Izvori i oblici prijetnji sustavu sigurnosti informacija Republike Hrvatske

Kraljević, Elena

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Poslovanje i upravljanje

ELENA KRALJEVIĆ

IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA REPUBLIKE HRVATSKE

PREDDIPLOMSKI ZAVRŠNI RAD

Zaprešić, 2021. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Poslovanje i upravljanje

Usmjerenje Menadžment uredskog poslovanja

PREDDIPLOMSKI ZAVRŠNI RAD

IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA REPUBLIKE HRVATSKE

Mentor:
dr. sc. Dragutin Funda, prof. v. š.

Studentica:
Elena Kraljević

Naziv kolegija:
UPRAVLJANJE KVALITETOM U UREDSKOM POSLOVANJU

JMBAG studenta:
0124122684

SADRŽAJ

SAŽETAK

IZVORI I OBLICI PRIJETNJI SUSTAVU SIGURNOSTI INFORMACIJA REPUBLIKE HRVATSKE

Tema završnog rada „Izvori i oblici prijetnji sustavu sigurnosti informacija Republike Hrvatske“ za cilj ima predstaviti važnost teme sigurnosti informacija, izložiti sustav sigurnosno-obavještajne organiziranosti u Republici Hrvatskoj, pokazati izvore i oblike prijetnji, te naposlijetku izložiti međunarodnu normu koja osigurava izvrsnost u području informacijske sigurnosti.

U svijetu je primjetna sve veća važnost zaštićenosti i sigurnosti informacija, kako osobnih tako i državnih. Kroz period od deset godina može se primijetiti koliko se tehnološka slika svijeta i Republike Hrvatske promijenila. Hakerski napadi postali su učestali, a čak i obični građani podložni su različitim prijevarama. Zaštita informacijskog sustava i samim time sigurnosti informacija veoma je kompleksna tema jer uključuje konstantnu promjenu, prilagodljivost, praćenje trendova, suradnju s drugim državama, razmjenu informacija, nadzor i procjenu rizika koja interno otkriva najranjivije dijelove sustava koji se odmah trebaju sanirati i unaprijediti.

U prvom dijelu rada pažnja je usmjerena na objašnjavanje terminologije informacijske infrastrukture i sustava. Nakon objašnjavanja terminologije, drugo poglavlje uvodi u neke od nacionalnih okvira i zakona koji se bave zaštitom informacijskog sustava, koji će poslužiti kao temelj pregleda informacijske sigurnosti u Republici Hrvatskoj, što podrazumijeva pregled temeljnih ustanova koje se direktno bave temom informacijske sigurnosti. Na kraju poglavlja, dio je posvećen praktičnim primjerima napada kojima su Republika Hrvatska ili njezini građani bili izloženi u proteklo vrijeme. Ovi praktični primjeri služe kao primjer kako nijedan informacijski sustav, koliko god zaštitnih mjera poduzeo, neće biti 100% siguran.

Naposlijetku, potpuno poglavlje posvećeno je međunarodnom standardu informacijske sigurnosti s kojima su hrvatski zakoni i pravilnici usklađeni. U poglavlju se daje pregled ISO/IEC 27001 i 27002 normi, njihovim sličnostima, različitostima i važnostima za implementaciju.

Tema informacijske sigurnosti sve više dobiva na važnosti, a u pojedinim organizacijama je često i zanemarena. Usvajanje međunarodnih normi dobar je put ka napredovanju pri boljoj zaštiti državnih tajni i pojedinaca, državljana Republike Hrvatske.

Ključne riječi: informacijska sigurnost, sigurnosne norme, standardi, ISO/IEC

27001:2013, ISO/IEC 27002:2013, sigurnost informacija, sigurnosno-obavještajne agencije, zakoni

SOURCES AND FORMS OF THREATS TO THE INFORMATION SECURITY SYSTEM OF REPUBLIC OF CROATIA

ABSTRACT

The topic of this work is „Sources and Forms of Threats to the Information Security System of Republic of Croatia“. Its goal is to present the importance of the topic of safety of information, to observe scheme of security intelligence organization in Republic of Croatia, to show sources and forms of threats and to lay out international norms which ensure excellence in the field of security of information.

What we can see as a trend in the world is the increase of the importance of being protected and to know that your information is secured. Through last ten years one can see how the technology has changed the world and consequently Republic of Croatia. Hackers' activity has increased exponentially, and even the regular citizens have become the target of malicious attacks. Protection of system of information and the safety of information is very complex topic since it involves the need for constant change, adjustability, trend following, cooperation with other countries, information exchange, oversight of all suspicious activities and risk assessment which always pinpoints the most vulnerable parts of system that needs to be changed and improved.

First part of this paper is focused on terminology which revolved around informational infrastructure and system of information. After terminology has been layed down, second chapter brings more information of national laws and recommendations which directly deal with the topic of system of information and its safety. Laws and recommendations gives this paper the framework to deal with the topic of security of information in the Republic of Croatia, which entails the overlook of key institutions involved in this matter. At the end of the chapter, the reader will be introduced to some real life examples of attacks which citizens of the Republic of Croatia or the State have experienced in the past. These examples serve to show that there is no 100% safe system of information, no matter the groundwork that has been layed down.

Complete chapter has been dedicated to international standards of safety of information, which Croatian laws follow. The reader will be able to find out more about ISO/IEC 27001 and 27002 norms.

The topic of safety of information is getting more and more serious role in our everyday lives, and some organization even overlook this topic's importance. By implementing international standards we're taking one step forward to better protection of citizens and countries in general.

Key words: security of information, information security, norms, standards, ISO/IEC 27001:2013, ISO/IEC 27002:2013, safety of information, security intelligence agencies, laws

1. UVOD

Završni rad „Izvori i oblici prijetnji sustavu sigurnosti informacija Republike Hrvatske“ u početku je krenuo kao ideja o predstavljanju sustava sigurnosti informacija i njegovog ustroja, no naposlijetku je pretvoren u pregled važnosti sustava sigurnosti informacija te mu je glavni fokus postao predstavljanje normi vezanih uz zaštitu sustava informacija. Razlog tome je jednostavan – analizirajući zakone i akte Republike Hrvatske, brzo se došlo do zaključaka da ne postoji savršen sustav koji će besprijekorno zaštititi bilo koji informacijski sustav na svijetu. Naprotiv, borba protiv zlonamjernih napada je konstantna i nikada ne prestaje. Od „izuma“ interneta do danas, zlonamjerni napadi su se povećali, a običan korisnik nikada nije bio ranjiviji na Internetu. S druge strane, čak ni državna tijela nisu nedodirljiva – usprkos resursima, napadači internetskog prostora i osobe koje žele ukrasti povjerljive informacije uvijek će osmisliti nove načine.

Rad je podijeljen u četiri glavne cjeline. Prvo poglavlje bavi se terminologijom vezanom uz termine poput sustava informacija, informacijske sigurnosti, načina definiranja i implikacija koje se vezane uz navedene definicije. Prvo poglavlje u cilju imati postaviti podlogu za daljnje razumijevanje teksta. Drugo poglavlje predstavlja neke od zakonodavnih okvira koji se aktivno bave informacijskom sigurnosti, poput Nacionalne strategije za kibernetičku sigurnost. Drugo poglavlje služi kao prikaz državnih koraka u interesu zaštite informacijskog sustava. Treće poglavlje podrobnije se bavi informatičkim sustavima i njihovom sigurnosti tako da predstavlja konkretne institucije u Republici Hrvatskoj koje se aktivno bave sigurnosti informacija. U trećem poglavlju predstavljeni su i pravi slučajevi ugroza informacijskog sustava u Republici Hrvatskoj – dan je primjer hakiranja Ministarstva vanjskih poslova, kao i hakiranja podataka građanina Republike Hrvatske. Ovi slučajevi poslužit će kao primjer da, usprkos mnogim zaštitama, ne postoji nedodirljiva osoba u internetskom prostoru usprkos mnogim zidovima koje hakeri moraju proći i koje ne bi trebali probiti. Naposlijetku, četvrto poglavlje dublje se bavi međunarodnim normama postavljenima od strane ISO-a i IEC-a u području informacijske sigurnosti. Radi se o normama koje propisuju načine analiziranja rizika za organizaciju te djelovanje shodno prepoznatim prijetnjama. Norme naglašavaju kontinuiranu procjenu i prilagodbu uvjetima, slično

kao što se tehnologija i maliciozni napadi mijenjaju i prilagođavaju različitim sustavima zaštite.

U izradi rada koristila se stručna literatura, ali i mnoštvo internetskih izvora sa stranica relevantnih institucija ili istraživačkih centara. U cilju je bilo doprijeti do što više informacija preko mrežnog pozivanja – naime, u međunarodnim normama i u Nacionalnoj strategiji često će se istaknuti važnost informiranosti javnosti i njezine edukacije za što bolju sigurnost informacijskih sustava. Ako takva literatura nije dostupna na mrežnom dijelu, norme i strategije su promašile svoj cilj. Rad je teorijske prirode i donosi općeniti pregled teme informacijskih sustava, sigurnosti te mu je u cilju prikazati povezanost državne i javne organiziranosti za sveukupnu bolju zaštitu svih informacija koje izlažemo pred potpune strance ili državne institucije.

2. INFORMACIJSKI SUSTAV I INFORMACIJSKA SIGURNOST

Shvaćanje važnosti zaštite i sigurnosti podataka uvelike se promijenio 1969. godine jednom kraticom – ARPANET, odnosno prototipom onoga što danas znamo pod nazivom Internet. Iza kratice ARPANET stoji Advanced Research Project Agency Net, odnosno Agencija za napredne istraživačke projekte na računalnoj mreži. Bila je to mreža osnovana od strane američkog Ministarstva obrane kojoj je u cilju bilo umrežiti veliki broj računala u SAD-u i na taj način omogućiti bržu i pouzdaniju komunikaciju vojnih entiteta u periodu hladnog rata. 1989. Tim Berners-Lee, otac Interneta kakvog poznajemo danas, izumljuje servis World Wide Web (WWW), bez kojega se cijeli svijet ne bi mogao umrežiti na način koji danas koristimo Internet.

Iako je Tim Berners-Lee od početka bio zagovornik transparentnosti Interneta, u posljednjih 10 godina i on sam se aktivirao u području zaštite informacija, informacijskih sustava i sigurnosti podataka na Internetu. U intervjuu danom početkom 2021. godine The New York Timesu, Berners-Lee izjavio je kako je online život „zastranio“, te kako postoji previše moći i osobnih podataka koje pohranjuju tehnološki divovi poput Googlea i Facebooka[1]. U spomenutom intervjuu naglasio je kako je Internet koji je on zamišljao trebao dati individualnim korisnicima veću moć u području kontrole digitalnog otiska koji ostavljaju. U tu svrhu, Berners-Lee izradio je softver za poduzeća i državne agencije koji bi trebao pomoći u zaštiti podataka pojedinaca i svih državljana.

Kako smo došli od nevine ideje pristupa informacijama za sve stanovnike Zemlje do problema zaštite podataka i općenite sigurnosti u tridesetak godina postojanja Interneta i kako suzbiti (ili barem pokušati umanjiti) različite napade kojima je u cilj ukrasti, iskoristiti i trgovati tuđim podatcima, bili oni od pojedinca ili od cijelog državnog organa? U sljedećim potpoglavljima predstavit će se temeljna terminologija rada koja će potom poslužiti za predstavljanje i analizu sigurnosti informacija, te oruđa koja bi potencijalno mogla pomoći u borbi protiv kriminalnih aktivnosti na

[1]New York Times (2021.) *He Created the Web. Now He's Out to Remake the Digital World*. URL: https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html. Pristupljeno: 30.06.2021.

području zaštita informacija.

2.1 INFORMACIJSKI SUSTAV I PODATKOVNA INFRASTRUKTURA

Šaljivo se govori kako su prvi opsežni informacijski sustavi bili kartični podatci u knjižnicama, pa ako ste imali zakasninu, knjižnice su itekako znale gdje vas pronaći. Slično je bilo i sa poreznim podatcima građana. Omogućavanjem pristupa Internetu globalnoj zajednici i napretkom tehnologije, informacijski sustav danas nosi drugačije značenje.

Prema mrežnom izdanju Hrvatske enciklopedije, informacijski sustav (skraćeno: IS) je „organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu“[2]. Temelji informacijskog sustava su informacijska i komunikacijska tehnologija, a podatci i informacije pohranjuju se u bazama podataka.

Tipičan informacijski sustav sastoji se od pet komponenti: hardvera, softvera, podataka, ljudi i procesa[3]. Hardver, softver i podatci smatraju se tehnološkom kategorijom, dok su ljudi i procesi komponente koje izravno djeluju na tehnologiju i upravo oni čine ranjivost informacijskog sustava.

Nađ i Adelberger (2016: 118) ove komponente razlažu na ponešto drugačiji način i objašnjavaju ih kao resursi unutar kojih se nalaze informacije: uz hardver, softver i osoblje, navode mreže, mjesta, osnovne usluge i organizacijsko okruženje kao glavne instance informacijskog sustava. Hardver ima fizičku ulogu obrađivača informacija, softver omogućava operativnost sustava i aplikacija, a osoblje su svi ljudi koji djeluju u okviru informacijskog sustava (Nađ i Alderberger, 2016: 118).

Nađ i Alderberger definiraju mrežu kao „komunikacijske sklopove korištene za međuvezu nekoliko fizički udaljenih kompjutera ili elemenata informacijskog sustava“ – dakle, Internet – dok pod mjesta podrazumijevaju baze podataka koje skladište sve prikupljene informacije. Naposlijetku, organizacijsko okruženje je cijeli

[2]Hrvatska enciklopedija, mrežno izdanje (2021.) *Informacijski sustav*. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=27410. Pristupljeno 30. 6. 2021.

[3] Bourgeois, D. (2014). Chapter 1: What Is an Information System? – Information Systems for Business and Beyond. URL: https://bus206.pressbooks.com/chapter/chapter-1/. Pristupljeno 28.06.2021.

organizacijski okvir koji obuhvaća ljude, pravila i procedure za obradu informacija. Osnovne usluge spomenute od strane Nađ i Alderbergera određene su ovisno o vrsti djelatnosti koju određena tvrtka ili odjel obavljaju tijekom obrade i pohrane informacija – porezne usluge, transakcijske usluge, komunikacijske usluge i slično.

Proširenjem i napretkom tehnologije, informacijski sustav dobiva različite definicije, no u suštini uvijek leže dvije komponente – tehnologija kao „hladni pogon" sustava, kao potpora obradi i skupljanju informacija, te ljudska komponenta koja donosi finalnu odluku gdje će prikupljene informacije biti iskorištene, te među ostalim daje značenje prikupljenim informacijama.

Tehnološka komponenta nema značenja bez ljudske komponente, a ljudska komponenta je beznačajna bez tehnološke komponente. Umjetna inteligencija u tehnološku komponentu je unijela novi značaj načina obrade i usavršavanja informacija, no ljudska komponenta je ona zbog koje se pitanje sigurnosti informacija postavlja kao jedan od glavnih problema Interneta i internetske zaštite podataka u cjelini. U nastavku će biti prikazan pojam informacijske sigurnosti informacija, ključan termin koji čini okosnicu ovoga rada.

2.2 INFORMACIJSKA SIGURNOST

Sigurnost je pojam koji je u svakodnevici shvaćen kao završni stadij neke aktivnosti ili kao proizvod koji će nas zaštititi i otkloniti brige. Ipak, sigurnost nije takav pojam, već se on smatra (i mora biti) kontinuiranim procesom koji se konstantno održava, gradi, iznova procjenjuje i unapređuje. Postoje mnoge definicije sigurnosti u stručnoj literaturi te mnoge komponente koje čine sigurnost, no više-manje definicije ističu temelj pojma – sigurnost je proces!

Cingula (2004) definira sigurnost kao kontrolu neizvjesnosti u kojoj se eventualna prepoznata opasnost svodi u granice prihvatljivog rizika – drugim riječima, biti siguran znači prepoznati sve rizike u okolini i znati kako djelovati na njih, odnosno uspostaviti procese koji će u slučaju izbijanja rizika uspješno riješiti ili spriječiti rizik.

Pleskonjić, Maček, Đurđević i Carić (2007) definiraju pojam sigurnosti kao proces održavanja prihvatljive razine rizika. Dakle, slično Cinguli, suočavaju se s time kako

rizici postoje, no ono što je najbitnije u tom procesu na vrijeme prepoznati i djelovati u skladu s prepoznatim rizicima.

Iz temeljnog pojma sigurnosti izdvaja se krak koji se naziva informacijska sigurnost. Cisco Systems, jedna od vodećih IT tvrtki za razvoj, proizvodnju i kupovinu hardvera, softvera i telekomunikacijske opreme u svijetu, informacijsku sigurnost (InfoSec) definira kao procese i alate koji su osmišljeni kako bi zaštitili osjetljive poslovne informacije od izmjene, uništenja, krađe ili neovlaštenog ulaza. Važno je napomenuti kako informacijska sigurnost te cyber sigurnost nisu jednaki pojmovi kao što se često misli u javnosti: informacijska sigurnost je ključna stavka cyber sigurnosti, no odnosi se isključivo na procese koji su stvoreni za zaštitu podataka, odnosno informacija. Cyber sigurnost više je generalniji termin koji uključuje, među drugim instancama, i informacijsku sigurnost.

2.2.1 CIA TRIJADA

Informacijska sigurnost počiva na tri temeljna stupa – povjerljivosti, integritetu i dostupnosti. Ovi temelji zajednički se nazivaju CIA trijada sigurnosti informacija, prema engleskim riječima Confidentiality (povjerljivost), Integrity (integritet) te Availability (dostupnost), navode Samonas i Coss (2014). CIA trijada svoj početak formiranja bilježi već u 70-ima, a ozbiljnije bavljenje stupovima informacijske sigurnosti mogu se bilježiti krajem 80-ih godina prošlog stoljeća kada se pojavio prvi rašireniji malware (štetni softver) – Morris crv – koji je zarazio široki broj računala. CIA trijada danas se upotrebljava na globalnoj razini kao model za informacijsku sigurnost, a njezini stupovi predstavljaju principe kojima se svaki informacijski sustav koji vodi brigu o sigurnosti treba voditi:

1. Povjerljivost – samo autorizirani korisnici i procesi bi trebali imati pristup informacijama ili mogućnost da promijene te informacije. Juran (2012) ističe kako u slučaju nedostataka povjerljivosti sustav izlažemo različitim napadima poput hakiranja, trojanskim konjima ili pak neovlaštenim korisničkim aktivnostima.
2. Integritet – informacije se trebaju održavati na egzaktan način i nitko ne smije mijenjati te informacije na nepropisan način, bilo slučajno ili iz zlih namjera
3. Dostupnost – autorizirani korisnici moraju moći pristupiti informacijama kada

god to trebaju[4].

Prijedlog za usavršavanje i proširenje CIA trijade događa se 1998. godine kada je Donn Parker predložio proširenje stupova informacijske sigurnosti na šest elemenata umjesto dotadašnjih tri: povjerljivost, kontrola, integritet, autentičnost, dostupnost i korisnost. Ova „Parkerova heksada" kako je prozvana u sigurnosnim krugovima i na koju se referiraju Hintzbergen i Smulders (2010), tehnički ne donosi ništa novo prvotnoj trijadi, ali naglašava važnost različitih aspekata u informacijskoj sigurnosti. Autentičnost podrazumijeva istinitost o podrijetlu informacije, što bi moglo podrazumijevati digitalni otisak dokumenta kako bi se potvrdilo njegovo porijeklo. Kontrola ili vlasništvo odnosi se na posjedovanje kontrole nad informacijom koja se nalazi u sklopu informacijskog sustava u kojemu se ne smije dogoditi povreda povjerljivosti. Treći novi termin koji je Parker predložio u sklopu svoje heksade je korisnost – informacija je beskorisna ako nije iskoristiva u nekoj formi i ako joj se ne može ponovno pristupiti na neki od sigurnosnih načina. Iako su svi ovi „novi" pojmovi u nekom dijelu uključeni u temeljne pojmove trijade, one ipak pomažu uočiti dimenzije sigurnosnog aspekta koji se povremeno mogu previdjeti.

[4]CSO Online (n.d.) *The CIA Triad: Definition, Components and Examples*. URL: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html. Posjećeno 29.06.2021.

3. ZAKONSKI OKVIRI I NACIONALNA STRATEGIJA REPUBLIKE HRVATSKE

Kako bi se država odlučno borila protiv prijetnji informacijskom sustavu, potrebne su snažne legislative s kojima će institucije biti usklađene, a ujedno koje će pratiti međunarodnu scenu te rizike koji se događaju u drugim zemljama. Državni organi vezani uz informacijsku sigurnost organizirani su u piramidalnom obliku, kao što to ističu Klaić i Perešin (2011: 690). Prve tri razine organizacijske sheme čine provedbene politike sazdane od pravilnika, zakona i uredbi koje donose Ured Vijeća za nacionalnu sigurnost i ostali savjetnici, komplementirani sa aktima državnih tijela, CERT-a i Zavoda za sigurnost informacijskih sustava. Nakon provedbene politike, slijedi legislativni sloj koji se odnosi na politike informacijske sigurnosti. Njega čine pravilnici Ureda Vijeća za nacionalnu sigurnost, Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakon o tajnosti podataka te uredbe Vlade Republike Hrvatske. Na vrhu piramidalne sheme nalazi se Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njezinu provedbu (NN 108/2015). Ukratko će biti prikazani propisi svakog od navedenih dokumenata.

3.1 NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI I AKCIJSKI PLAN ZA NJEZINU PROVEDBU

Nacionalna strategija kibernetičke sigurnosti donesena je 2015. godine te služi kao krovni dokument vezan uz informacijsku sigurnost i sigurnost Interneta. Među glavnim ciljevima Strategije navedeni su:

1. Sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se u obzir uzela i kibernetička dimenzija i sigurnost vezana uz nju,

2. Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i

pouzdanosti kibernetičkog prostora,

3. Uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podatcima,

4. Jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora,

5. Poticanje razvoja usklađenih obrazovnih programa,

6. Poticanje razvoja e-usluga,

7. Poticanje istraživanja i razvoja,

8. Sustavni pristup međunarodnoj suradnji s ciljem prijenosa znanja.

Nacionalnom strategijom obuhvaćeni su svi sektori društva kao i načini suradnje dionika kibernetičke sigurnosti. Definirana su i područja kibernetičke sigurnosti koji obuhvaćaju javne elektroničke komunikacije, elektroničku upravu, elektroničke financijske usluge, kritična komunikacijska i informacijska infrastruktura i načini upravljanja kibernetičkim krizama. U Strategiji je među ciljevima istaknuto podizanje razine sigurnosti informacijskih sustava javnog sektora (Cilj B.2), kao i koraci za prevenciju rizika i poduzimanje mjera opreza (Cilj D.1 – Utvrditi kriterije za prepoznavanje kritične komunikacijske i informacijske infrastrukture; Cilj D.2 – Utvrditi obvezujuće sigurnosne mjere koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture; Cilj D.3 – Ojačati prevenciju i zaštitu kroz upravljanje rizikom). Ovo su bitni ciljevi kojim država priznaje važnost procjene rizika, bavljenja zaštitom informacijskog sustava te poduzimanja preventivnih koraka u cilju zaštite širokog broja građana.

Dio strategije posvećen je i kibernetičkoj sigurnosti, odnosno zaštiti osobnih podataka i podataka općenito, tehničkoj koordinaciji u obradi računalnih sigurnosnih incidenata, međunarodnoj suradnji na polju razmjena informacija, te obrazovanju, istraživanju, razvoju i jačanju svijesti o sigurnosti u kibernetičkom prostoru.

Zanimljiv cilj je i F.5 koji propisuje unificiranje pristupa u korištenju palete normi HRN ISO/IEC 27000, kojima je posvećeno posebno poglavlje u ovom radu. Zadavanje ovog cilja iznimno je bitno jer time Republika Hrvatska daje jasnu poruku za usvajanjem međunarodnih standarda izvrsnosti u informacijskoj sigurnosti i pripisuje to kao

obavezni pristup svim organima vlasti, ali i daje primjer svim organizacijama, poduzećima i građanima koji se na bilo koji način bave informacijama, skupljaju podatke ili posjeduju bazu podataka.

Akcijski plan za provedbu Strategije prati Nacionalnu strategiju te se propisuju provedbene mjere kojima je u cilju ispuniti strateške ciljeve dokumenta. U tu svrhu osnovano je Nacionalno vijeće za kibernetičku sigurnost kojemu je zadaća pratiti Strategiju i Akcijski plan te osigurati sustavno provođenje donesenih ciljeva i mjera.

3.2 ZAKON O SIGURNOSNO-OBAVJEŠTAJNOM SUSTAVU REPUBLIKE HRVATSKE

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06) iz 2006. godine službeno su osnovane SOA (Sigurnosno-obavještajna agencija) i VSOA (Vojna sigurnosno-obavještajna agencija), te su uspostavljeni organizacijski mehanizmi koji usmjeravaju rad agencija. Mehanizmi uključuju djelovanje Vijeća za nacionalnu sigurnost, Savjeta za koordinaciju sigurnosno-obavještajnih agencija, Ureda Vijeća za nacionalnu sigurnost, Zavoda za sigurnost informacijskih sustava te Operativno-tehničkog centra za nadzor telekomunikacija. Zakon propisuje opseg djelatnosti svih čimbenika sigurnosno-obavještajnog sustava Republike Hrvatske, te ovlašćuje agencije za djelatnosti prikupljanja informacija i njihovog obrađivanja i upotrebe.

3.3 ZAKON O INFORMACIJSKOJ SIGURNOSTI

Zakon o informacijskoj sigurnosti (NN 79/07) donesen je 2007. godine, a definira pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. U sklopu ovog Zakona službeno je definirano značenje informacijske sigurnosti:
„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“.

Zakon radi i razliku između neklasificiranih podataka, te klasificiranih podataka koji

su podijeljeni po stupnjevima tajnosti na „Povjerljivo“, „Tajno“, „Vrlo tajno“. Člankom 8. Zakona o informacijskoj sigurnosti definirana su i područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti: sigurnosna provjera, fizička sigurnost, sigurnost podatka, sigurnost informacijskog sustava te sigurnost poslovne suradnje. Nadalje, propisana su i središnja državna tijela za informacijsku sigurnost – Ured Vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava, kao i nacionalni CERT.

Ovaj Zakon sigurno bi trebao doživjeti novu inačicu koja bi detaljnije propisala načine informacijske sigurnosti, pogotovo s promjenom tehnologije, novih prijetnji, ugroza i rizika za sustave, ali i razvoj cjelokupne tehnološke slike Republike Hrvatske.

3.4 ZAKON O TAJNOSTI PODATAKA

Zakon o tajnosti podataka (NN 79/07) donesen je 2007. godine i s njim se utvrđuje pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom Zakona. Zakon se nadovezuje na Zakon o informacijskoj sigurnosti te nadalje objašnjava stupnjeve tajnosti te postupak klasificiranja i deklasificiranja podataka. Nadalje, Zakon objašnjava tko ima pristup klasificiranim podatcima i koja je procedura za davanje povjerljivih podataka institucijama koje ih traže.

Ovaj Zakon također bi trebao biti revidiran i usklađen sa zakonima na području EU, jer posljednja korekcija bila je 2008. godine i to objavom Uredbe o mjerama informacijske sigurnosti (NN 46/08).

3.5 ZAKON O SIGURNOSNIM PROVJERAMA

Zakon o sigurnosnim provjerama (NN 85/08) donesen je 2008. godine, a revidirana verzija objavljena je 2012. godine. Zakonom se uređuju pojam, vrste i stupnjevi sigurnosne provjere, sigurnosne zapreke i postupak provođenja sigurnosne provjere. Zakon se odnosi na sigurnosne provjere prilikom davanja pristupa klasificiranim podatcima, a odnosi se i na temeljne sigurnosne provjere te sigurnosne provjere u

svrhu zaštite sigurnosti štićenih osoba i objekata. Sigurnosna provjera ponavlja se svakih pet godina nad osobom koja obnaša neku službenu državnu dužnost ili radi u sklopu dvije sigurnosno-obavještajne agencije. Ovaj Zakon daje upute za sigurnosnom provjerom koja je nužna kako bi se osigurao kadar koji je povjerljiv, diskretan i osigurat će očuvanje informacija kojemu će imati pristup po zaposlenju ili istrazi. Ovo je također jedan od temelja međunarodnih normi za informacijsku sigurnost, koji upravo i sugeriraju da zaposlenici ne samo da provode temelje normi, već i da budu čuvari sigurnosti svojim postupcima i shvaćanjem organizacijskih potreba.

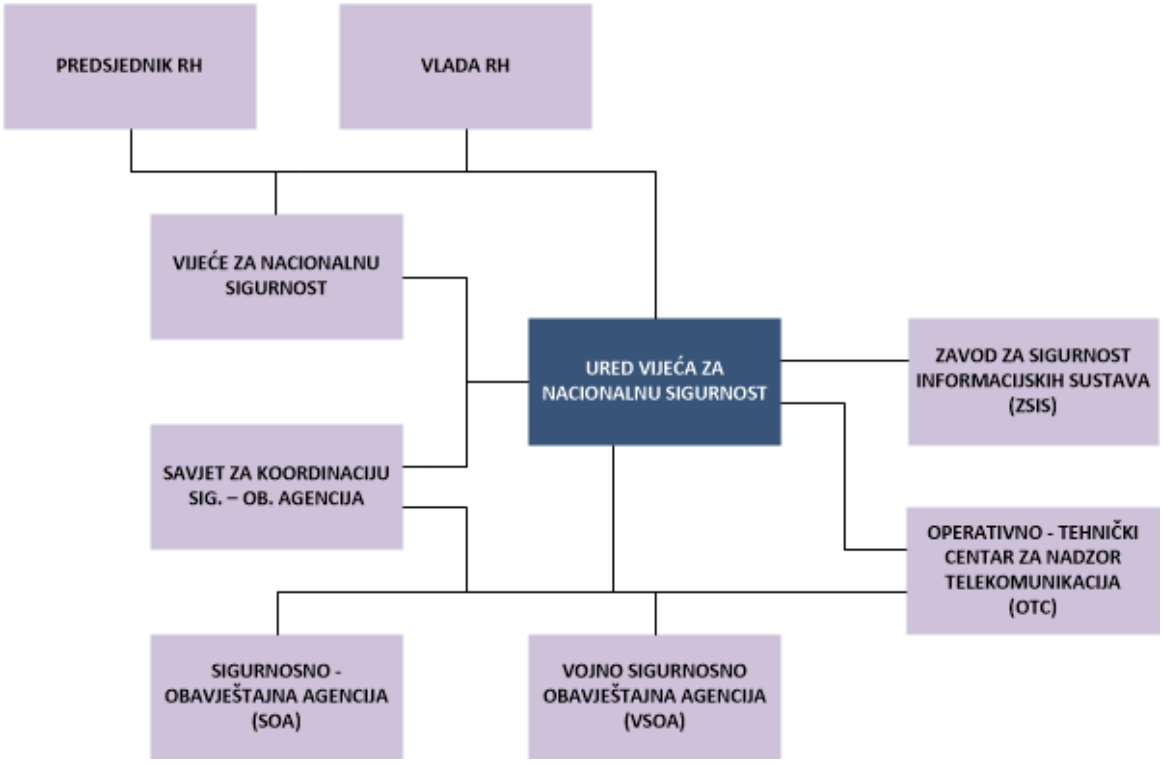
4. INFORMACIJSKA SIGURNOST U REPUBLICI HRVATSKOJ

U prethodnom poglavlju dan je pregled nacionalne strategije, zakona i pravilnika koji se odnose ili se referiraju na informacijsku sigurnost. U ovom poglavlju usredotočit će se na organizacije u Republici Hrvatskoj koje su direktno zadužene za informacijsku sigurnost, a time i domovinsku sigurnost u široj slici. Kroz pregled institucija i djelatnosti koje iste obavljaju, analizirat će se izvori i oblici prijetnji sustavu sigurnosti informacija u Republici Hrvatskoj, navest će se primjeri prijetnji koje je Republika Hrvatska već doživjela, te će se naposlijetku navesti i što je naučeno iz prijetnji te kako ojačati informacijsku sigurnost.

4.1 INSTITUCIJSKA UDRUŽIVANJA U SVRHU KOMPLETNE INFORMACIJSKE SIGURNOSTI

U Republici Hrvatskoj tema informacijske sigurnosti direktno je povezana sa sigurnosno-obavještajnom shemom, pa tako postoji nekoliko ureda i organizacija koja se aktivno bave temama zaštite građana od bilo kakvih prijetnji, opasnosti i vanjskih ugroza. Predsjednik Republike Hrvatske i Vlada Republike Hrvatske pod direktnom dirigencijom imaju dva tijela: Vijeće za nacionalnu sigurnost te Ured Vijeća za nacionalnu sigurnost. Iz njihovih djelatnosti granaju se daljnji uredi i organizacije koje svojim aktivnostima štite nacionalne interese. Shema sigurnosno-obavještajnog sustava Republike Hrvatske najbolje prikazuje povezanost institucija involviranih u

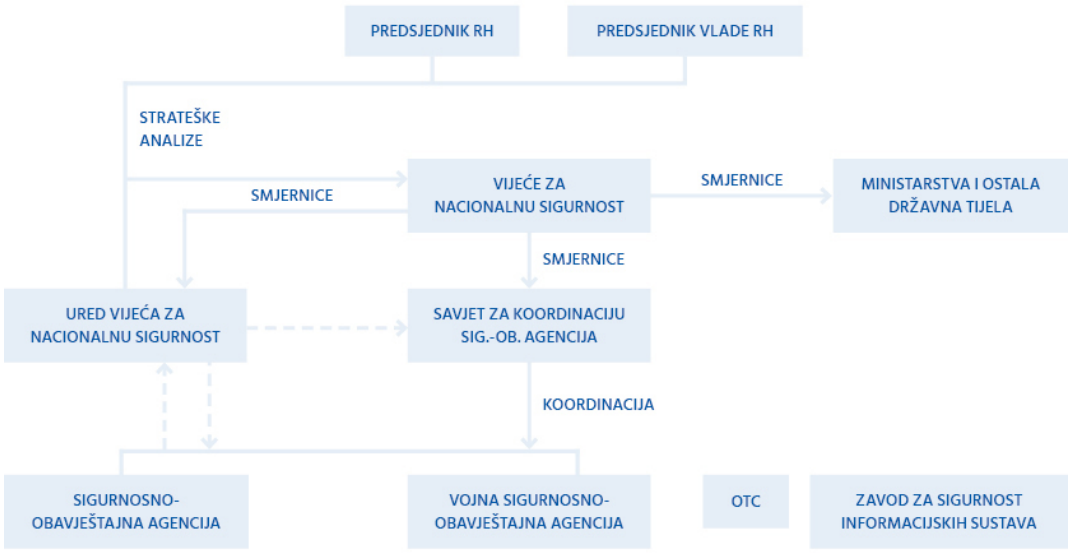
zaštitu građana Republike Hrvatske.



Slika 1. Sigurnosno-obavještajni sustav Republike Hrvatske

Izvor: uvns.hr

Shematski pristup djelovanja ovih institucija prikazan je i na SOA-inim internetskim stranicama.



Slika 2. Shema sigurnosno-obavještajnog sustava Republike Hrvatske

Izvor: soa.hr

Vijeće za nacionalnu sigurnost koordinacijsko je tijelo sigurnosno-obavještajnog sustava Republike Hrvatske. Njegova glavna zadaća je procjena sigurnosnih prijetnji i rizika. Na temelju procjena, Vijeće može donijeti smjernice i zaključke o načinima zaštite i ostvarivanja interesa nacionalne sigurnosti. Vijeće za nacionalnu sigurnost služi i kao vrsta savjetodavnog tijela za Predsjednika Republike Hrvatske i Vladu Republike Hrvatske jer im daje preporuke za usmjerenje rada agencija i tijela sigurnosno-obavještajnog sustava Republike Hrvatske. Članovi Vijeća za nacionalnu sigurnost su Predsjednik, predsjednik Vlade, ministar obrane, ministar unutarnjih poslova, ministar vanjskih poslova, ministar pravosuđa, savjetnik Predsjednika Republike Hrvatske, načelnik Glavnog stožera Oružanih snaga, predstojnik Ureda Vijeća za nacionalnu sigurnost, ravnatelji Sigurnosno-obavještajne agencije (SOA) i Vojno sigurnosno-obavještajne agencije (VOSA), kao i predsjednik Hrvatskog sabora. Po potrebi, druge osobe također mogu biti uključene u rad Vijeća.

SOA (Sigurnosno-obavještajna agencija) službeno je osnovana 2006. godine Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, i to spajanjem Protuobavještajne agencije i Obavještajne agencije u jedno tijelo. SOA prikuplja podatke od značaja za nacionalnu sigurnost, te prikupljene podatke analizira i obrađuje na način kako bi mogla Predsjednika Republike Hrvatske te Predsjednika

Vlade Republike Hrvatske pružati obavještajnu potporu. Cilj SOA-e je otkriti i spriječiti radnje pojedinaca ili skupine koje djeluju protiv interesa Republike Hrvatske. Uz zaštitu političkog poretka i samostalnosti Republike Hrvatske, SOA prikuplja i ostale informacije koje su od značaja za nacionalnu sigurnost, što uključuje i ekstremistička djelovanja, organizirani kriminal i korupciju, ali i neovlaštene ulaske u zaštićene informacijske i komunikacijske sustave državnih tijela te odavanju klasificiranih podataka. SOA pod područja rada specifično navodi i informacijsku sigurnost: „Razvojem tehnologije sve se više podataka važnih za nacionalnu sigurnost pohranjuje u informacijskim sustavima tijela državne uprave ili se razmjenjuju informacijsko-komunikacijskim kanalima. SOA je zadužena za otkrivanje i sprječavanje neovlaštenog ulaska u zaštićene informacijske i komunikacijske sustave državnih tijela te odavanje klasificiranih podataka.“. SOA na svojim internetskim stranicama ističe značaj međuresorne suradnje, pa tako po pitanju informacijske sigurnosti surađuje s „tijelima javne vlasti, državnim institucijama te drugim institucijama i ustanovama. Posebno je ta suradnja intenzivna s Vladom RH, UVNS-om, ZSIS-om, MUP-om, VSOA-om, Ministarstvom pravosuđa, DORH-om i MVEP -om.“.

VSOA (Vojno sigurnosno-obavještajna agencija) osnovana je istim Zakonom kojim je osnovana i SOA te čini drugu od ukupno dvije sigurnosno-obavještajne agencije u Republici Hrvatskoj. VSOA djeluje pod Ministarstvo obrane, a služi kao potpora Ministarstvu obrane te Oružanim snagama za „izvršenje zadaća obrane opstojnosti, suvereniteta, neovisnosti i teritorijalne cjelovitosti Republike Hrvatske.“. Slično djelovanju SOA-e, ali u vojnom sektoru, VSOA prikuplja, analizira, obrađuje i ocjenjuje podatke korisne za obrambeni sustav Republike Hrvatske.

Savjet za koordinaciju sigurnosno-obavještajnih agencija za ulogu ima usklađivanje rada agencija i drugih tijela sigurnosno-obavještajnog sustava, te provođenje odluka Vijeća za nacionalnu sigurnost. U sklopu Savjeta kao članovi zasjedaju: član Vlade zadužen za nacionalnu sigurnost koji obnaša dužnost predsjednika Savjeta, savjetnik Predsjednika Republike Hrvatske za nacionalnu sigurnost, predstojnik Ureda Vijeća za nacionalnu sigurnost te ravnatelji SOA-e i VOSA-e. Po potrebi, sjednicama Savjeta mogu se pridružiti i druge osobe relevantno za ovo polje.

ZSIS (Zavod za sigurnost informacijskih sustava) središnje je državno tijelo kojem je u cilju tehnički podržati državne institucije koje se bave informacijskom sigurnosti te su zaduženi za provođenje i održavanje standarda sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanjem materijalima koji se koriste u razmjeni klasificiranih informacija te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. ZSIS postavlja sigurnosne standarde koje sva državna tijela, jedinice lokalne i regionalne samouprave te pravne osobe s javnim ovlastima moraju slijediti.

Od državnih tijela, okvir sigurnosno-obavještajnog djelovanja u Republici Hrvatskoj zatvara OTC (Operativno-tehnički centar za nadzor telekomunikacija). Ovaj centar je državno tijelo koje jedino ima ovlasti tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa. Njegovim djelovanjem upravlja SOA i druga tijela koja su zakonom ovlaštena, a nadziranje na zahtjev tijela i/ili SOA-e odobrava Vrhovni sud.

Osim državnih tijela, u Republici Hrvatskoj postoji i posebna institucija koja se bavi isključivo informacijskom sigurnosti. CERT je dio CARNET-a (Hrvatska akademska i istraživačka mreža) te je službeno osnovan 2007. godine. CERT obnaša ulogu „nacionalnog tijela za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno -sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj“. CERT promatra podatkovni promet nad .hr domenama te nad hrvatskim IP adresama te prikuplja podatke, obrađuje ih i djeluje u skladu sa Zakonom o informacijskoj sigurnosti Republike Hrvatske i u skladu s nacionalnim tijelima. Na CERT-ovoj internetskoj stranici građani mogu prijaviti incidente, provjeriti ranjivost svojih podataka ili računala, pristupiti bazi znanja koja sadrži različite dokumente, prezentacije, brošure, savjete i ostali edukativni materijal za šire obrazovanje javnosti o informatičkim sustavima i prijetnjama nad istima. Uz to, CERT daje tjedne i godišnje izvještaje o zabilježenim incidentima gdje pojedinci mogu saznati koliko prijetnji je CERT detektirao ili spriječio. CERT redovito daje i novosti o novim prijetnjama, što CERT čini veoma relevantnom stranicom i institucijom za sve novosti o informatičkoj sigurnosti u Republici Hrvatskoj.

Uz CERT, zgodno je za napomenuti kako je do 2018. godine aktivnosti vezane uz informacijsku sigurnost obnašao i CIS. Centar informacijske sigurnosti (CIS) osnovan

je 2010. godine na poticaj LSS-a (Laboratorija za sustave i signale) Zavoda za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva (FER) u Zagrebu. CIS se uskoro promeće kao referentni autoritet u široj javnosti po pitanju informacijske sigurnosti, što je i u smislu djelovanja za sami CIS. Djelovanje CIS-a usmjereno je prema podizanje svijesti i sposobnosti šireg građanstva na temu informacijske sigurnosti, što uključuje redovito informiranje javnosti o hakerskim napadima, potencijalno štetnim internetskim stranicama, važnosti zaštite osobnih podataka na Internetu i slično. U bilo kojem trenu, građani su mogli posjetiti CIS-ovu internetsku stranicu te se informirati o posljednjim novostima iz svijeta informacijske sigurnosti, a uz to su mogli pronaći i edukativni materijal o osnovnim internetskim procesima, pojmovima, zaštiti svojeg računala i Interneta i sličnome. Bitno za napomenuti je i da, uz državna tijela te centre na hrvatskoj sceni koja se bavi informacijskom sigurnosti i zaštitom, postoji i niz privatnih poduzeća koje nude usluge zaštite i savjetovanja malim, srednjim i velikim poduzećima.

4.2 PRIJETNJE SUSTAVU SIGURNOSTI INFORMACIJA

Prije nego što se donese određeni zaključak ili radnja kojemu je u cilju spriječiti prijetnju, potrebno je znati s kojim prijetnjama se moguće susresti na polju sigurnosti informacija. Iz tog razloga, ključno je razlikovati rizik, prijetnje i ranjivosti kao temeljne pojmove informacijske sigurnosti.

4.2.1 RIZIK, PRIJETNJA I RANJIVOST SUSTAVA

Rizik, prijetnja i ranjivost terminologija je koja se ubraja među sastavne dijelove informacijske sigurnosti. Kako bismo znali djelovati i procijeniti na koji način djelovati, važno je razumjeti sve sastavnice. Poznate međunarodne norme koje su namijenjene informacijskoj sigurnosti (ISO 27001, ISO 27002, ISO 17799 primjerice) u svojoj dokumentaciji također navode definicije ovih termina iz prethodno spomenutih razloga, a bitno je za napomenuti i kako su hrvatski propisi informacijske sigurnosti usklađeni s ovim normama. Klaić (2010: 2) sažima definicije međunarodnih normi, pa tako *rizik* parafrazira kao kombinaciju vjerojatnosti određenog događaja i njegovih utjecaja. Peraković i Cvitić (2015) rizik definiraju kao „vjerojatnost ostvarenja svjesnog, neželjenog događaja“.

Klaić parafrazira *prijetnju* kao „potencijalni uzrok neželjenog incidenta koji može naštetiti sustavu ili organizaciji“, dok Peraković i Cvitić definiraju prijetnju kao ljudsku namjeru ili čin koji za cilj ima iskoristiti manjkavosti ili ranjivosti informacijskog sustava.

Naposlijetku, *ranjivost* za Peraković i Cvitić asignira slabost sustava, odnosno moguće propuste koje sustav ima i koji se mogu iskoristiti na štetan način. Klaić parafrazira ranjivost kao slabost resursa ili skupine resursa koje prijetnje mogu iskoristiti.

Iz pruženih definicija i parafraza moguće je iščitati kako rizik, prijetnja i ranjivost nisu odvojeni termini, već se itekako nadopunjavaju. Prijetnja se može realizirati isključivo ako postoje propusti u sustavu, odnosno ako je sustav ranjiv. S druge strane, rizik je pojam koji je konstantno prisutan u bilo kojem sustavu. Jedini način kako spriječiti rizik jest da se bude svjestan prijetnji, da postoje spremni procesi koji će ciljati prijetnju, te ako se ukloni ili smanji ranjivost sustava. Upravo iz te namjere su uspostavljene spomenute međunarodne norme, dok će jedna od njih - ISO/IEC 27001:2013 kao najpopularniji standard informacijske sigurnosti u svijetu – biti predstavljena zasebno kasnije. Prije toga, predstavit će se vrste prijetnji koje sustav može susresti i koje mu mogu naštetiti.

4.2.2 VRSTE PRIJETNJI

Klasifikacija prijetnji bitna je kako bi se zaštitio informacijski sustav, jer u slučaju nepostojanja poznavanja prijetnje, ne postoji ni način zaštite od istog. Kolokvijalno – najgori je onaj neprijatelj kojega ne poznaješ. Gerić i Hutinski (2007) dali su pregled vrsti prijetnji informacijskim sustavima grupiranih u ukupno sedam skupina.

1. *Pogreške i izostavljanja* prijetnje su koje se često podcjenjuju i izazvane su ljudskim faktorom. Primjerice, djelatnik koji svakodnevno unosi podatke u bazu zbog količine podataka može izazvati nenamjernu grešku koja može utjecati na točnost i pouzdanost podataka ili pak izložiti podatke nekom riziku. Mogućnost utjecanja na ovu prijetnju je veoma mala, odnosno u sklopu sustava je nepredvidljiva. Autori sugeriraju kako je u ovom slučaju najbolje usredotočiti se na edukaciju i dobrobit zaposlenika kako bi zaposlenici bili odmorniji, informiraniji i koncentriraniji na posao. Postoji i mogućnost

programerskih grešaka koji rezultiraju takozvanim „bugovima“ koji mogu uzrokovati disfunkcionalnost sustava koji je programiran. U tu svrhu, IT sektor u posljednje vrijeme ulaže resurse u ljude koji podrobno testiraju cijeli sustav prije nego se isti stavi na živu verziju dostupnu korisnicima.

2. *Prevare i krađe* odnose se na djelatnosti unutar poduzeća, organizacija ili državnih organa. Osim unutarnjih djelatnosti, postoji mogućnost unajmljivanja pojedinaca koji će izvršiti prevaru ili krađu umjesto pojedinca unutar poduzeća, organizacije ili državnog organa. Aktivnosti se odnose na krađu novaca, podataka ili nečeg trećeg od kojeg će pojedinac profitirati osobno. Ovo je ponovno ljudska komponenta na koju se ne može tako lako utjecati, osim strožim uvjetima zaposlenja, temeljitom provjerom pojedinčeva motiva zaposlenja i socioekonomskih uvjeta i sličnog.

3. *Sabotaža od strane zaposlenika* odnosi se na direktno uništenje informacija ili sustava od strane zaposlenika, koja bi ubrajala uništavanje hardvera, podmetanje logičkih bombi za uništenje programa ili podataka, krivi unos podataka, uzrokovanje rušenja sustava, brisanje podataka, promjena podataka ili pak sadržavanje podataka za sebe.

4. *Gubitak fizičke ili infrastrukturne podrške* odnosi se na gubitak električne energije, komunikacije, poplave, požara i bilo koje druge elementarne ili prirodne nepogode na koju se ne može direktno utjecati.

5. *Hakeri* se djelomično mogu povezati sa točkom 2, no njihovi motivi nisu uvijek jasni. Hakeri su pojedinci koji na neautorizirani način nastoje ući u sustav i iskoristiti informacije za svoju korist ili korist pojedinca koji ih je unajmio da izvrše ilegalni upad u sustav. Ukoliko su hakeri uspješni u svom naumu, mogu upasti u bilo koju bazu i ukrasti sve podatke koje baza skladišti. Zbog ranjivosti koju donose ljudima, hakeri se smatraju iznimno opasnima.

6. *Zlonamjerni softveri (malware)* dijele se na kompjuterske viruse, trojanske konje te crve. Kompjuterski virusi dio su programskog koda koji se, jednom kada su skinuti, skloni replikaciji i izazivanju ponašanju programa koji nisu više pod kontrolom korisnika (formatiranje kompjuterskog diska, brisanje podataka

i slično). Trojanski konji su programi koji se samostalno instaliraju na kompjuter i vrše neželjene radnje koje ponekad mogu rezultirati gubitkom cijelog hardvera. Crvi su programi koji utječu na performanse sustava na negativan način – opterećivanjem performansi smanjuje se radna aktivnosti i sposobnost kompjutera da vrši maksimalni broj radnji koji bi u normalnim uvjetima izvršio.

7. *Prijetnje osobnoj sigurnosti* danas su rastuća prijetnja koje su institucije već pokušale regulirati - primjerice, u Europi na razini Europske unije donesen je GDPR (General Dana Protection Regulation 2016/679) koji propisuje svim poduzećima koja spremaju korisničke podatke kako ti podatci trebaju biti spremljeni, te daju pravo korisnika da zahtijeva brisanje svih svojih osobnih podataka s određenog servera ili baze podataka poduzeća. Ova prijetnja odnosi se na krađu osobnih podataka, od podataka s osobne iskaznice, preko bankovnih podataka, pa sve do privatnih stvari poput liječničkih podataka.

Nakon što se pogleda ova raščlamba prijetnji autora, sve navedene prijetnje mogu se svrstati u četiri generalne kategorije i to prema izvorima prijetnje:

1. Prirodne nepogode
2. Tehničke prijetnje
3. Nenamjerne prijetnje uzrokovane ljudskim faktorom
4. Namjerne prijetnje uzrokovane ljudskim faktorom.

Upravo ovakvu kategorizaciju navodi i ISO 17799 međunarodna norma, kao i sve naknadne ISO 27000 norme koje služe za zaštitu informacijskih sustava.

Dodatno, uz vrste prijetnji možemo identificirati i vrste napada koje se mogu dogoditi nad informacijskim sustavom i spadaju u maliciozne napade, odnosno napade kojima je u cilj nanijeti štetu ili okoristiti se na tuđi račun. Neke od njih smo već spomenuli tijekom objašnjavanja vrsta prijetnji, a detaljno ih razlaže Vuković (2012: 17-20):

1. Kibernetski kriminal – usmjeren na prevare na polju internetskog bankarstva
2. Kibernetska špijunaža – usmjeren prema krađi informacija

3. Kibernetski terorizam – usmjeren prema napadima na informacijske sustave
4. Kibernetsko ratovanje – simbiotička aktivnost pokrenuta od države prema drugoj državi.

4.3 PRIMJERI PRIJETNJI INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ

CERT je u Godišnjem izvještaju za 2020. godinu predstavio statistiku o obrađenim incidentima i ranjivostima koje je tijekom protekle godine zabilježio u izvršavanju svojih aktivnosti. Tijekom 2020. godine zabilježeno je ukupno 1710 prijava za računalno-sigurnosne incidente, a kao vodeći tipovi incidenata zabilježeni su:

1. *Phishing URL* - 446 slučajeva, s bilježenjem ovog tipa incidenta u porastu u usporedbi s 2019. godinom. Phishing URL odnosi se na lažna mrežna sjedišta, gdje napadači postavljaju krive linkove na stvarne internetske stranice i tako obmanjuju posjetitelja, skupljajući njegove podatke;
2. *Phishing* (277 slučajeva, također u porastu). Phishing se odnosi na izvlačenje podataka korisnika tako da preko elektroničke pošte ili servisa za dopisivanje pošalje zahtjev korisniku za promjenom podataka, skupljajući tako osobne podatke korisnika;
3. *Pogađanje zaporki* (205 slučajeva, također u porastu). Radi se o pokušaju provale u korisničke račune pogađajući zaporku koju korisnih ima za određeni mrežni sustav, poput lozinki društvenih mreža, elektroničke pošte i sličnoga;
4. *Web defacement* (188 slučajeva, također u porastu). Web defacement odnosi se na kompromitirano mrežno sjedište koje ima izmijenjeni izgled i sadržaj stranice.
5. *Malware URL* (132 slučaja, također u porastu). Malware URL označava poveznice koje sadrže zlonamjerni programski kod na kompromitiranom mrežnom sjedištu – kada korisnik klikne na takvu poveznicu, na njegovo računalo ili pametni mobitel skida se malware koji uništava dijelove softvera, uništava podatke ili ih krade.

Uz navedene tipove incidenata koji imaju najveći broj primjera, CERT navodi i po

jedan slučaj napada na aplikacijskom sloju (DOS), zlonamjerno rudarenje kriptovalute (takozvani cryptojacking) i slično. Pandemijski uvjeti uzrokovani pojavom COVID-19 u svim zemljama svijeta također su pokrenuli porast računalnih incidenata, pa su zabilježene aktivne phishing kampanje u kojima se šalju lažne poruke i privitci o lijeku i lažnim vijestima. Početkom 2020. godine zabilježen je i DDoS napad na mrežno sjedište Srce-a (Sveučilišnog računalnog centra) koji je uzrokovao poteškoće u radu.

U prethodnom potpoglavlju istaknuto je kako je potrebno poznavati prijetnje kako bi se uspješno razvili sustavi zaštite informacijske sigurnosti. Unatoč tome što je većina prijetnji iz CERT-ovog Godišnjeg izvještaja poznata, ipak je s vremena na vrijeme nemoguće razviti sustave zaštite protiv prijetnji iz razloga što napadači uvijek osmisle novi, inovativniji način prevare korisnika. Ipak, neki primjeri napada i reakcija na iste pokazuje kako poznavanje rizika i razrada akcija protiv rizika može uroditi plodom i može zaštititi informacijski sustav na vrijeme. U narednim redovima bit će predstavljeni slučajevi prijetnji informacijske sigurnosti koji su bili zastupljeni na području Republike Hrvatske u posljednje vrijeme.

4.3.1 NAPAD NA MVEP

U drugoj polovici 2016. godine zabilježen je hakerski napad na kompjutorski sustav Ministarstva vanjskih poslova Republike Hrvatske[56], koji je nastavak hakerskog napada na političke institucije u Njemačkoj i Francuskoj. Zahvaljujući upravo prethodnim napadima, Republika Hrvatska dobila je upozorenje sigurnosno-obavještajnih agencija iz Europe te je uspjela reagirati na napad i zaštititi podatke. Inače, Ministarstvo vanjskih poslova povezano je putem sustava sa Uredom tadašnje predsjednice, kao i s Uredom premijera, više ministarstava i hrvatskim diplomatskim misijama u inozemstvu. Ovaj sustav veoma je aktivan u razmjeni informacija, te se radi o nizu povjerljivih dokumenata i prepisaka s diplomatskim misijama u svijetu. Da

[5]Jutarnji.hr (03.12.2016.) *OVAKAV HAKERSKI NAPAD U HRVATSKOJ NIKADA NIJE ZABILJEŽEN Otkrivamo tko je zaslužan sa spašavanje podataka iz sustava MVEP-a*. URL: https://www.jutarnji.hr/vijesti/hrvatska/ovakav-hakerski-napad-u-hrvatskoj-nikada-nije-zabiljezen-otkrivamo-tko-je-zasluzan-sa-spasavanje-podataka-iz-sustava-mvep-a-5339295 Posjećeno 27.06.2021.

[6]Dnevnik.hr (02.12.2016.) *Hakirano hrvatsko Ministarstvo vanjskih poslova*. URL: https://dnevnik.hr/vijesti/hrvatska/na-mvep-izvrsen-hakerski-napad-niti-jedna-vazna-informacija-nije-kompromitirana-ministar-stier---459254.html?fb_comment_id=1162642803783715_1162996163748379. Posjećeno 27.06.2021.

su hakeri uspjeli probiti ukrasti navedene informacije (iako su se domogli nekih dokumenata koji su navodno od manje važnosti za cijeli sustav), došli bi u posjet ključnih informacija od nacionalnog interesa te bi u ugrozu stavili cijeli politički sustav Republike Hrvatske. Iako su hakeri uspjeli probiti antivirusne programe, zahvaljujući pomoći inozemnih sigurnosnih službi, ubačeni spyware uspješno je izoliran te je ostatak informacijskog sustava zaštićen od daljnjeg proboja.

Napad na Ministarstvo vanjskih poslova 2016. godine nije bio jedini napad na hrvatske institucije – slični hakerski napadi zabilježeni su u veljači 2012. godine kada je hrvatski ogranak hakerske skupine Anonymous srušio stranicu ZAMP-a, Ministarstva vanjskih poslova te hakirao stranicu Ureda predsjednika zbog ACTA-e[78] (Trgovinskog sporazuma protiv krivotvorenja). Hakerski napad nad Ministarstvom vanjskih poslova ponovno se dogodio u travnju 2012. godine kada je hakerska skupina Teampoison srušila stranicu navedenog ministarstva, motivirani sudjelovanjem Republike Hrvatske u NATO-ovim operacijama[9].

4.3.2 SOA NA WIKILEAKSU

Iako se ne radi o direktnom napadu na hrvatske servere i institucije, slučaj otkrivanja poslovanja SOA-e na WikiLeaksu, servisu koji objavljuje povjerljive dokumente iz raznih anonimnih izvora, itekako je bila neugodna epizoda u sigurnosnim krugovima. Naime, u srpnju 2017. godine hrvatski mediji otkrili su kako je SOA planirala kupovinu softvera koji nadzira komunikaciju na servisima za dopisivanje i video pozive, poput WhatsAppa, Vibera, Skypea i sličnoga[1011]. Hakerski napad na bazu podataka Hacking

[7]Jutarnji.hr (16.02.2012.) *Anonymous hakirao stranice Ministarstva vanjskih poslova*. URL: https://www.jutarnji.hr/vijesti/hrvatska/anonymous-hakirao-stranice-ministarstva-vanjskih-poslova-ne-zelimo-nikome-naskoditi-samo-upozoravamo-na-acta-u-1639545. Posjećeno 27.06.2021.

[8]Index.hr (16.02.2021.) Anonymousi hakirani Ministarstvo vanjskih poslova. URL: https://www.index.hr/vijesti/clanak/Anonymousi-hakirali-Ministarstvo-vanjskih-poslova-Ali-mi-nismo-nadlezni-za-ACTA-u/599445.aspx Posjećeno 27.06.2021.

[9]Tportal (04.03.2012.) *Opet hakirana stranica Pusićkinog ministarstva*. URL: https://www.tportal.hr/vijesti/clanak/opet-hakirana-stranica-pusickinog-ministarstva-20120403. Posjećeno 27.06.2021.

[10]24sata.hr (12.07.2015.) *Hakerski skandal: SOA htjela kupiti softver za prisluškivanje* URL: https://www.24sata.hr/tech/hakerski-skandal-soa-htjela-kupiti-softver-za-prisluskivanje-427916 Posjećeno 27.06.2021.

Teama, tvrtke koja pruža uslugu korištenja i održavanja spomenutog softvera, otkrio je korespondenciju između Hacking Teama, SOA-e, VSOA-e i Ministarstva unutarnjih poslova, te tvrtke koja je posredovala između navedenih institucija. Hakeri koji su probili zaštitu tvrtke Hacking Team i njihovog softvera za prisluškivanje na Internetu su učinili dostupnim izvorni kod za softver, te tako omogućili i drugim hakerima i tvrtkama da saznaju za propuste u zaštiti. SOA se ipak nije upustila u kupnju navedenog softvera. U slučaju da se akvizicija dogodila, SOA-ino posjedovanje softvera postalo bi bezvrijedno, s obzirom da se sigurnost i vrijednost softvera smanjila nakon hakerskog napada, što bi ujedno utjecalo i na rad SOA-e kao takve.

4.3.3 POKUŠAJ HAKIRANJA HRVATSKIH INSTITUCIJA

U rujnu 2017. godine SOA je izvijestila u svom javnom izvješću kako su u 2018. godini presreli nastojanja kibernatičkih napada na informacijske i komunikacijske sustave državnih organa Republike Hrvatske[12]. SOA nije direktno navela tko je bio organizator napada, no hrvatski mediji smatraju da su napadi bili orkestrirani od strane Rusije i Kine. SOA je u javnom izvješću navela kako uspješnost kibernatičkih napada pokazuje kako postoji nedostatak sigurnosnih politika koje bi povećale otpornost sustava. U 2016. godini dogodilo se ukupno šest sličnih napada, među kojima su i već spomenuti napadi na Ministarstvo vanjskih poslova. SOA je također 2019. i 2020. godine upozorila na povećane informatičke prevare i krađu informacija kao nove vrste hibridnih ugroza. Jedna od njih je i širenje lažnih vijesti u svrhu destabilizacije zemlje i stvaranja negativne slike o zemlji u međunarodnoj zajednici[13].

[11] ICT Business (n.d.) *ŠPIJUNSKA AFERA: Hacking Team, SOA, Alfatec, Sedam IT i Diverto u kolopletu hakiranja ili kako su progonjeni uvijek za korak ispred progonitelja*. URL: https://www.ictbusiness.info/vijesti/spijunska-afera-hackingteam-soa-alfatec-i-sedam-it-i-dvierto-u-kolopletu-hackiranja-ili-kako-su-progonjeni-uvijek-za-korak-ispred-progonitelja.phtml Posjećeno 27.06.2021.

[12]Telegram.hr (n.d.) *Godišnje izvješće SOA-e: Rusi i Kinezi pokušavali su hakirati hrvatske institucije.* URL: https://www.telegram.hr/politika-kriminal/godisnje-izvjesce-soa-e-rusi-i-kinezi-pokusavali-su-hakirati-hrvatske-institucije/ Posjećeno 28.06.2021.

[13]Telegram.hr (n.d.) *SOA posebno upozorava na hibridne trolove.* URL: https://www.telegram.hr/politika-kriminal/soa-posebno-upozorava-na-hibridne-trolove-koji-vrebaju-gradane-i-politicare-kazu-ima-ih-posvuda/ Posjećeno: 1.7.2021.

4.3.4 HAKIRANI PODATCI FACEBOOK KORISNIKA

U travnju 2021. godine CERT je izvijestio[14] kako je došlo do proboja Facebookovog sigurnosnog sustava, te kako je na hakerskom portalu objavljeno preko 500 milijuna osobnih podataka Facebook korisnika, što je uključivalo imena, prezimena, elektroničke adrese, brojeve telefona i lokacije. Ovo je bio samo nastavak curenja podataka s Facebooka, jer je zadnji zabilježeni proboj Facebooka bio u prvoj polovici 2019. godine. Facebook je tada tvrdio da je ranjivost zakrpana, no hakeri su ponovno pronašli nove ranjive strukture u Facebookovoj bazi podataka. CERT je izvijestio javnost kako mogu provjeriti jesu li i njihovi podatci iskorišteni putem dvije stranice: Have I Been Zucked, koja se odnosi na podatke s društvenih mreža, te Have I Been Pwned, koja se odnosi na podatke koji su iscurili na portalima. Naknadnim istraživanjem otkrilo se kako su osobni podatci 660 tisuća hrvatskih korisnika bili zahvaćeni ovim incidentom[15].

Koliko god bili upoznati s vrstama prijetnji na regionalnoj i državnoj razini, ponekad se teško boriti s inovativnošću hakera koji su motivirani različitim sredstvima – od slanja poruka zbog neslaganja potezima države, pa do krađe podataka za tuđu korist. Borba za informacijsku sigurnost konstantna je, a kako se razvija tehnologija, tako se otvara i sve veća potreba za što kompleksnijim sustavima zaštite. Ovaj problem prepoznat je na međunarodnoj razini, a najaktivnije djelatnosti i konkretni potezi događaju se u Međunarodnoj organizaciji za standardizaciju (ISO – International Organization for Standardization), koji nastoje donositi norme koje će osigurati sigurnost i kvalitetu sustava. Jedan od ključnih normi za informacijsku sigurnost je ISO/IEC 27001:2013, norma koja je postala najpopularniji standard informacijske sigurnosti na svijetu.

[14]CERT.hr (n.d.) *Procurilo 533 milijuna telefonskih brojeva i osobnih podataka korisnika Facebooka.* URL:https://www.cert.hr/procurilo-533-milijuna-telefonskih-brojeva-i-osobnih-podataka-korisnika-facebooka/ Posjećeno: 1.7.2021.

[15]Bug.hr (03.04.2021.) *Osobni podaci 660 tisuća hrvatskih korisnika Facebooka procurili u javnost* URL: https://www.bug.hr/sigurnost/osobni-podaci-660-tisuca-hrvatskih-korisnika-facebooka-procurili-u-javnost-20366 Posjećeno: 1.7.2021.

5. STANDARD INFORMACIJSKE SIGURNOSTI U SVIJETU – ISO/IEC 27001 NORME

Međunarodna organizacija za standardizaciju (eng. ISO - International Organization for Standardization) glavni je autoritet za donošenje međunarodnih standarda. ISO je osnovan 1947. godine i djeluje kao neovisna međunarodna nevladina organizacija koja okuplja ukupno 165 zemalja članica. Misija i vizija ISO-a kao međunarodne organizacije je donošenje međunarodnih normi i standarda kako bi različitim poduzećima, organizacijama i državnim organima pomogli u razvoju proizvoda i usluga koji su sigurni, pouzdani i vrhunske kvalitete. ISO je tijekom svojih godina djelatnosti iznjedrio preko 20.000 standarda koji pokrivaju sve od proizvodnje proizvoda i tehnologije, pa sve do sigurnosti hrane, zdravlja, a naposlijetku i informacijskog sustava. U narednim redovima analizirat će se značaj ISO/IEC 27001:2013 međunarodne norme koja se danas smatra najboljim standardom informacijske sigurnosti u svijetu, te u fokus stavlja zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka unutar organizacije.

5.1 TEMELJI ISO/IEC 27001 NORMI

U prethodnim dijelovima rada spomenute su tri ISO norme: ISO 27001, ISO 27002, ISO 17799. *ISO 17799* prethodnik je ISO 27001 obitelji normi, te je to ISO certifikat koji se odnosi na informacijsku tehnologiju, odnosno sigurnosne tehnike kojima se implementira, održava i unapređuje informacijska sigurnost u organizaciji. Norma je

donesena 2005. godine na temelju norme iz 2000. godine (ISO/IEC 17799:2000), stoga je puni naziv ove međunarodne norme ISO/IEC 17799:2005. Norma obuhvaća najbolje primjere kako kontrolirati određene segmente informacijske sigurnosti popust politike sigurnosti, organizaciju informacijske sigurnosti, organizaciju imovine, sigurnost ljudskih resursa, fizičku i okolišnu sigurnost, akviziciju, razvoj i održavanje informacijskog ustava i slično. Norma je utemeljena na rezultatima ekstenzivne procjene rizika te je jedna od odrednica normi temeljita procjena rizika određene organizacije i djelovanje sukladno prepoznatim rizicima. Korekcije norme donesene su 2007. godine, a naposlijetku ovu normu mijenja ISO/IEC 27002:2013. Kratica IEC u nazivu ovih normi označava Međunarodno elektrotehničko povjerenstvo (International Electrotechnical Comission) koja je zadužena za sve standarde u području elektrike, elektrotehnike i sličnih tehnologija. IEC je osnovan 1906. godine te je glavni autoritet u oblasti elektrotehnologije.

ISO/IEC 27001 i ISO/IEC 27002 međunarodni su standardi iz iste obitelji normi, te su namijenjeni isključivo standardima u području informacijske sigurnosti. Oni su ujedno i glavni autoritet za sve ostale međunarodne norme donesene na njihovim temeljima, koji se protežu do broja ISO/IEC 27050, ISO/IEC 273013 te ISO/IEC TR 27103, a obuhvaćaju širok spektar tema – od sigurnosti pohrane, analize i interpretacije digitalnih dokaza, sigurnosnih tehnika, menadžmenta incidenata, osiguranja pristupa IP adresama i VPN-ovima, kibernetičku sigurnost i ostalo. Glavna razlika između ISO/IEC 27001 i ISO/IEC 27002 normi je ta što ISO/IEC 27002 ne nudi zahtjeve i potrebe sustava kao što to nudi ISO/IEC 27001, no s druge strane ISO/IEC 27002 proširuje originalni tekst i nadopunjava ga sa informacijama o sigurnosti mobilnih uređaja i savjetima za implementaciju sigurnosnih mjera. Današnja preporuka stručnjaka je implementirati obje norme u svoj informacijski sustav.

5.2 ISO/IEC 27001 NORME

ISO/IEC 27001 međunarodna je norma koja se danas smatra najvrsnijim standardom informacijske sigurnosti u svijetu. Prema podatcima ISO-a iz 2019. godine, u svijetu je izdano ukupno 36.362 ISO/IEC 27001 certifikata, a zemlje koje su vodeće u posjedovanju ovih certifikata su Kina (8.356), Japan (5.245), Velika Britanija (2.818),

Indija (2.309), Italija (1.390) i Njemačka (1.175). Po podatcima iz 2019. godine, Hrvatska ima ukupno 190 certifikata na ukupno 207 područja. Najviše certifikata, za sektore za koje je to poznato, ima područje informacijskih tehnologija. Djelatnost ove skupine normi može se podvesti pod kraticu *ISMS* (eng. Information Security Management System), odnosno sustav upravljanja sigurnošću informacija, što označava način pristupa upravljanju informacijskog sustava tako da informacije budu osigurane i kako bi se zaštitile od neovlaštenog korištenja, upotrebe, krađe i bilo kojeg drugog potencijalnog rizika za informacijski sustav.

Iako je popularno mišljenje da norme propisuju sve korake kako nešto napraviti i aplicirati, u slučaju ISO/IEC 27001 normi ovo nije pravilo, niti namjera. Naime, informacijska sigurnost stavljena u prvi plan ove norme toliko se razlikuje od organizacije do organizacije, da je nemoguće i pomalo neprofesionalno pred sve organizacije postaviti ista pravila. Glavna ideja ove norme jest pred organizacijama istaknuti važnost procjene rizika i djelovanja u području zaštite na temelju rezultata procjene rizika.

Norme pomaže organizacijama da provodu ovaj proces baziran na njihovim internim procesima i načinu poslovanja, umjesto da nameće jedan okvir za sve one koji trebaju zaštititi svoj informacijski sustav. Preporučeni koraci za implementaciju norme jesu pristupiti kompletnoj procjeni rizika, odnosno što se sve loše može dogoditi organizaciji i informacijama koje organizacija posjeduje, a potom donijeti odluke koje će voditi prema implementaciji procesa koje će spriječiti ili umanjiti rizik od realizacija potencijalnih opasnosti. Norma propisuje razvijanje i implementacija sigurnosnih koraka koji su doista potrebni, a ne onih koraka za koji svi smatraju da organizacija treba posjedovati.

Procjena rizika ili analiza rizika je najkompliciraniji dio implementacija ove norme jer na rezultatima analize se zadaju konkretni koraci za zaštitu informacijskog sustava, odnosno daje se „lijek za rizik“. Područje menadžmenta rizika danas je u porastu te se radi o veoma kompliciranoj disciplini, no postoji šest osnovnih koraka s kojima se uspješno može provesti analiza rizika koje je sažeo Dejan Košutić, CEO Advisere i 27001Academy te certificiran ekspert za ISO 27001/22301 norme:

1. *Uspostavljanje metodologije za procjenu rizika* – kao što je već spomenuto, potrebno je definirati pravila kako će se provesti analiza rizika kako bi se definirali

glavni problemi u informacijskom sustavu. Organizacija treba odabrati želi li napraviti kvalitativnu ili kvantitativnu procjenu rizika, koja mjerila će se uzeti za odabrani pristup, koje su prihvatljive razine rizika i slično.

2. *Implementacija procjene rizika* – nakon uspostavljanja osnovnih pravila procjene rizika, potrebno je iscrtati shemu svih resursa u vlasništvu, koje prijetnje i ranjivosti se odnose na te resurse, procijeniti utjecaj prijetnji na pojedinačne resurse i izračunati razinu rizika. Ovaj proces treba biti opsežan i doista treba prodrijeti u sve dijelove organizacije jer što boljom analizom rizika se isti rizik može i prevenirati ili smanjiti.

3. *Implementacija liječenja rizika* – prethodni korak trebao je pomoći u identifikaciji svih rizika, no u ovom koraku fokus je na najvažnijim rizicima koji se svrstavaju u neprihvatljive. Postoje četiri načina izbjegavanja neprihvatljivog rizika – aplikacija sigurnosnih kontrola iz ISO 27001 standarda, povjeravanje rizika primjerice osiguravajućoj tvrtki, prestanak izvršavanja akcija koje bi rezultirale rizikom ili pak prihvaćanje rizika kao takvog.

4. *Dokumentacija procjene rizika* – stavljanje na papir svega što je učinjeno u prethodnim koracima; ova dokumentacija pomoći će u analizi stanja u narednim periodima poslovanja organizacije.

5. *Izjava o primjenjivosti* – izjava je temeljni dokument koji će certificirani revizor temeljno proučiti kako bi na jednom mjestu vidio koje rizike je organizacija prepoznala, koje kontrolne točke je postavila za sprječavanje rizika, zašto su odabrali baš te metode te kako ih se planira provesti u stvarnosti ukoliko dođe do incidenta, odnosno realizacije rizika.

6. *Plan liječenja rizika* – ova vrsta dokumentacije služi kako bi se pokazali praktični koraci koji će se dogoditi prilikom implementacije kontrolnih točaka i definiraju vremenski period, budžet i slično. Plan liječenja rizika zapravo je akcijski plan implementacije preventivnih mjera te je apsolutna kruna cijelog procesa za dobivanje norme ISO/IEC 27001. Ovaj dokument mora biti sistematičan, realističan i konkretan.

Navedenih šest koraka zapravo prati 10 poglavlja koji su sadržaj norme ISO/IEC 27001, a koji sistematično prate kontekst organizacije, rukovođenje, planiranje,

podršku, djelovanje, ocjenu učinka i poboljšanje za organizaciju. Bitno za napomenuti kod ISO 27001 normi jest to da se ona ne odnosi samo na IT sektor poslovanja organizacije – IT ovdje čini samo 50% udjela. Ovaj standard nalaže sveukupnu procjenu rizika na sve odjele koji čine jedno poduzeće, uključujući plan poslovanja.

Uvođenje ove norme za hrvatske organizacije, poduzeća i organe vlasti podrazumijeva se i usklađenost navedenih oblika poslovanja sa Zakonom o informacijskoj sigurnosti, Zakonom o provedbi opće uredbe o zaštiti podataka te Uredbom o načinu pohranjivanja i mjerama tehničke zaštite posebnih kategorija osobnih podataka. Za hrvatske organizacije to znači i da su pravovremeno ocijenili moguće rizike, imaju plan akcija, imaju kontrolu nad provjerom i praćenjem dobavljača te su poduzeli potrebne korake za zaštitu tehničkog i fizičkog aspekta poslovanja, kao i resursa, opreme i instalacija. Ovom normom i koracima prema realizaciji zaštite od rizika ostvaruje se i pravilna uporaba informatičke i komunikacijske opreme, tehnološka zaštita od raznih malwareova, zaštita i povrat podataka u slučaju incidenata, osigurava se stalno funkcioniranje važnih poslovnih i procesnih aplikacija i programa te se osigurava podložnost poslovanja hrvatskim regulatornim agencijama i zakonima.

5.3 ODNOS NORMI: ISO/IEC 27001:2013 – ISO/IEC 27002:2013

Hrvatski zavod za norme usvojio je ISO/IEC 27001:2013 normu pa ju tako u hrvatskim normativnim dokumentima organizacije mogu pronaći pod kraticom HRN EN ISO/IEC 27001:2017 (uključene ispravke i revizije iz 2014., 2015. i 2017. godine nalaze se pod istom normom). Puni naziv u hrvatskom normativnom dokumentu za ovu normu jest: „Informacijska tehnologija -- Sigurnosne tehnike -- Sustavi upravljanja informacijskom sigurnošću – Zahtjevi“. Na početku ovog poglavlja spomenuta je razlika između ISO/IEC 27001 i ISO/IEC 27002 normi, no u narednim redovima predstavit će se glavni zaključci svake od ove norme kako bi se jasnije istaknule važnosti svake od navedenih normi te kako bi se uvidjelo da je implementacija obje norme najbolji pristup za bilo koje poduzeće.

ISO/IEC 27001:2013 drugo je izdanje ove norme koja ima službeno ime „Informacijske tehnologije – Sigurnosne tehnike – Sustavi upravljanja informatičkom sigurnošću – Zahtjevi“; prvo izdanje doneseno je 2005. godine. Ovaj standard donosi

zahtjeve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sustava upravljanja informacijskom sigurnošću. Sustav upravljanja informacijskom sigurnošću prepoznat je kao strateška odluka organizacije te organizaciji donosi očuvanje povjerljivosti, integriteta i dostupnosti informacija aplikacijom procesa procjene rizika. Cjelokupna norma, ističe se u dokumentaciji norme, mora se prilagoditi potrebama i veličini organizacije.

ISO/IEC 27002:2013 norma također je revizija originalne norme iz 2005. godine, a službeno ime joj je „Informacijska tehnologija – Sigurnosne tehnike – Kodeks prakse za kontrolu informacijske sigurnosti“. Norma je namijenjena organizacijama kako bi odabrali kontrole u procesu implementacije sustava upravljanja informacijskom sigurnošću koji su bazirani na prvoj normi, ISO/IEC 27001:2013. Dakle, vidljivo je iz usporedbe kako se 27002 norma nadovezuje na teoretske postavke i zahtjeve koje propisuje 27001 norma, te kako su ove dvije norme neodvojive. Kontrole koje se ovdje spominju odnose se na procese, procedure, organizacijsku strukturu, te softverske i hardverske funkcije koje organizacije posjeduju. U 27002 normi ističe se kako uspješan ISMS zahtjeva potporu svih zaposlenika organizacije, ali potencijalno i svih dobavljača i ostalih eksternih sudionika u poslovanju organizacije.

27001 norma fokusirana je, kao što joj i ime sugerira, zahtjeve koje bi organizacija trebala ispuniti, odnosno na što sve organizacija treba biti spremna kako bi implementirala najviše sigurnosne standarde za zaštitu informacijskog sustava – procjena rizika i postupci u informacijskoj sigurnosti ovdje igraju glavnu ulogu, kao što je već napomenuto i istaknuto u prethodnim potpoglavljima. 27002 norma nadopunjuje 27001 normu tako što daje pravce organiziranja ISMS-a, što uključuje selekciju, implementaciju i menadžment kontrola koje pomažu organizaciji u području sprječavanja rizika. Ukratko, 27001 je teorijska podloga za organizacije, dok 27002 norma daje praktičniji pristup dolaska do adekvatnog sigurnosnog rješenja za zaštitu informacija. 27001 norma je menadžmentski standard koji daje smjernice kako sustav treba raditi i definira ISMS. Sustav mora biti temeljito isplaniran, implementiran i redovito unapređivan. 27002 norma na detaljniji način objašnjava dijelove 27001 norme, no bez prvotne norme njegov značaj je malen.

Organizacije ne mogu pristupiti certificiranju za ISO/IEC 27002 normu ukoliko nisu

postavili temelje za ISO/IEC 27001 normu i upravo iz tog razloga organizacijama se preporuča implementacija obje norme te sustavno ulaganje u ISMS. Ako organizacija uspije ispuniti sve korake i implementirati sigurnosne korake za svoj informacijski sustav, po standardima ovih normi organizacija ima izvrsnost u zaštiti informacija. Organizacije koje žele pristupiti ovom procesu moraju imati strpljenja, biti iskreni prema svojoj organizaciji, osigurati suradnju svih zaposlenika te osigurati kulturu koja će ove standarde shvatiti ozbiljno.

6. ZAKLJUČAK

Nakon pregleda terminologije i ustroja sigurnosno-obavještajnih organizacija u Republici Hrvatskoj, kao i stvarnih slučajeva hakiranja informacija, moglo bi se zaključiti kako nitko nije siguran. U procjeni rizika to bi svakako bio valjan zaključak i važna pouka svima onima koji ne samo da nastoje zaštititi svoje podatke na Internetu i općenito, već i za one koji se aktivno bave temom sigurnosti informacija i informacijskih sustava. To nikako nije panična izjava, već je prva stepenica u prihvaćanju činjenice kako za zaštitu informacija u današnje vrijeme morate ulagati doista velike napore i uvijek biti oprezan.

Rad je nastojao dati pregled funkcioniranja sustava informacijske sigurnosti općenito i u Republici Hrvatskoj. Iako Republika Hrvatska ima razvijene mehanizme zaštite, na primjeru Ministarstva vanjskih poslova može se vidjeti kako ni najnovija tehnologija ponekad ne može u potpunosti garantirati sigurnost. Međunarodne norme nastoje to promijeniti sugerirajući organizacijama da itekako budu svjesni rizika, te da na te rizike moraju znati reagirati propisnim aktivnostima. Ako organizacije ne krenu ozbiljnije shvaćati temu zaštite informacija, u budućnosti možemo očekivati još više hakerskih incidenata. Društvene mreže su u proteklim godinama pokazale veliku ranjivost, a nastojanja institucija i organizacija poput Europske unije da donesu legislative o tome nisu utjecale pretjerano na inovaciju u području sigurnosti informacija.

Republika Hrvatska također bi morala revidirati i ponovno ispisati određene zakone i pravilnike koji se tiču sigurnosti informacija, i to na puno praktičniji i primjenjiviji način nego do sada. Jer upravo država mora biti primjerenije zaštite i aplikacije određenih noviteta.

IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Elena Kraljević

Matični broj studenta: 1-171/18

Naslov rada: Izvori i oblici prijetnji sustavu sigurnosti informacija Republike Hrvatske

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum Potpis studenta

_____ _____

7. POPIS LITERATURE

7.1 KNJIGE I ČLANCI

1. Cingula, M., Žugaj, M., Šehanović, J. (2004) Organizacija.Varaždin: FOI.
2. Gerić, S., Hutinski, Ž. (2007) Information System Security Threats Classifications. Journal of Information and Organizational Sciences, Vol. 31 No. 1.
3. Juran, A. (2014) Sigurnost informacijskih sustava. Diplomski rad. Rijeka: Pomorski fakultet u Rijeci.
4. Kezerić, AM. (2016) Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: radnjivost informacijske infrastrukture. Diplomski rad. Zagreb: Fakultet političkih znanosti u Zagrebu.
5. Klaić, A. (2010) Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodama upravljanja informacijskom sigurnošću. Kvalifikacijski doktorski ispit. Zagreb: Fakultet elektrotehnike i računarstva.
6. Klaić, A., Perešin, A. (2011) Koncept regulativnog okvira informacijske sigurnosti. U: Toth, Ivan (ur) Dani kriznog upravljanja (str. 678-708). Velika Gorica: Veleučilište Velika Gorica.
7. Nađ, I., Adelsberger, Z. (2016) Informacijska sigurnost u kontekstu kriznog upravljanja . U: Nađ, Ivan (ur) Dani kriznog upravljanja (116-126). Velika Gorica: Veleučilište Velika Gorica.
8. Orehovec, Z. (2016) 25 godina od osamostaljenja, i dalje bez Strategije nacionalnog razvoja. Defender 2(5): 28-31.
9. Pavlić, M. (2011). Informacijski sustavi. Zagreb: Školska knjiga.
10. Peraković D., Cvitić, I. (2015) Sigurnost i zaštita informacijsko komunikacijskog sustava – skripta, Sigurnost i zaštita informacijsko komunikacijskog sustava. Zagreb: Fakultet prometnih znanosti.
11. Perešin, A., Klaić, A. (2012) Uloga kibernetičke sigurnosti u zaštiti kritične infrastrukture. U: Toth, Ivan (ur) Dani kriznog upravljanja (str. 335-357). Velika Gorica: Veleučilište Velika Gorica.
12. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M. (2007.) Sigurnost računarskih sistema i mreža, Mikro knjiga: Beograd.
13. Samonas, S.; Coss, D. (2014). "The CIA Strikes Back: Redefining Confidentiality,

Integrity and Availability in Security". Journal of Information System Security. 10 (3): 21–45.

14. Singer, P., W., Friedman, A. (2014) Cybersecurity and Cyberwar: what everyone needs to know. New York: Oxford University Press.

7.2 INTERNETSKI IZVORI

1. Bourgeois, D. (2014). Chapter 1: What Is an Information System? – Information Systems for Business and Beyond. URL: https://bus206.pressbooks.com/chapter/chapter-1/. Pristupljeno 28.06.2021.
2. Bug.hr (03.04.2021.) *Osobni podaci 660 tisuća hrvatskih korisnika Facebooka procurili u javnost*. URL: https://www.bug.hr/sigurnost/osobni-podaci-660-tisuca-hrvatskih-korisnika-facebooka-procurili-u-javnost-20366 Posjećeno: 1.7.2021.
3. CERT.hr (n.d.) *Procurilo 533 milijuna telefonskih brojeva i osobnih podataka korisnika Facebooka.* URL:https://www.cert.hr/procurilo-533-milijuna-telefonskih-brojeva-i-osobnih-podataka-korisnika-facebooka/ Posjećeno: 1.7.2021.
4. CERT.hr (2021) *Godišnji izvještaj za 2020. godinu*. URL: https://www.cert.hr/wp-content/uploads/2021/02/Carnet_Cert_godisnji_izvjestaj_2020_0402-3.pdf Posjećeno: 27.6.2021.
5. CERT.hr (n.d.) O nama. URL: https://www.cert.hr/onama/. Posjećeno: 28.6.2021.
6. Cisco Systems (n.d.) What is Information Security. URL: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html (Pristupljeno 29.06.2021.)
7. CSO Online (n.d.) The CIA Triad: Definition, Components and Examples. URL: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html. Posjećeno 29.06.2021.
8. Dnevnik.hr (02.12.2016.) Hakirano hrvatsko Ministarstvo vanjskih poslova. URL: https://dnevnik.hr/vijesti/hrvatska/na-mvep-izvrsen-hakerski-napad-niti-jedna-vazna-informacija-nije-kompromitirana-ministar-stier---459254.html?fb_comment_id=1162642803783715_1162996163748379. Posjećeno 27.06.2021.
9. Hintzbergen, J. et al. (2010). Foundations of Information Security Based on Iso27001 and Iso27002. Best Practice: Van Haren Publishing.

10. Index.hr (16.02.2021.) Anonymousi hakirani Ministarstvo vanjskih poslova. URL: https://www.index.hr/vijesti/clanak/Anonymousi-hakirali-Ministarstvo-vanjskih-poslova-Ali-mi-nismo-nadlezni-za-ACTA-u/599445.aspx Posjećeno 27.06.2021.

11. Informacijski sustav. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=27410. Pristupljeno 30. 6. 2021.

12. IT Governance (n.d.) ISO 27000 Series of Standards. URL: https://www.itgovernance.co.uk/iso27000-family. Posjećeno: 1.7.2021.

13. ISO Open Text Content Service (n.d.) ISO Survey of certifications to management system standards – Full results. URL: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. Posjećeno: 1.7.2021.

14. ISO.org (n.d.) ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. Posjećeno: 1.7.2021.

15. ISO.org (n.d.) ISO/IEC 27002:2013(en) Information technology — Security techniques — Code of practice for information security controls. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. Posjećeno: 01.07.2021.

16. Jutarnji.hr (16.02.2012.) Anonymous hakirao stranice Ministarstva vanjskih poslova. URL: https://www.jutarnji.hr/vijesti/hrvatska/anonymous-hakirao-stranice-ministarstva-vanjskih-poslova-ne-zelimo-nikome-naskoditi-samo-upozoravamo-na-acta-u-1639545. Posjećeno 27.06.2021.

17. Jutarnji.hr (03.12.2016.) OVAKAV HAKERSKI NAPAD U HRVATSKOJ NIKADA NIJE ZABILJEŽEN Otkrivamo tko je zaslužan sa spašavanje podataka iz sustava MVEP-a. URL: https://www.jutarnji.hr/vijesti/hrvatska/ovakav-hakerski-napad-u-hrvatskoj-nikada-nije-zabiljezen-otkrivamo-tko-je-zasluzan-sa-spasavanje-podataka-iz-sustava-mvep-a-5339295 Posjećeno 27.06.2021.

18. Košutić, D. (n.d.) ISO 27001: Risk Assessment Treatment – 6 Basic Steps. URL: https://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/- Posjećeno: 01.07.2021.

19. New York Times (10.01.2021) *He Created the Web. Now He's Out to Remake the Digital World.* URL: https://www.nytimes.com/2021/01/10/technology/tim

-berners-lee-privacy-internet.html. Pristupljeno: 30.06.2021.

20. Repozitorij Hrvatskog zavoda za norme (n.d.). HRN EN ISO/IEC 27001:2017. URL: https://repozitorij.hzn.hr/norm/HRN+EN+ISO%2FIEC+27001%3A2017. Posjećeno: 1.7.2021.

21. Telegram.hr (n.d.) Godišnje izvješće SOA-e: Rusi i Kinezi pokušavali su hakirati hrvatske institucije. URL: https://www.telegram.hr/politika-kriminal/godisnje-izvjesce-soa-e-rusi-i-kinezi-pokusavali-su-hakirati-hrvatske-institucije/ Posjećeno 28.06.2021.

22. Telegram.hr (n.d.) *SOA posebno upozorava na hibridne trolove.* URL: https://www.telegram.hr/politika-kriminal/soa-posebno-upozorava-na-hibridne-trolove-koji-vrebaju-gradane-i-politicare-kazu-ima-ih-posvuda/ Posjećeno: 1.7.2021.

23. Tportal (04.03.2012.) Opet hakirana stranica Pusićkinog ministarstva. URL: https://www.tportal.hr/vijesti/clanak/opet-hakirana-stranica-pusickinog-ministarstva-20120403. Posjećeno 27.06.2021.

24. UVNS.hr (2015) *Nacionalna strategija kibernetičke sigurnosti*. URL: https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kiberneticke%20sigurnosti%20(2015.).pdf. Posjećeno: 25.6.2021.

25. UVNS.hr (n.d.) Vijeće za nacionalnu sigurnost. URL: https://www.uvns.hr/hr/o-nama/vijece-za-nacionalnu-sigurnost. Posjećeno: 27.6.2021.

26. UVNS.hr (n.d.) O Vojnoj sigurnosno-obavještajnoj agenciji. URL: https://www.morh.hr/o-vojnoj-sigurnosno-obavjestajnoj-agenciji/. Posjećeno: 27.6.2021.

27. UVNS.hr (n.d.) Savjet za Koordinaciju sigurnosno-obavještajnih agencija. URL: https://www.uvns.hr/hr/o-nama/savjet-za-koordinaciju-sigurnosno-obavjestajnih-agencija. Posjećeno: 27.6.2021.

28. Zakon.hr (n.d.) Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske. URL: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske Posjećeno: 01.07.2021.

29. Zakon.hr (n.d.) Zakon o informacijskoj sigurnosti. URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti. Posjećeno: 01.07.2021.

30. Zakon.hr (n.d.) Zakon o tajnosti podataka. URL: https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka. Posjećeno: 01.07.2021.

8. POPIS SLIKA, TABLICA I GRAFIKONA

ŽIVOTOPIS

europass

Elena Kraljević

Datum rođenja: 12/03/1995 | **Državljanstvo:** hrvatsko | **Spol** Žensko | (+385) 994718231 | elena.kraljevic.ek@gmail.com |

Vinogradarski put 40, 10370, Dugo Selo, Hrvatska

RADNO ISKUSTVO

01/01/2013 – 15/11/2014 – Zagreb, Hrvatska
PROMOTOR

-demonstracija i informiranje o promoviranim proizvodima/uslugama
-distribucija uzoraka, brošura
-kreiranje pozitivne slike i vođenje računa o korisnicima usluga
-promocija na štandovima, slaganje zaliha proizvoda

2013 – 2015 – Zagreb, Hrvatska
RAD SA DJECOM – VOLONTIRANJE

-pomaganje u učenju
-čuvanje
-vještine u igrama i edukacija
-dobar smisao za humor
-strpljenje i razumijevanje djece

2013 – 2014 – Dugo Selo, Hrvatska
STUDENTSKI POSLOVI – KAUFLAND, SILVER

-noćne smjene
-punjenje polica sa proizvodima
-inventure

-prodaja nakita
-obračuni i zatvaranje

01/04/2015 – 31/07/2015 – Zagreb, Hrvatska
UGOSTITELJ

-pripremanje pića, miješanje koktela, čišćenje prostora
-obračun na kraju radnog dana
-otvaranje/zatvaranje ugostiteljskog objekta

15/09/2015 – 06/07/2017 – Zagreb, Hrvatska
LOGISTIKA – MINISTARSTVO OBRANE REPUBLIKE HRVATSKE

-obračuni plaće
-planiranje, nabava, skladištenje, raspodjela, čuvanje i distribucija materijalnih sredstava
-zaprimanje pošte, urudžbiranje

06/07/2017 – TRENUTAČNO – Zagreb, Hrvatska
VOJNA POLICIJA – MINISTARSTVO OBRANE REPUBLIKE HRVATSKE

-zaštita života, slobode, prava, sigurnosti i nepovredivosti vojnih osoba, državnih službenika i namještenika na službi
-zaštita imovine kojom upravlja Ministarstvo obrane i Oružane snage
-sprječavanje i otkrivanje kaznenih djela i prekršaja
-potpora vojnostegovnim tužiteljstvima i vojnostegovnim sudovima
-upravljanje prometom vojnih vozila na cestama te nadzor vojnih vozila, vozača i drugih vojnih sudionika u prometu
-osiguranje osoba, objekata i prostora od posebnog sigurnosnog interesa za Ministarstvo obrane i Oružane snage
-sudjelovanje, po potrebi, u sigurnosnoj potpori MUP-u, stranim vojnim organizacijama i tijelima, te drugim tijelima državne vlasti,

europass

-sudjelovanje u otklanjanju posljedica izazvanih prirodnim nepogodama, tehničko-tehnološkim i ekološkim nesrećama te prometnim nezgodama većih razmjera
-ostali poslovi određeni zakonom i drugim propisima.

JEZIČNE VJEŠTINE

Materinski jezik/jezici: HRVATSKI

Drugi jezici:

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna produkcija	Govorna interakcija	
ENGLESKI	B2	B2	B2	B2	B1

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

DIGITALNE VJEŠTINE

Internet | MS Office (Word Excel PowerPoint) | Rad na računalu | Informacije i komunikacija | Rad na društvenim mrežama | Brzo učenje | Brzo tipkanje

ORGANIZACIJSKE VJEŠTINE

Poslovne vještine

-vođenje
-produktivnost
-multitasking
-razumijevanje
-pomoć

Komunikacijske vještine

-razvijene komunikacijske vještine
-vještine funkcioniranja unutar tima
-aktivno slušanje, prezentiranje

OBRAZOVANJE I OSPOSOBLJAVANJE

2009 – 2013
GEOLOŠKI TEHNIČAR – Prirodoslovna škola Vladimira Preloga

2013 – 2014
INDUSTRIJSKA EKOLOGIJA – Metalurški fakultet

2018 – TRENUTAČNO
POSLOVANJE I UPRAVLJANJE - MENADŽMENT UREDSKOG POSLOVANJA – Veleučilište s pravom javnosti Baltazar Zaprešić