.

5. METODE ZAŠTITE PODATAKA PIS-A

Značaj koji imaju podatci za neku tvrtku su veliki. Sve poslovne aktivnosti su vezane uz određene podatke koji se pohranjuju u sustavu odnosno u dokumentima računalnog sustava. Rizik za *cyber* napade koji se pojavljuje u tvrtkama i njihovim poslovnim sustavima postaje sve veći. Danas se ne može zamisliti poslovanje bez prisustva podataka, jer na taj način tako i samo poslovanje ne bi bilo dugoročno. Bosilj Vukšić i suradnici (2020). objašnjavaju kako se tvrtke u poslovanju bave s malim i velikim podatcima. Mali podatci se odnose na one podatke koji su nastali pri obavljanju svakodnevnih izvršnih aktivnosti, dok su veliki podatci oni koji se unose u računalni sustav, oni se pristižu u velikom broju, raznoliki su i stižu velikom brzinom. Ti podatci nastaju unutar tvrtke, ali i mogu pristizati iz okoline poduzeća. Vujanić (2018). navodi kako postoji nekoliko metoda kojima se može zaštititi poslovni sustav poduzeća:

- ažuriranje sustava,
- ograničenje pristupa,
- sigurnosne kopije podataka,
- edukacija zaposlenika,
- antivirusni programi.

Šimundić i Franjić (2009). navode još nekoliko metoda zaštite sustava:

- vatrozid (eng. *Firewall*),
- pravna zaštita podataka.

5.1. Firewall i antivirusni programi

U računalnom svijetu vatrozid (eng. *Firewall*) Sviličić i Kraš (2005). objašnjavaju kako on služi upravo za zaštitu velikih podataka, a pri tome odvaja privatnu od javne mreže. Vatrozid djeluje tako da jedan omogući dopušteni promet, a drugi sprječava da se dogodi bilo kakav neovlašteni pristup. Centar informacijske sigurnosti (n.d.) dijeli dvije primarne vrste vatrozida, jedan je poslovni, a drugi osobni vatrozid. Poslovni vatrozid ima glavnu funkciju da štiti informacijski sustav tvrtke, a sastoji se od zaštite *hardwarea* ili *softwarea,* dok je osobni vatrozid za računala koja koriste pojedinci.

Jedna od važnijih prednosti koju ima vatrozid je ta da se mogu eliminirati odnosno ukloniti pravila iz vatrozida, a da pri tome to ne utječe na njegovo izvršavanje zadataka. Gouda i suradnici (2004). objašnjavaju kako se prilikom ažuriranja sigurnosnih postavki može dogoditi

da ta pravila nastanu u tom procesu. Pravila mogu smanjiti učinkovitost sustava koju ima vatrozid, a pogotovo kod sustava koji pretražuju masovne podatke, jer samim time su i složeniji i potrebno je određeno vrijeme da sustav učita podatke. Poslovni svijet je kompleksan, isprepleten s velikom količinom podataka i zaposlenika koji ih koriste. Prema Kaplesh i suradnicima (2019). vatrozid štiti tvrtku na nekoliko načina:

- može zaustaviti protok informacija koji zaposlenici šalju neovlašteno van tvrtke,
- sprječava zaposlenike da posjećuju druge internetske stranice,
- može zaustaviti pokušaj da se računalima iz vanjskog sustava pristupi računalima unutar tvrtke.

Prema McGuire i suradnicima (2013). štetu koju rade zlonamjerni programi poput virusa, trojanskog konja i drugih sličnih programa, je nefunkcionalnost rada računala, oštećenje datoteka i diska, uništenje i oštećenje mrežnih sustava, krađa informacija i drugo. Šimundić i Franjić (2009). navode nekoliko načina prema kojima se sustav može osigurati od zlonamjernih programa:

- onemogućavanje pristupa sustavu bez potrebnih dozvola,
- onemogućavanje pristupa kroz šifriranje sustava,
- kontrola integriteta odnosno autentičnosti sustava,
- praćenje operacija sustava,
- korištenje antivirusnih programa,
- sigurnosno kopiranje podataka,
- korištenje unaprijed odobrenih programa za sustav.

Da bi antivirusni program uspješno izvršio zadatak potrebno je da prije svega prepozna da se radio o zlonamjernom programu. Metode kojima antivirusni program otkriva virus prema Yasar (n.d.) su sljedeće:

- virusni potpisi koji se usporede s drugim datotekama i programima,
- provedba analize prilikom koje sustav otkriva kako se pojedini program ponaša,
- analiza sustava kroz algoritam,
- analiza oblaka (engl. *Cloud*).

S obzirom na svakodnevne rizike s kojima se susreće poslovanje i zaposlenici u njima, antivirusni programi su neophodni za održavanje sigurnosti sustava, od malih pa sve do velikih podataka.

5.2. Uporaba IDS/IPS sustava

IDS sustav ili *Intrusion Detection Systems* te IPS sustav ili *Intrusion Prevention Systems* su jedni od elemenata bez kojih poslovni informacijski sustavi ne mogu funkcionirati. Prema Chakraborty (2013). IDS sustav otkriva moguće prijetnje u poslovnom sustavu, a to su različite vrste *cyber* napada. IPS služi kao pomoć sustavu kada IDS otkrije napad na poslovanje, tada IPS sprječava daljnje radnje koje mogu imati velike posljedice za poslovni sustav.

IDS i IPS sustavi djeluju zajedno u aktivnostima očuvanja poslovnog informacijskog sustava. Prema Chandak i Bartere (2013). može se dogoditi situacija u kojoj u brzini neke aktivnosti koja napada sustav, da ju IDS ne može na vrijeme pročitati i prepoznati. Korisnici moraju biti svjesni da niti jedan sustav za zaštitu podataka nije u potpunosti siguran, već i oni mogu imati propuste. Iako rijetko, propusti se mogu dogoditi, te podatci koji se nalaze u sustavu mogu vrlo lako biti zloupotrijebljeni. Način na koji radi IPS prema IBM (n.d.) je takav da on ima nekoliko metoda koje koristi pri otkrivanju upada u sustav:

- na temelju potpisa – svaki napad ima određeni obrazac ponašanja kako ulazi u sustav poslovanja, te tako se otkriva je li riječ o štetnom programu.
- Na temelju anomalija – u ovom slučaju se koristi umjetna inteligencija kako bi se otkrili napadi na sustav. IPS može otkriti čak i najnovije napade na sustav koji nisu bili mogući da se otkriju putem drugih metoda.
- Na temelju pravila – u slučaju kršenja strogo definiranih pravila u području sigurnosti sustava, tada IPS zabranjuje daljnje aktivnost kako bi zaštitio poslovni sustav.
- Na temelju reputacije – u ovom slučaju IPS blokira sve IP adrese koje nisu sigurne za sustav, odnosno svaka adresa koja je povezana sa zlonamjernim programom.

Centar informacijske sigurnosti (2011). dijeli IDS sustave na sljedeći način:

- mrežne sustave – njihova zadaća je da pregledava mrežu podataka, i usporedi ga s mogućim napadima, odnosno u svojoj bazi ima obrazac napada, te na temelju toga zaključuje o kojem napadu se radi.
- *Host* sustave – glavna zadaća *host* sustava je pregledati zapisnik aplikacija i samog sustava, te da naposljetku prepozna neuobičajene aktivnosti koje se mogu dogoditi.
- Distribuirane sustave – on se sastoji od mrežnih i *host* sustava, a glavna zadaća mu je slanje izvještaja u središnju upravljačku jedinicu sustava. Te na temelju toga sustav provodi daljnje aktivnosti ako se uvidi potreba za njima.

5.3. Edukacija zaposlenika

Većina pogrešaka u poslovanju, tijekom kojeg nastanu problemi sa nekom vrstom napada na podatke poslovanja, je zbog zaposlenika. Podatci koji ukazuju na veliki udio ljudske greške je prema Ion i suradnicima (2021). gdje je čak 95 % slučajeva greška ljudske ruke u 2021. godini. Pattinson i suradnici (2018). objašnjavaju kako sama efikasnost edukacije zaposlenika je specifična zbog ISA rezultata. ISA označuje *Information Security Awareness,* odnosno svijest o informacijskoj sigurnosti, koja se procjenjuje kod zaposlenika unutar određene tvrtke. Kada se završi obuka dobije se rezultat koji govori koliko je pojedini zaposlenik svjestan informacijske sigurnosti i prijetnji, a svijest nakon obuke se može povećati ili ostati ista. Edukacija o informacijskoj sigurnosti, prema Ion i suradnicima (2021). uključuje:

- metode zaštite,
- tehnologije zaštite,
- analiza sredstava napada na sustav.

Metode zaštite sustava, se odnose na koji način će se moći zaštititi sustava, koje osobe mogu pristupiti sustavu i uz koje mjere. Kroz edukaciju se uče i tehnologije zaštite, odnosno koje programe koristiti, koju mrežu za zaštitu koristiti. Kod analize sredstava napada na sustav, proučavaju se sve moguće vrste napada, kako bi ih se pravovremeno prepoznalo i onemogućilo da zloupotrijebi podatke sustava poslovanja. CybSafe (2023). je sastavio izvještaj u kojem tijekom 2023. godine ljudska greška je činila 75 % slučajeva napada na sustave. Kada se usporedi s Ion i suradnicima (2021). koji su proveli analizu u 2021. godini, može s vidjeti kako se u dvije godine edukacija isplatila. Zaposlenici su postali svjesniji rizika i postali su educiraniji o samom informacijskom sustavu. Brojka se snizila s 95 % na 75 %, što znači da se u budućnosti može očekivati kako će postotak i dalje opadati. Kako se poslovanje odvija sve više na računalnim sustavima i koliko su bitni za poslovanje, zaposlenici će postati svjesniji rizika, a samim time i mogućnosti da mogu napraviti štetu svojoj tvrtki. Postoje brojne prednosti edukacije koje objašnjava Alonsagay (n.d.). Prva i najbitnija prednost je zaštita podataka sustava, kada se zaposlenici educiraju o tome kako zaštititi podatke cijela tvrtka je odmah sigurnija. Druga prednost je smanjena šteta u novcima koje bi tvrtke platile kao naknadu za nastalu štetu, umjesto da novac troše za saniranje posljedica, mogu unaprijediti zaposlenike za edukaciju, čime postižu značajne uštede. Produktivnost rada zaposlenika, koji bi se nakon edukacije osjećali snažnije, spremnije i sigurnije za rad s velikim brojem informacija, čime bi se smanjio njihov stres na radnom mjestu.

6. ETIKA I ZAKONITOSTI U CYBER SIGURNOSTI

Temeljna vrijednost za organizaciju su ljudi. Bez ljudskog znanja, vještina i motivacije bilo bi teško odrađivati bitne poslove, ali i vidjeti svijet koji postoji danas. Vrlo je važno ulagati u isti taj ljudski kapital. Lenninger (2011). objašnjava kako su temeljne vrijednosti koje ima pojedina organizacija važni za razlikovanje na tržištu. S pomoću tih vrijednosti imaju konkretne zajedničke ciljeve koje ih vode dalje u poslovanju. Svaki zaposlenik ima drugačije mišljenje i predodžbu o konkretnim stvarima, te različiti unutarnji sustav vrednovanja unutar tvrtke, ali ih mora voditi glavni kodeks koji je odabran u tvrtki.

U današnjem digitalnom dobu vrlo je važna etika i moralnost u poslovanju, a pogotovo kada se ono odvija putem računalnih sustava. Zaposlenicima je dana ključna uloga u očuvanju i održavanju *cyber* sigurnosti. Kroz različite programe edukacije zaposlenicima se podiže svijest o tome koliko je zapravo važno očuvati podatke tvrtke, i zbog njih, ali i zbog tvrtke. Njihovo ponašanje može ili doprinijeti očuvanju integriteta tvrtke ili ga mogu ugroziti. Iz tog razloga ponašanje mora biti etično i moralno, odnosno njihov odnos prema radu mora biti motivirajući uz poznavanje najaktualnijih zakona. Glavna zadaća etičkog ponašanje koju objašnjava Kizza (2014). je da zaposlenici prije svega razlikuju dobre postupke od onih loših. Etika će dati temelj za to da kada čovjek napravi ili dobro ili loše djelo, da ga se poslije za to djelo može prosuditi.

Temeljni principi vrijednosti u *cyber* sigurnosti koje navodi Christen i suradnici (2020). su:

- **sigurnost** – ima različita značenja, može ga se razumjeti kao sigurnost pojedinca, sigurnost države, sigurnost sustava i informacija. U svim ovim aspektima sigurnosti želi se zaštititi i odgovoriti na sve neetične situacije i moguće probleme koji nastanu u *cyber* svijetu poslovanja.
- **Privatnost** – zaposlenici jedni s drugima moraju postupati jednako sa dostojanstvom, bitno je poštovati njihov osobni prostor i njihovu neovisnost. Kod privatnosti je također bitno da podatci koji su od iznimne važnosti za poslovanje ne kolaju i ne pohranjuju u sustavu bez znanja nadležnih osoba. Vrlo je bitno za etičnost, da se ne iskorištavaju niti podatci, niti zaposlenici, kako bi se postigli viši osobni ciljevi.
- **Pravednost** – sinonim je za jednakost među zaposlenicima. Različite prijetnje u poslovnom svijetu koje se odvijaju računalno, mogu imati drugačije učinke na same zaposlenike. Zaposlenici koji su doživjeli *cyber* napad osjećaju se demokratski oštećeniji od onih koji nisu imali taj problem. Ova vrijednost ističe važnost da

sigurnosne mjere od napada budu kod svih ljudi jednake, jer bi u suprotnom to bilo u etičnom i moralnom smislu nepravedno.

- **Odgovornost** – ukazuje na moralne probleme kao što su nedopuštena obrada podataka. Naglašava se stvaranje okruženja u kojem je odgovornost u poslovanju na visokoj razini i gdje se ponašanje koje je moralno i etički ispravno nagrađuje. U tom postupku podupire se jačanje odnosa u organizaciji i između zaposlenika gdje se na posljetku stvara sigurno i etično okruženje za sve.

Cilj etičkog kodeksa je da on pruži savjet i smjernice u raznim situacijama u kojima su neka pitanja i odnosi nejasni. Način na koji se gradi povjerenje među zaposlenicima također je dio etičkog kodeksa, a glavni etički kodeksi dijele se u četiri sfere koje navodi Kizza (2014).:

- načela koja služe kao osnova na temelju koje nastaje dokument,
- politike koje služe smjernice za ponašanje koje je jedino dozvoljeno i etično,
- pravna ponašanja koja se provode putem suda,
- obrazac ponašanja koji uključuje načine ponašanja kroz etički kodeks.

U samom dijelu zakonitosti i razvijanja politike koja će biti pravedna i uspješna u provođenju mjera kojima će se smanjiti udio *cyber* napada na sustav, gdje će sigurnost biti prioritet i glavna asocijacija na tvrtke. Razvoj lojalnosti počinje s razvojem iskrenih i sigurnih odnosa, a kao glavni primjer za to je bankarski sustav. Prskalo (2022). objašnjava područje Republike Hrvatske u sklopu *cyber* sigurnosti. Naglašava se kako je *cyber* sigurnost, koja je porasla u razdoblju pandemije Covid-19, sve važnija u obuhvatu dokumenta nacionalne sigurnosti. Sigurnosno-obavještajna služba je definirana kao agencija čiji je jedan od primarnih poslova da obavijesti samu javnost, odnosno državljane Republike Hrvatske o stanju nacionalne sigurnosti. Kao glavni razlog napada na poslovne sustave su bile informacije koje su se nalazile u sustavima. Zgurić i suradnici (2022). su istog mišljenja kao i autor Prskalo (2022). gdje također navode Covid-19 kao bazu nastanka velikog broja *cyber* napada, no naglašava se kako strategija sigurnosnih politika u području *cyber* sigurnosti je konkretnija u odnosu na druge dokumente u domeni sigurnosnih politika. Razrađeni aspekti su konkretni u područjima informacijskih sustava i zaštite podataka, ali nisu u velikom dijelu obuhvaćene stavke poput područja međunarodne sigurnosti i nacionalnih interesa.

6.1. Zakonski propisi

Razvoj zakonskih regulativa kojima se uspostavlja poboljšana i sigurnija poslovanja kako u raznim organizacijama tako ima i učinak na samo gospodarstvo zemlje. Pravilan razvoj zakona kroz politiku su ključni u smanjenju *cyber* kriminala. Osim u smanjenju rizika od napada na poslovne sustave, povećava se povjerenje kod korisnika, odnosno zaposlenika. Karake-Shalhoub i suradnici (2010). objašnjavaju kako *cyber* napadi predstavljaju prijetnju u proširenju internetskih trgovina, također elektronske uprave, a kao glavni čimbenik upravljanja u smanjenju zločina je vlada zemlje. Vlada kroz promicanje politika za zaštitu sigurnosti razvija sektore poput telekomunikacija, te potiče i razvija ljudsko znanje i infrastrukturu.

Cyber napadi koji su kritični prema promaknuću održivosti nacionale sigurnosti se dijele na nekoliko vrsta prema Prskalo (2022).:

- napad na državne institucije,
- napad na subjekte poslovanja,
- napad na institucije koja se bave financijama,
- napad na računalne sustave institucija koja su od iznimne važnosti za funkcioniranje države, kao što je na primjer komunalne usluge.

Svaka vrsta napada predstavlja problem za državu i društvo u cjelini. Bilo koja vrsta napada može utjecati na živote ljudi, na način kojim će se domaći povjerljivih podataka i narušiti integritet same države i društva. Takav jedan napad je dovoljan da uzrokuje prekid u opskrbi osnovnih usluga društva. Posljedica koja može dovesti do smanjenog povjerenja, te oslabljene sposobnosti države da odgovori na iznimne hitne situacije, te je bitno da se zakonska regulativa postepeno jača kroz razvoj najboljih strategija za obranu sustava poslovanja. Prema zakonu o *cyber* sigurnosti (2024). koji je kvalitetno izrađen i proveden naglašava se nekoliko temeljnih vrijednosti u razvoju Zakona o kibernetičkoj sigurnosti. Dokument govori o ključnim, ali i strateškim mjerama u održavanju sigurnosti sustava poslovanja privatnog i državnog sektora.

U samom početku definiranog Zakona o kibernetičkoj sigurnosti utvrđuje se mjera i način na koji će se postići i održati sigurnost sustava. Kategoriziraju se poslovni subjekti koji su od važnosti za državu i društvo u cjelini. Način na koji ovi poslovni subjekti moraju usvojiti određene mjere su ključni i važni za nacionalnu sigurnost. Određuje se sigurnosni okvir za upravljanje u kritičnim vremenima kada se događaju radnje koje se svrstavaju pod *cyber* zločin, te potiče suradnja sektora i razvoj svijesti o *cyber* sigurnost (Zakon.hr, 2024).

6.1.1. CSIRT

Kako bi se spriječili *cyber* zločini CSIRT-a (eng. *Computer Security Incident Response Team*), je odjel ili tim za odgovor na računalne incidente u sigurnosti sustava. Fauziyah i suradnici (2022). objašnjavaju kako je ovaj odjel specifičan zbog razvoja novih područja u sigurnosti informacijskog sustava. Jedan od noviteta je bilo računalstvo u oblaku. Ovaj odjel radi prvenstveno po postupku da objasni klijentima način rada i skup usluga koji pružaju. Usluge koje oni nude moraju biti povezane s poslovnim zahtjevima njihovih klijenata. Funkcije u nadležnosti CSIRT-a koje navode Skjerka i suradnici (2015). su sljedeće:

- funkcija u okviru jedne države,
- funkcija u okviru određenog sektora,
- funkcija u okviru organizacijama, odnosno tvrtkama,
- funkcija u okviru cijele regije.

Prema Zakonu o kibernetičkoj sigurnosti (2024). članak 4. stavka 3. CSIRT se definira kao mreža koja je povezana s CSIRT mrežama drugih država u Europskoj uniji, na način da se promovira suradnja među tim državama. CSIRT je zapravo Nacionalni CERT, gdje sudjeluje u sigurnosti sustava, u nacionalnoj domeni. Razvoj povjerenja među državama članica Europske unije je jedan od pozitivnih strana, gdje će ljudi zajedničkim snagama stvoriti okruženje poslovnih sustava sigurnim i uspješnim u sve većem razvoju digitalnog svijeta poslovanja.

6.1.2. ENISA

Važnost agencije za cyber zaštitu i sigurnost je od velikog značaja ne samo za Republiku Hrvatsku, već i za cijelu Europsku uniju. U Zakonu o kibernetičkoj sigurnosti (2024). članak 4. stavka 8. ističe ENISU-u kao „agenciju Europske unije koja je nadležna za *cyber* sigurnost“. Ključna uloga ove agencije prema Enisa (n.d.) je u tome da pomaže državama članica Europske unije u procesu razvoja sigurnosnih mjera. Važan segment je u tome da države razumiju njihove pravne obveze u razvoju Zakona, te tehnički dio u primjeni tih zakona. Naglašava se potreba da se u cijeloj Europskoj uniji uskladi sigurnosna mjera u zaštiti poslovnih sustava, kako ne bi došlo do situacija koje bi bile neetične i nepravedne prema drugim državama članica Europske unije. Kada se usporedi CSIRT i ENISA, može se vidjeti kako one obnašaju sličnu funkciju, ali im nadležnosti nisu iste. Povezane su kroz promicanje cyber sigurnosti u Europi, no njihov fokus, skup nadležnosti te aktivnosti koje provode se razlikuju. ENISA je usko povezana uz implementaciju i podršku u *cyber* sigurnosti sustava poslovanja, dok CSIRT ima više timova u različitim sektorima. U tim sektorima identificira i provodi zaštitne mjere, a zajednička stavka

im je usklađivanje i razvoj sigurnosnih mjera u Europskoj uniji, čime se potiče suradnja i jednakost među državama u dijelu zaštite sustava poslovanja.

6.1.3. EU-CyCLONe mreža

Jedan od načina zaštite podataka u poslovanju je i putem EU-CyCLONe mreže (hrv. Europska mreža za povezanost u cyber kriznim situacijama). Zakon o kibernetičkoj sigurnosti (2024). u članku 4. stavka 6., objašnjava ovu mrežu, kao poveznicu europskih organizacija kojima je u cilju da se smanji kriza povezana s *cyber* zločinima. Važnost u ovoj mreži se pojašnjava kroz to što ona posreduje tehničke razina za koju je odgovoran CSIRT i klasične političko-pravne razine. Ta povezanost osigurava ujedinjen i skladan pristup pri zaštiti poslovnih informacijskih sustava, a čini i da je sustav više otporniji i sigurniji unutar same Europske unije. Ajmera i suradnici (2023). pobliže objašnjavaju kako Europska komisija, uz CyCLONe mrežu i uz CSIRT, zajedno ili pojedinačno na vlastiti zahtjev zatražiti da prouče ili pregledaju određeni problem vezan uz nedopuštenu *cyber* aktivnost od ENISA-e. ENISA u tom postupku sastaviti izvješće koje će predati na uvid strankama odnosno u ovom slučaju agencijama i timovima za zaštitu *cyber* sigurnosti. Kada se usporedi CSIRT i EU-CyCLONe mrežu, CSIRT je usmjereniji prema tehničkom odgovoru i upravljanju nedopuštenim radnjama u svojoj nacionalnoj domeni, dok je EU-CyCLONe na razini cijele Europe. Važnost ove mreže je u njezinoj sposobnosti da poveže organizacije da se zajedno bore u snažnijem i otpornijem digitalnom svijetu, a samim time se postiže sigurno poslovno okruženje za sve.

6.1.4. GDPR

GDPR se objašnjava kao „Opća uredba o zaštiti podataka Europske unije“, čija su pravila i zahtjevi koje ona izdaje unaprijed određeni u postupku obrade osobnih odnosno privatnih podataka u Europskoj uniji. Nije definirana na samo organizacije, već i na pojedince koji prikupljaju podatke. Ova uredba ima za cilj zaštititi svu privatnost osobnih podataka, a prava koja osobe i organizacije imaju su propisane u GDPR-u (E-građani, n.d.). Vrlo je bitno naglasiti da i organizacija i pojedinci koji prikupljaju i obrađuju podatke moraju biti svjesni njihovih obveza koje imaju prema GDPR-u. Prema Demirer i suradnicima (2024). tvrtke su u obvezi da poštuju propise koje nalaže GDPR, neovisno o kojoj vrsti podataka se radi ili u koja je svrha njihova prikupljanja. Što znači da moraju osigurati transparentnost i sigurnost pri obradi podataka, ali tim se iskazuje i poštovanje prema pojedincima koji se podatci koriste. Sami podatci se moraju prikupljati u sklopu ove odredbe i njihovih zahtjeva, kako ne bi došlo do narušavanja i zlouporabe podataka, što je kažnjivo zakonom.

7. RASPRAVA

Provedeno istraživanje potaknulo je razvoj svijesti o kritičnosti i rizicima u kojima se nalaze poslovni sustavi. Većina tvrtki je svjesna koliko opasnosti prijeti njihovom poslovanju u sve više digitaliziranom svijetu. Poslovni subjekti postaju zastrašeni činjenice da mogu izgubiti ne samo svoj ugled koji su godinama gradili na tržištu, ali i lojalnost potrošača i velike financijske gubitke. Upitno je može li se tvrtka oporaviti nakon provedenog napada na njih poslovni sustav, ovisno o tome koliko je napad bio razarajući za poslovanje. Čak i nakon što se oporavi potrebno je dosta vremena da povrati svoju primarnu slavu koju su stekli na tržištu.

Cyber sigurnost razvija jako puno mjera kojima se štiti poslovanje, počevši od suradnje države s Europskom unijom, te suradnjom s drugim državama članicama gdje se povezuju i jačaju na strategiji zaštite svojih dragocjenih podataka. Europska unija razvija i dalje sustave kojima se smanjuje mogućnost da se napadi dogode. Glavna stavka koju oni predlažu je povezivanje svih država članica da se ujedine, odnosno da sustav sigurnosti bude u svakoj državi jednak. Razlog tomu je da ne dođe do situacija u kojima se itko može žaliti kako neke države su bolje opremljenije u sigurnosti svog poslovanja od drugih. Tvrtke koje su najotpornije na cyber napade odnosno one u kojima se događa najmanji udio napada su i one koje najviše ulažu u svoje zaposlenike da se educiraju. Redovni radovi na razvoju poslovnog sustava gdje se radi na poboljšanju *softwarea*, od velike su važnosti za poslovanje gdje se uklanja mogućnost daljnjeg propusta i slabosti koju bi sustav mogao imati.

Prednosti koje nudi zaštita informacijske sigurnosni u poslovanju uključuje zaštitu podataka koji su vrlo povjerljivi i osobni, čijim se otuđivanjem ruše glavna građanska prava. Niti jedna osoba ne bi htjela biti žrtva ovakve vrste napada, pa je samim time potrebno i najviše opreza imati u poslovanju s velikim brojem podataka. Svaka tvrtka ima svoju reputaciju na tržištu koju grade godinama, ali vrlo malo je potrebno vremena da se ta reputacija naruši. Glavni sinonim za tvrtku kada je spomenu potrošači, kupci ili korisnici je ta da je ona sigurna i povjerljiva. Time se jača povezanost među njima, ali i raste lojalnost. Zaposlenici koji rade u tvrtkama osjećaju se bolje i u znanju su da neće biti odgovorni ako se dogodi *cyber* napad, time jača njihova motivacija pri radu, ali i fokusiranost. Osim osjećaja sigurnosti i povezanosti, u procesu zaštite sustava poslovanja, prilikom sklapanja ugovora s raznim *software* tvrtkama mog sklopiti i prijateljstva, ali i buduće čvrste poslovne suradnje. Nedostatci koji se mogu pojaviti prilikom zaštite *cyber* sustava u poslovnim informacijskim sustavima jesu prije svega veliki troškovi.

Troškovi se odnose na razvoj sustava sigurnosti poslovanja, zatim korištenja naprednih tehnologija i raznih programa koji se naplaćuju. Osim korištenja tih tehnologija potrebno ih je i održavati i ažurirati. Zaposlenici čije tvrtke se odluče za edukaciju, također moraju platiti određeni iznos novaca kako bi se njihovi zaposlenici usavršili. Takva vrsta troškova ne mora biti od velikog značaja za tvrtke koje posluju s velikim godišnjim prihodima, već za one tvrtke koje posluju s ograničenim resursima i koje nemaju dovoljno novca u svom proračunu. Jedan od nedostataka je ako se prekrši GDPR, snose se odgovornosti koji stoje u pravilniku, ali i bilo koje druge zakonitosti za kršenje integriteta poslovnih podataka.

Kako i se poboljšala sigurnost poslovnih informacijskih sustava kroz prijedloge važno je naglasiti da se poveća investicija u zaposlenike tvrtke kako bi bili spremni odgovoriti na bilo kakvu vrstu *cyber* napada. Važno je da se uspostavi politika koja će biti stroža, te koja će testirati redovito protokole sigurnosti u poslovnim sustavima. Razvoj antivirusnih programa koji će biti dostupni u svakoj tvrtki jednako, te koja će pružiti istu razinu sigurnosti, bez obzira na financijsku podlogu tvrtke. Kao najgora verzija s kojom se tvrtke mogu susresti je zlonamjerni program *ransomware.* Iako je težina i posljedice koju ostavljaju na poslovanju svakog zlonamjernog programa relativno ista, ovaj program se razlikuje. Ransomware je kao programski „otmičar“, gdje traži otkupninu za sve podatke koje je otuđio iz sustava. Kada mu se ne dostavi željena otkupnina, svi podatci koji su bitni za poslovanje ili nastavak poslovnog procesa se trajno gube. Jedan je od vrlo mudrijih zlonamjernih programa, te ga se može usporediti da radi po principu klasičnog lopova i otmičara u jednom. Kako bi se razvijala sigurnost podataka, potrebno je nakon svake provedene poslovne akcija, pohraniti podatke na posebne kartice koji se izvade iz računalnih sustava, te po potrebi u svakom poslovnom procesu uzimaju podatci iz kartice kako bi se zaštitili.

Na temelju provedenog istraživanja, vrlo je jasno kako su tvrtke sve više izložene *cyber* napadima, posebno se treba pribojavati i raditi na razvijanju sigurnosti poslovnih informacijskih sustava zbog zlonamjernog programa kao što je *ransomware*. Uz sve napore u očuvanju sigurnosti poslovanja, tvrtke se suočavaju s izazovima kao što su visoki financijski troškovi, koji sužavaju njihove mogućnosti da na pravilan i poboljšan način obrane sigurnost poslovnog sustava. Unatoč preprekama koje ih okružuju, ulaganja u sigurnost podataka i svakodnevna unapređenja standarda sigurnosti su neophodni za poslovanje. Za pravilan i siguran način rada tvrtke, ali i održavanja njihove konkurentnosti na tržištu i razdoblju digitalizacije vrlo je bitno održavati korak s drugim tvrtkama, kako ne bi tvrtke bile stalna i slaba meta *cyber* napada.

8. ZAKLJUČAK

U završnom radu tema koja je istražena je: „Cyber sigurnost u poslovnim informacijskim sustavima“. Naglasak u ovom radu je na važnosti zaštite sigurnosti poslovanja, te metode koje tvrtke moraju poduzeti u procesu zaštite svojih informacijskih sustava. Podatci čine osnovu na temelju kojih se donose bitne odluke te samim time je važno osigurati pravilnu zaštitu sustava. Rad mogu koristiti sve osobe koje su zainteresirane za zaštitu, razvoj i poboljšanje poslovnih informacijskih sustava, poput na primjer menadžera i IT stručnjaka.

Cilj je bio pružiti uvid u stanje na području *cyber* sigurnosti, koji su ključni, ali i kritični elementi na kojima tvrtke moraju raditi. Preporuke za poboljšanje uključuju kontinuirano praćenje razvoja tehnologije i zakonitosti u *cyber* sigurnosti, razvoj novih prijetnji na poslovanja, te istraživanje različitih strategija zaštite, ali i detekcije *cyber* napada. Ovaj rad daje na važnosti razumijevanju cyber sigurnosti i edukacije zaposlenika u poslovanju kako bi se efikasno obranio poslovni informacijski sustav.

POPIS LITERATURE

Knjige

1. Centar informacijske sigurnosti (2011). Snort IDS. Laboratorija za sustave i signale, Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu.
2. Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity* (p. 384). Springer Nature.
3. Garača, Ž. (2008). Poslovni informacijski sustavi, Sveučilište u Splitu, Ekonomski fakultet, Split
4. Gouda, M. G., & Liu, X. Y. (2004). Firewall design: Consistency, completeness, and compactness. In *24th International Conference on Distributed Computing Systems, 2004. Proceedings.* (pp. 320-327). IEEE.
5. Hardcastle, E. (2008). *Business information system*, Bookboon.
6. James, L. (2005). *Phishing exposed*. Elsevier.
7. Janczewski, L., Colarik, A. (2007). *Cyber warfare and cyber terrorism*. IGI Global.
8. Karake-Shalhoub, Z., & Al Qasimi, L. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing.
9. Kizza, J. M. (2014). *Computer network security and cyber ethics*. McFarland.
10. Njavro, Đ., Njavro, M., Erdeljac., M. (2022). Blockchain: Harvard Business Review: Zagreb: Mate.
11. Skierka, I., Morgus, R., Hohmann, M., Maurer, T. (2015). *CSIRT basics for policy-makers*. Types & culture of computer security incident response teams. GPPI
12. Srića, V., Spremić, M. (2000). Informacijskom tehnologijom do uspjeha. Zagreb: Sinergija.
13. Šimundić, S., Franjić, S. (2009). Računalni kriminalitet, Sveučilište u Splitu, Pravni fakultet, Split.
14. Škanata, D. (2022). Modeli rizika. Zagreb: Element.
15. Težak, Đ. (2010). Internet - poslije oduševljenja. Zagreb: Hrvatska sveučilišna naklada.

Znanstveno-stručna djela i članci

1. Ajmera, P., & Nusselder, S. (2023). INTERSECT Policy Brief 2: Cyber Solidarity Act Proposal
2. Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.
3. Bundi, D., Odero, E., Omosa, O. (2019). The Impact of Cyber Attacks on E-Businesses.

4. Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research (IJCBR)*, *4*(2), 1-8.
5. Chandak, M. D. K., & Bartere, M. M. Comparative Study of IPS over IDS. *International Journal of Advanced Information Science and Technology (IJAIST),* Vol.11, No.11
6. Ćurko, K. (2001). Skladište podataka–sustav za potporu odlučivanju. Ekonomski pregled, *52*(7-8), 840-855.
7. Demirer, M., Hernández, D. J. J., Li, D., & Peng, S. (2024). *Data, Privacy Laws and Firm Production: Evidence from the GDPR* (No. w32146). National Bureau of Economic Research
8. Europski revizorski sud (2019). Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a.
9. Fauziyah, F., Wang, Z., & Joy, G. (2022). Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). *Journal of Information Security*, *13*(4), 294-311.
10. Galičić, V., i Ivanović, S. (2008). 'QUALITY MANAGEMENT OF HOTEL INFORMATION SYSTEM', *Informatologia*, 41(4), str. 286-292.
11. Ion, B., Rodica, B., & Dumitru, C. (2021). Support of education in cybersecurity. *Pro Publico Bono–Public Administration*, *9*(1), 128-147.
12. Kala, E. (2023). The Impact of Cyber Security on Business: How to Protect Your Business. *Open Journal of Safety Science and Technology*, 13, 51-65.
13. Kaplesh, P., i Goel, A. (2019). Firewalls: A study on Techniques, Security and Threats. *Pramana Res. J.*, 201941-201952.
14. Lenninger, H., & Chan, A. (2011). The communicative role when establishing core values as motivators for employee engagement.
15. Lozić, J., & Čiković, K. F. (2023). Digitalna transformacija: korištenje poduzetničke podloge u kontekstu blockchain tehnologije. Politehnika i dizajn *Politehnika i dizajn*, *11*(04).
16. Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace*: Jurnal Pendidikan Teknologi Informasi, 2*(2), 109-134.
17. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

18. Pattinson, M. R., Butavicius, M. A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting Cyber-Security Training to Your Employees. In *HAISA* (pp. 67-79).
19. Prskalo, D. (2022). Kibernetička sigurnost kao ključna determinanta nacionalne sigurnosti Republike Hrvatske. *Zbornik sveučilišta Libertas*, *7*(8), 185-199.
20. Raza, M., Iqbal, M., Sharif, M., Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World applied sciences journal*. *19*(4), 439-444.
21. Sicard, K. (2019). The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks. *The Kennesaw Journal of Undergraduate Research* 6(2), 4
22. Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). CSIRT basics for policy-makers. *Types & culture of computer security incident response teams, the history*.
23. Sviličić, B., & Kraš, A. (2005). Computer systems privacy protection. *Pomorstvo*, 19(1), 275-284.
24. Zgurić, B., & Petek, A. (2022). Analiza ciljeva hrvatske sigurnosne politike. *Hrvatska i komparativna javna uprava: časopis za teoriju i praksu javne uprave*, *22*(4), 735-764.

Internetske stranica

1. Alonsagay, I. A. (n.d.). 7 reasons why training your employees on Cyber Security is important. Dostupno na: https://www.upskilled.edu.au/skillstalk/why-training-employees-on-cyber-security-is-important, pristupljeno 8.6. 2024.
2. Centar informacijske sigurnosti (n.d.) Zaštita mreže - Vatrozid. Dostupno na: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html, pristupljeno 19.5. 2024.
3. CybSafe (2023). Security Awareness: 7 reasons why security awareness training is important in 2023. Dostupno na: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/, pristupljeno 8.6. 2024.
4. Eclipse consulting (n.d) Business Firewalls: How To Protect Your Computer Network. Dostupno na: https://eclipse-online.com/news/business-firewalls-computer-network/, pristupljeno 5.5.2024.
5. E-građani (n.d.) Što je opća uredba o zaštiti podataka (eng. General Data Protection Regulation - GDPR)? Dostupno na: https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868?lang=hr, pristupljeno 12.6. 2024.

6. ENISA (n.d.) Cybersecurity policy. Dostupno na: https://www.enisa.europa.eu/topics/cybersecurity-policy, pristupljeno 11.6. 2024.
7. ENISA (n.d.) Eu cyclone. Dostupno na: https://www.enisa.europa.eu/topics/incident-response/cyclone, pristupljeno 11.6. 2024.
8. Faster capital (2024). Security firewall and antivirus: Protecting Your Startup: The Importance of Security Firewall and Antivirus. Dostupno na: https://fastercapital.com/content/Security-firewall-and-antivirus--Protecting-Your-Startup--The-Importance-of-Security-Firewall-and-Antivirus.html, pristupljeno 5.5. 2024.
9. Forcepoint (2018). What is Spoofing? Dostupno na: https://www.forcepoint.com/cyber-edu/spoofing, pristupljeno 5.5. 2024.
10. Froehlick, A. (n.d.) What is snooping and how can it be prevented? Dostupno na: https://www.techtarget.com/searchsecurity/definition/snooping, pristupljeno 5.5. 2024.
11. Huang, K., Wang, X., Wei, W., i Madnick, S. (2023). The devastating business impacts of a cyber breach. *Harvard Business Review*. Dostupno na: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach, pristupljeno 18.5. 2024.
12. IBM (n.d.) What is an intrusion prevention system (Ips)? Dostupno na: https://www.ibm.com/topics/intrusion-prevention-system, pristupljeno 31.5. 2024.
13. Imperva (n.d.) What is session hijacking: types, detection & prevention. Dostupno na: https://www.imperva.com/learn/application-security/session-hijacking/, pristupljeno 5.5. 2024.
14. Mass, S. (2018). *Economic and financial consequences of corporate cyberattacks*. Dostupno na: https://www.nber.org/digest/jun18/economic-and-financial-consequences-corporate-cyberattacks, pristupljeno 18.5. 2024.
15. SecureFlag. (n.d.) *Log injection vulnerability*. SecureFlag Security Knowledge Base. Dostupno na: https://knowledgebase.secureflag.com/vulnerabilities/inadequate_input_validation/log_injection_vulnerability.html, pristupljeno 5.5. 2024.
16. Yasar, K. (n.d.) What is antivirus software? Dostupno na: https://www.techtarget.com/searchsecurity/definition/antivirus-software, pristupljeno 24.5. 2024.

Vjesnik:

1. Vrkić Dimić, J. (2014). 'Suvremeni oblici pismenosti', *Školski vjesnik*. Odjel za pedagogiju Sveučilište u Zadru, Zadar. Dostupno na: https://hrcak.srce.hr/136084

Zakon:

1. Zakon.hr (2024). Zakon o kibernetičkoj sigurnosti. Dostupno na: https://www.zakon.hr/z/3718/Zakon-o-kiberneti%C4%8Dkoj-sigurnosti, pristupljeno 11.6.2024.

Završni i diplomski radovi:

1. Štefanić, L. (2021). Poslovni informacijski sustavi. Završni rad, Sveučilište u Rijeci. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:195:654998
2. Vidaković, V. (2022). Implementacija transakcijskog informacijskog sustava. Završni rad, Sveučilište u Zagrebu, Fakultet organizacije i informatike. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:211:427388
3. Vujanić, Ž. (2018). Zaštita informacijskog sustava od Ransomware napada. Završni rad, Visoko učilište Algebra. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:225:298466