Sigurnosna zaštita gospodarskog subjekta

Leško, Elena

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department of Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:632068

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

SIGURNOSNA ZAŠTITA GOSPODARSKOG SUBJEKTA

ELENA LEŠKO

Split, rujan 2024.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

SIGURNOSNA ZAŠTITA GOSPODARSKOG SUBJEKTA

MENTOR: doc. dr. sc. Tonći Prodan

ELENA LEŠKO

0200030590

Split, rujan 2024.

Rad je izrađen u Sveučilišnom odjelu za forenzične znanosti Sveučilišta u Splitu pod nadzorom mentora doc. dr. sc. Tonćija Prodana u vremenskom razdoblju od svibnja do kolovoza 2024. godine.

Datum predaje diplomskog rada: 01. rujna 2024.

Datum prihvaćanja rada: 17. rujna 2024.

Datum usmenog polaganja: 23. rujna 2024.

Povjerenstvo: 1. prof. dr. sc. Josip Kasum

2. doc. dr. sc. Marko Perkušić

3. doc. dr. sc. Tonći Prodan

Sadržaj

1. Uvod

Sigurnost predstavlja bitnu komponentu ljudskog života. Ljudi su se kroz povijest kontinuirano trudili štititi i ispuniti svoju potrebu za sigurnošću. Ovaj proces razvoja sigurnosti prilagođavao se novim izazovima, od zaštite od divljih životinja i prijetnji od drugih ljudi, kroz ratovanje mačevima, kopljima i strijelama, pa sve do suvremenih prijetnji poput vatrenog i nuklearnog oružja. U današnje vrijeme, sofisticiranije vrste napada poput kibernetičkih napada postali su svakodnevna prijetnja, stoga je razvoj sigurnosnih standarda kod pojedinca neizbježan.

Svaki pojedinac je svjestan većine prijetnji koje ga okružuju, kako u osobnom, tako i u profesionalnom okruženju. Osim izravnih prijetnji, bitna je svijest pojedinca i o prijetnjama koje mu prijete indirektno u poslovnom okruženju, i to kako bi mogao što bolje reagirati na iste i osigurati nesmetano poslovanje subjekta. Sigurnost gospodarskog subjekta predstavlja važnu sastavnicu u sustavu nacionalne sigurnosti jer o sigurnosti jednog određenog gospodarskog subjekta ovisi sigurnost nekoliko desetaka, stotina ili tisuća zaposlenika, a isto tako i njihovih obitelji. Tako se danas značajan trud, znanje i novac ulažu u obrazovanje ljudi i u sustave koji će štititi gospodarske subjekte.

Zaštitu gospodarskog subjekta potrebno je provesti kroz nekoliko različitih koraka kako bi bila sveobuhvatna; bitno je utvrditi opasnosti, procijeniti i odrediti koji su rizici te provesti analizu i evaluaciju istih. Na temelju procjene rizika izrađuje se plan upravljanja rizicima gospodarskog subjekta, koji uključuje konkretne aktivnosti i preventivne mjere te, između ostalog, osigurava provedbu istih. Plan upravljanja rizicima sadržava i konkretan plan sigurnosne zaštite, koji obrađuje elemente kao što su mehanička, fizička, tehnička i kibernetička sigurnost, odnosno sigurnost samih poslovnih procesa u širem smislu. Konkretni akcijski plan povećanja razine sigurnosne zaštite usmjeren je na konkretne probleme detektirane procjenom rizika, a za cilj ima učiniti gospodarski subjekt težom „metom“.

2. Cilj rada

Cilj rada je na sustavan način prikazati kako izraditi kvalitetnu procjenu rizika i plan upravljanja rizicima te kako sastaviti sveobuhvatni i konkretni plan sigurnosne zaštite gospodarskog subjekta. Očekivani istraživački rezultat s forenzičkog polazišta pružit će doprinos razumijevanju i poboljšanju sigurnosti gospodarskih subjekata.

Ovim radom žele se istražiti sljedeće hipoteze:

H0 – Sigurnosna zaštita gospodarskih subjekata od višestruke je važnosti za gospodarski sustav.

H1 – Velik broj gospodarskih subjekata nema adekvatne planove sigurnosne zaštite ili ih uopće nema.

H2 – Razvoj novih tehnologija dovodi do sve složenijih sigurnosnih prijetnji, poput kibernetičkih napada, i bitno nanosi štetu gospodarskom subjektu.

3. Izvori podataka i metode

Kako bi se što obuhvatnije prikazala izrada sigurnosnog plana gospodarskog subjekta, u ovom su radu korišteni različiti izvori podataka, poput stručnih knjiga, znanstvenih radova, zakonskih i podzakonskih propisa, *online* izvora.

Pri pregledu relevantne literature korištene su standardne znanstveno-istraživačke metode: analiza, sinteza, induktivna i deduktivna metoda, metoda deskripcije i kompilacije, komparativna metoda.

4. Rasprava i rezultati

4.1. Općenito o sigurnosti

Sigurnost je stvar percepcije svakog pojedinca, a pronalazi se u svim segmentima života, kako u poslovnom, tako i u privatnom, pa je većina građana upoznata ili je makar čula za pojmove osobne, nacionalne, međunarodne sigurnosti i sl. Nobilo (1) u svom radu navodi da je sigurnost jedan od najčešće upotrebljavanih, a u isto vrijeme neobjašnjenih, pojmova. U znanstvenim se krugovima može pronaći velik broj različitih definicija samog pojma sigurnosti, a u daljnjem će se tekstu navesti i analizirati nekoliko definicija sigurnosti. Sigurnost „U svojem izvornom stoičkom shvaćanju, »nepotresenost« *(ἀταραξία)* izvanjskim događajima, »bezbrižnost« *(se-cura)* u smislu potpunoga duševnoga mira.“ (2)

Nobilo (1) objašnjava sigurnost kao potrebu, sustav sigurnosti, funkciju i stanje. Prema Mihaljević i Nađ (3), sigurnost je „stanje i stupanj otpornosti i zaštićenosti od ugroženosti i opasnosti“, a također je definirana kao „stanje u kojem je osiguran uravnotežen fizički, duhovni i društveni te materijalni opstanak pojedinca i društva u odnosu prema drugim pojedincima, društvima i prirodi“. Sigurnost je stanje bez opasnosti i ugrožavanja, koje uključuje ne samo osjećaj sigurnosti, već i aktivnosti i sustave usmjerene na njezino postizanje (4).

Tatalović i Bilandžić (5) dijele sigurnosti na: individualnu, nacionalnu, regionalnu, međunarodnu i globalnu sigurnost, koje možemo pratiti na razini pojedinca (osobna sigurnost), društva, poslovnih subjekata, država, regija, čak i na svjetskoj razini.

Rizik predstavlja „opasnost koja se do stanovite mjere može predvidjeti i kojoj se može odrediti intenzitet“, a Međunarodna organizacija za normizaciju (engl. *International Organization for Standardization*) donosi standard ISO 31000:2018 prema kojem je rizik učinak neizvjesnosti na ciljeve (pozitivan ili negativan ili oboje) (6, 7).

Pojam sigurnosti uključuje tri ključna elementa:

1. objekt sigurnosti (ono što se štiti: čovjek, poslovni subjekt, teritorij, imovina, materijalna sredstva, informacija, društvo i sl.)
2. subjekt sigurnosti (onaj tko je odgovoran za zaštitu objekta)
3. subjekt opasnosti (izvor opasnosti za objekt) (3).

Sigurnost se odnosi na stanje u kojem se objekt sigurnosti, bilo da je riječ o pojedincu, društvu ili bilo kojem drugom objektu, osjeća slobodnim od prijetnji koje imaju potencijal ugrožavanja. Sigurnost se postiže kroz zaštitu objekta, a najčešće je riječ o privatnoj zaštiti, koja se može odnositi na zaštitu osoba, imovine, poslovnog subjekta i sl. U takvom stanju pojedinci i društvo postižu bolji život za sebe jer mogu nesmetano djelovati i napredovati.

Potrebno je naglasiti kako je potpuni osjećaj sigurnosti vrlo teško postići jer će pojedinci uvijek nailaziti na nove prijetnje, a minimizacija i edukacija o izbjegavanju prijetnji predstavljaju veliki pomak, iznimno bitan kako bi se osigurao kvalitetniji život u zajednici. Također, kad se govori o povećanju vlastite sigurnosti, potrebno je obratiti pažnju na osjećaj sigurnosti ostalih pojedinaca u okruženju ili, ako je u pitanju povećanje sigurnosti na državnoj razini, o percepciji sigurnosti susjednih država; povećanjem vlastite sigurnosti, ostali pojedinci ili države u okruženju to mogu percipirati kao prijetnju. Potrebno je sagledati sve elemente koji utječu na sigurnost objekta koji je potrebno zaštititi i na temelju toga donijeti odluke primjerene stupnju zaštite koja se želi postići.

4.2. Pojmovi

Kako bi se bolje razumio rad, potrebno je objasniti pojmove koji će se koristiti i spominjati u radu, poput sigurnosne zaštite, gospodarskog subjekta, korporativne sigurnosti, osobne, tehničke, mehaničke i tjelesne zaštite.

Prema Zakonu o sigurnosnoj zaštiti pomorskih brodova i luka (NN 108/17, 30/21) (8), „sigurnosna zaštita je sustav preventivnih mjera namijenjenih zaštiti brodova i luka od prijetnje namjernim nezakonitim činom“. Općenito bi se moglo reći da sigurnosna zaštita predstavlja pojam koji se odnosi na skup mjera, postupaka i sredstava koji osiguravaju sigurnost osoba, imovine i informacija od različitih prijetnji. Ključna je za sprječavanje štetnih događaja i osiguranje stabilnog i sigurnog okruženja za rad, razvoj i život pojedinaca, društva, organizacija, država. Može biti:

- osobna
- informacijska
- tehnička
- tjelesna
- mehanička.

Osim pojedinca, društva i država, osiguravaju se i gospodarski subjekti, koje je kao temu ovog rada potrebno posebno definirati.

Prema Zakonu o javnoj nabavi (NN 120/16, 114/22) (9) čl. 3., st. 8. „gospodarski subjekt je fizička ili pravna osoba, uključujući podružnicu, ili javno tijelo ili zajednica tih osoba ili tijela, uključujući svako njihovo privremeno udruženje, koja na tržištu nudi izvođenje radova ili posla, isporuku robe ili pružanje usluga“.

Fizičku osobu predstavlja čovjek koji je nositelj prava i dužnosti (pravni subjekt). Suvremeno pravo govori kako čovjek postaje fizička osoba svojim rođenjem, a prestaje smrću ili proglašenjem nestale osobe umrlom (10).

Pravna osoba je „udruženje fizičkih osoba ili imovina namijenjena određenoj svrsi kojoj zakon priznaje pravnu samostalnost“ (11). Pravne osobe mogu biti:

- pravne osobe koje obavljaju gospodarsku djelatnost – npr. trgovačka društva
- pravne osobe koje djeluju izvan gospodarstva – npr. ustanove
- pravne osobe koje imaju javnopravne ovlasti – npr. jedinice lokalne i regionalne/područne samouprave

- udruge (12).

Najbrojniji pravni subjekti su trgovačka društva koja mogu biti društva osoba i društva kapitala. Društva osoba ističu individualnost članova, a ne kapital. Nastaju udruživanjem najmanje dvije osobe koje uključuju svoju imovinu, prava i rad, uz očekivanja osobnog doprinosa radu društva. Barem jedan član je odgovoran cijelom svojom imovinom. Društva osoba mogu biti:

- javno trgovačko društvo (j.t.d.) – društvo dvije ili više fizičkih ili pravnih osoba koje se udružuju radi trajnog obavljanja djelatnosti pod zajedničkom tvrtkom, a svaki član neograničeno solidarno odgovara za obveze društva te ima pravo i obvezu voditi poslove društva i zastupati ga
- komanditno društvo (k.d.) – društvo u kojem se najmanje jedna osoba, koja ima neograničenu osobnu odgovornost, udružuje s najmanje jednom osobom koja odgovara samo do visine svog uloženog kapitala
- gospodarsko interesno udruženje (GIU) – osnivaju dvije ili više fizičkih i pravnih osoba s namjerom olakšavanja i unaprjeđenja gospodarskih djelatnosti svojih članova (12).

Društva kapitala su trgovačka društva čiji je fokus na kapitalu, a ne individualnosti članova, koji sudjeluju u odlučivanju na temelju svojih kapitalnih udjela. Članovi nemaju osobnu odgovornost za obveze društva. Društva kapitala mogu biti:

- dioničko društvo (d.d.) – trgovačko društvo čiji su članovi dioničari koji sudjeluju u minimalnom temeljnom kapitalu od 200.000,00 kuna (25.000,00 eura) koji je podijeljen u dionice, a temeljni akt je statut, dok je sustav upravljanja dualistički ili monistički
- društvo s ograničenom odgovornošću (d.o.o.) – trgovačko društvo u kojem članovi unose uloge u minimalni temeljni kapital 20.000,00 kuna (2.500,00 eura), obvezni organi su uprava i skupština, a društveni ugovor određuje postojanje nadzornog odbora
- jednostavno društvo s ograničenom odgovornošću (j.d.o.o.) – trgovačko društvo s najviše pet članova, a najniži temeljni kapital iznosi 10,00 kuna (1 euro) i uplaćuje se samo u novcu, a u slučaju da se poveća temeljni kapital na 20.000,00 kuna, odnosno 2.500,00 eura, počinju se primjenjivati odredbe kao za d.o.o. (12).

Zbog obujma posla i odgovornosti subjekata u financijskom sektoru države, bitna je sama zaštita istih kroz korporativnu sigurnost, odnosno sigurnost poslovnih subjekata na različitim razinama. Korporacija je „u srednjem vijeku, udruga stvorena radi zaštite, očuvanja ili postizanja ekonomskih probitaka u nekom proizvodnom području; u suvremenom pravu i ekonomskim sustavima, udruga ili organizacija koja kao pravna osoba zastupa interese svojih

pripadnika, štiti njihova prava, ostvaruje svojom djelatnošću određene zajedničke gospodarske, socijalne, vjerske ili koje druge ciljeve; u novije doba, jedan od oblika organizacije državne gospodarske djelatnosti i upravljanja javnom imovinom“ (13).

Povijesno gledano, razvoj korporativne sigurnosti, odnosno sigurnosti koja je obuhvaćala veće površine i veći broj ljudi, vidljiv je već 1960-ih godina, kad su postojali noćni stražari koji su pazili na opasnosti koje prijete mjestu na kojem se nalaze (14). Drugu polovicu 20. stoljeća obilježilo je čuvanje posjeda, patroliranje te kontrola pristupa i slični poslovi – era zelenih koliba, engl. „*Green Shack Era*“ (14). Kako se s godinama razvijala sigurnost, takve vrste poslova su postale uredske – era fizičke sigurnosti, engl. „*Physical Security Era*“ (14). Korporativna sigurnost se počela primjenjivati 1980-ih godina, a „osim funkcije zaštite, obuhvaća i krizni menadžment i analizu rizika s ciljem uklanjanja svih oblika ugrožavanja, smanjenja posljedica njihovog djelovanja i osiguranje kontinuiteta poslovanja“ (3).

Kad se razmišlja o korporativnoj sigurnosti, prva pomisao je sigurnost velikih poslovnih subjekata, no danas sve više manjih subjekata brine o svojoj sigurnosti. O vrsti djelatnosti kojom se bavi poslovni subjekt ovise vrsta i razina sigurnosti koja se planira i implementira u određenom poslovanju kako bi se zaštitili interesi poslovnog subjekta (3). Svaki poslovni subjekt je odgovoran za sigurnost svojeg poslovanja, koje može biti izvedeno zapošljavanjem stručnjaka sigurnosne struke ili angažiranjem sigurnosnih stručnjaka izvana. Poslovi korporativne sigurnosti obuhvaćaju i zaštitu od nekih kriminalnih radnji. Mihaljević i Nađ (3) navode korporativni kriminal, kriminal plavog i bijelog ovratnika, zlouporabu autorskih prava i zlouporabu intelektualnog vlasništva kao neke od prijetnji sigurnosti poslovnom subjektu. Iz toga slijedi važnost prevencije kako bi se počinitelje odvratilo od počinjenja, ali i važnost otežavanja provođenja djela zbog kojih može doći do kriznih situacija.

Kako bi se krizne situacije što lakše i bolje sanirale, potrebno je osnovati krizni menadžment, koji kroz analize i planove definira koji su to rizici i koji su najbrži načini otklanjanja neželjenih posljedica na poslovanje. „U poslovnoj ekonomiji kriza označava stanje koje dovodi u pitanje opstanak poduzeća, stanje ugroženosti njegove egzistencije“ (3). Karakteristike kriznih situacija su da nisu vrlo vjerojatne, ali ako do istih dođe, imaju velik utjecaj na poslovni subjekt. Kako bi se utjecaj na poslovanje minimizirao, sastavljaju se planovi u slučajevima kriznih situacija. Kroz planove se pripremaju ljudi i sredstva za adekvatan odgovor na novonastalu situaciju.

Korporativnom sigurnošću se štite temeljne vrijednosti poslovanja na način da se djeluje protiv ugrožavajućih faktora koji predstavljaju opasnost za narušavanje osobne sigurnosti, sigurnosti poslovanja i njene imovine (3). Korporativna sigurnost normatizirana je velikim brojem zakona i pravilnika, kao što su Zakon o privatnoj zaštiti, Zakon o zaštiti na radu (Narodne Novine (NN) 154/14), Zakon o zaštiti od požara (NN 92/10), Zakon o zdravstvenoj zaštiti (NN 154/14), Zakon o zaštiti prirode (NN 80/13), Zakon o zaštiti okoliša (NN 78/15), Zakon o zaštiti osobnih podataka (NN 106/12), Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003-3163), Pravilnik o razvrstavanju građevina, građevinskih dijelova i prostora u kategorije ugroženosti od požara (NN 62/1994-1114) (3). Kako bi se osigurao mir na institucionalnoj razini, potrebna je gospodarska stabilnost (3).

Mihaljević i Nađ (3) navode kako se pojavom suvremenih oblika ugrožavanja mijenja i posao koji obuhvaća korporativnu sigurnost. Potrebna su stručna i praktična znanja, vještine i sposobnosti za obavljanje ovog posla, koji uključuje: provjeru životopisa, zaštitu od sabotaža, očuvanje poslovnih tajni, sigurnost informacijskih sustava te prevenciju i otkrivanje korupcije i pranja novca (3). Ivandić Vidović, Karlović i Ostojić (15) navode kako model poslovnog procesa obuhvaća: privatnu zaštitu, privatnu istražnu djelatnost, informacijsku sigurnost, zaštitu podataka, zaštitu intelektualnog vlasništva, sprječavanje pranja novca, sprječavanje financiranja terorizma, poslovna inteligencija (engl. *business intelligence*), zaštitu na radu, zaštitu od požara, zaštitu okoliša, zaštitu i spašavanje i obrambene pripreme.

Odjelom korporativne sigurnosti upravlja voditelj koji odgovara odboru direktora ili predsjedniku uprave. Uz voditelja, unutar odjela korporativne sigurnosti zaposleni su stručnjaci iz područja sigurnosti, koji su odgovorni za poslove kao što su služba nadzora, sigurnost na radu, zaštita informacijskog sustava, menadžment rizika, poslovi fizičko-tehničke zaštite i analitički poslovi (3).

Mihaljević i Nađ (3) razine sigurnosti dijele na:

1. nisku razinu
2. uspostavljenu (realnu) razinu
3. željenu (maksimalnu) razinu.

Također navode kako je razina sigurnosti nemjerljiva pa vrlo često predstavlja subjektivan osjećaj sigurnosti (3). Narušavanje sigurnosti dovodi do niske sigurnosti, dok je u situacijama kad ne postoje opasnosti riječ o realnoj sigurnosti, koju se želi dovesti do maksimalne sigurnosti (3).

Kako bi se osiguralo što bolje i sigurnije poslovanje, bitan aspekt je i osobna sigurnost svakog pojedinog zaposlenika. Pod osobnom sigurnošću misli se na sigurnost svake osobe, odnosno da se osoba/građanin u određenom trenutku osjeća sigurnim, bez brige od opasnosti. Razna američka sveučilišta (16–19) imaju na svojim stranicama navedene savjete kako poboljšati svoju osobnu sigurnost, primjerice:

- smanjiti i eliminirati situacije u kojima možete postati metom (npr. male ulice, neosvijetljena ili slabo osvijetljena mjesta)
- povećati svjesnost na mjestima gdje se ne osjećate ugodno
- vjerovati svojim instinktima
- pripremiti svoj dnevni raspored imajući na umu svoju sigurnost
- biti svjesni potencijalnih opasnosti
- izbjegavati sve što se ne čini sigurnim
- izbjegavati hodanje uz ulaze u zgrade, grmlje i ostala mjesta gdje se netko može sakriti
- ne razgovarati sa strancima na cesti, samo nastaviti hodati itd.

Osim što navode savjete koji su primjenjivi u svim segmentima života i za sve dobne skupine, imaju savjete koji se tiču života izvan sveučilišta (sigurnost u autobusu, automobilu, kod kuće, na društvenim mrežama). Također, u sklopu svojih stranica sveučilišta imaju mjesta na kojima se može prijaviti kazneno djelo ili bilo kakvo sumnjivo ponašanje. Hrvatska sveučilišta nemaju takav oblik edukacije svojih studenata; jedino što se nudi na stranicama hrvatskih sveučilišta su savjetovališta ili psihološka pomoć, dok preventivnog dijela nema. Svakako je bitno uzeti u obzir činjenicu da u Hrvatskoj nije zabilježen toliko velik broj napada na život i tijelo osobe kao što se to događa u Americi, što ipak ne znači da takvi savjeti, barem oni jednostavni poput reći „ne“, vikati upomoć, bježati ili reći nekome tko vjeruje (20), nisu potrebni.

Abraham Maslow je izradio hijerarhiju potreba, prema kojoj je vidljivo kako je sigurnost, uz fiziološke potrebe, potrebe za osjećajem pripadanja i ljubavi, poštovanjem i samopoštovanjem, te potrebe za osjećajem pripadanja, potreba svakog pojedinca (3). Promicanje osobne sigurnosti kao bitnog aspekta života trebalo bi biti uvršteno u sve faze obrazovanja. Učenje o osobnoj sigurnosti doprinosi poboljšanjima u svim ostalim vrstama iste jer pojedinac kreće od sebe i svojih potreba pa prema tome želi i više razine kad su u pitanju sigurnost društva i organizacije, informatička i informacijska sigurnost i ostale.

U promatranju sigurnosti gospodarskih subjekata, potrebno je uzeti u obzir i sigurnost informacija. Svakodnevno okruženje puno je informacija koje predstavljaju obavijesti o

činjenicama, rezultate obrade podataka, odnosno podatke u bilo kojoj fazi obrade (15). Sukladno tome, potrebno je razlikovati informaciju od podatka, „informacija je podatak koji je obrađen, odnosno podatak koji ima određenu spoznajno-uporabnu vrijednost“ (15). Sve informacije se nalaze u određenim sustavima koji su česta meta napada te je potrebna zaštita istih.

S razvojem informatike i IT sektora, sigurnost informacijskih sustava postaje bitan aspekt poslovanja, u koji se ulaže sve više financijskih sredstava i napora za očuvanjem. Zakon o informacijskoj sigurnosti (NN 79/07, 14/24) (21) definira istu člankom 2. kao „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“. Temelj informacijske sigurnosti je informacija. Tri glavne značajke informacije su u njenoj:

- tajnosti (*engl. Confidentiality*)
- cjelovitosti (*engl. Integrity*)
- dostupnosti (*engl. Availability*) (22).

Prema Zakonu o informacijskoj sigurnosti (21), članku 8., područja informacijske sigurnosti su podijeljena u nekoliko područja, a to su:

1. sigurnosna provjera – utvrđivanje mjera i standarda koji se „primjenjuju na osobe koje imaju pristup klasificiranim podacima“ („Povjerljivo“, „Tajno“, „Vrlo tajno“) (čl. 9., st. 1.)
2. fizička sigurnost – utvrđivanje mjera i standarda „za zaštitu objekta, prostora i uređaja u kojemu se nalaze klasificirani podaci“ (čl. 10., st. 1.)
3. sigurnost podataka – utvrđivanje mjera i standarda koji „se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka“ (čl. 11., st. 1.)
4. sigurnost informacijskog sustava – „područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava“ (čl.12., st.1.)
5. sigurnost poslovne suradnje – primjenjivanje „propisanih mjera i standarda informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom

dokumentacijom koji obvezuju pravne i fizičke osobe iz članka 1. stavka 3. ovoga Zakona“ (čl. 13. st.1.).

Nadalje, Zakon (21) u članku 5. propisuje mjere i standarde informacijske sigurnosti, koji „obuhvaćaju:

- nadzor pristupa i postupanja s klasificiranim podacima
- postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka
- planiranje mjera prilikom izvanrednih situacija
- ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje“.

Potrebno je još istaknuti kako je bitno razlikovati informacijsku i informatičku sigurnost. Informacijska sigurnost se odnosi na sigurnost svih informacija, bez obzira na oblik istih, dok informatička predstavlja sigurnost informatičkih sustava, mreža, računala.

Osim informacijske sigurnosti i sigurnosti ljudi i informacija, potrebna je tehnička zaštita. Danas je to jedan od prvih oblika zaštite koji se postavljaju pri osiguranju objekta, prostora ili osoba. Mnoge privatne tvrtke u Republici Hrvatskoj bave se provedbom tehničke zaštite pa je donesen Pravilnik o uvjetima i načinu provedbe tehničke zaštite. Tako je člankom 1. tehnička zaštita definirana kao „skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini kao što su:

- protuprovalno djelovanje
- protuprepadno djelovanje i
- protusabotažno djelovanje“ (23).

Sustav tehničke zaštite predstavlja povezivanje dvaju ili više povezanih sredstava, naprava i uređaja koji čine funkcionalnu cjelinu. Prema Pravilniku (23), članku 3., sredstva i naprave tehničke zaštite su:

- „sredstva i naprave za tjelesno sprječavanje nedopuštenog ulaska osoba u štićeni objekt“ – specijalne ograde, rampe i barikade, protuprovalna vrata, brave sa serijskim brojem/kodom, specijalne građevne konstrukcije, neprobojna stakla, kase, trezori, naprave za detekciju metalnih predmeta, rendgenski uređaji za kontrolu prtljage i dr.

- „elektronički sigurnosni sustavi koji omogućuju učinkovitu zaštitu štićenog objekta“ – protuprovalni sustavi, video nadzorni sustavi, centralni dojavni sustav, centralni tehnički nadzor
- „sredstva i naprave za neposrednu zaštitu ljudi – protuprepadni alarm“
- „protusabotažni elementi – specijalna ručna ogledala za pregled podvozja vozila“.

Uz tehničku, dodatno se postavlja mehanička zaštita kako bi se postigao viši stupanj sigurnosti. Mehanička sredstva omogućuju nadzor, zabranu kretanja i usmjeravanje pješaka i vozila u slučajevima kada trajni ljudski nadzor nije moguć ili financijski opravdan. Odabir sredstava zahtijeva analizu potreba i očekivanja, uzimajući u obzir unutarnji ili vanjski prostor, razinu sigurnosti, protočnost i prisutnost zaštitarskog nadzora. Pod mehanička sredstva zaštite spadaju rampe, pješačke barijere, prepreke, cilindri i brave, odnosno „sredstva i naprave za tjelesno sprječavanje nedopuštenog ulaska osoba u štićeni objekt“ (23) (sredstva i naprave tehničke zaštite) (24).

Bitan je i članak 4. Pravilnika (23) koji definira što podrazumijeva provedba tehničke zaštite:

1. „snimku postojećeg stanja štićenog objekta i analizu problema s ocjenom;
2. izradbu prosudbe ugroženosti;
3. izradbu sigurnosnog elaborata;
4. definiranje projektnog zadatka;
5. projektiranje sustava tehničke zaštite;
6. izvedbu sustava tehničke zaštite;
7. stručni nadzor nad izvedbom radova;
8. obavljanje tehničkog prijama sustava tehničke zaštite;
9. održavanje i servisiranje sustava tehničke zaštite;
10. uporaba sustava tehničke zaštite“.

Kod provedbe tehničke i mehaničke zaštite, postoji razlika u štićenju objekata pa se prema tome objekti kategoriziraju. Postoji šest kategorija za kategoriziranje štićenih objekata (I-VI), gdje kategorija I. predstavlja najviši stupanj zaštite, a VI. minimum zaštite. Također se izrađuje i prosudba ugroženosti koja pridonosi kod donošenja odluka o stupnju štićenosti pojedinog objekta (23).

Prema članku 8. Pravilnika o uvjetima i načinu provedbe tehničke zaštite, uz prosudbu ugroženosti, potrebno je izraditi sigurnosni elaborat i projektni zadatak, na temelju kojih se izrađuje projekt sustava tehničke zaštite i utvrđuju se:

- „vrsta tehničke zaštite;
- smještaj centra tehničke zaštite;
- smještaj uređaja i opreme;
- način polaganja instalacija“ (23).

Pri projektiranju sustava tehničke zaštite odabiru se vrsta i opseg zaštite, zatim uređaji i oprema, razrađuje se koncepcija zaštite te se na kraju izrađuje projektna dokumentacija (23).

Izvedba tehničke zaštite obuhvaća sljedeće korake, prema članku 15.:

1. izvedba same instalacije – postavljanje potrebne infrastrukture za tehničku zaštitu (kablovi, senzori i druge tehničke komponente)
2. ugradnja uređaja i opreme – montaža i instalacija uređaja (kamere, alarmi, kontrolni paneli i dr.)
3. programiranje, konfiguriranje i testiranje sustava te puštanje u probni rad – konfiguracija i testiranje sustava, provjera ispravnosti i učinkovitosti
4. certifikacija uređaja i opreme, sustava i tehnički prijem – provjera funkcionalnosti i učinkovitosti instaliranih uređaja i opreme te formalni tehnički prijem sustava
5. izrada uputa za rukovanje – kreiranje detaljnih uputa za upotrebu i održavanje sustava;
6. obuka osoblja – edukacija osoblja koja će koristiti i održavati sigurnosni sustav (osiguranje ispravnosti i sigurne uporabe) (23).

Uz prije navedene zaštite, uvodi se čovjek kao crta štićenja, odnosno tjelesna zaštita njegovim prisustvom. Tjelesna zaštita predstavlja još jedan od oblika zaštite objekata, prostora, osoba ili imovine, a obavlja se prisutnošću osobe koja je ovlaštena za obavljanje poslova zaštite prema Zakonu o privatnoj zaštiti i Pravilniku o uvjetima i načinu provedbe tjelesne zaštite.

Prema Zakonu o privatnoj zaštiti (NN 16/20, 114/22) (25), tjelesnu zaštitu obavljaju čuvari, zaštitari (obavljaju poslove tjelesne zaštite osoba i imovine) i zaštitari specijalisti (također obavljaju poslove tjelesne zaštite osoba i imovine, ali imaju višu razinu osposobljenosti, nužne u primjeni sredstava prisile i zaštite entiteta visoke ugroženosti). U poslove tjelesne zaštite visokog rizika ubrajaju se:

- objekti i prostori od interesa za RH
- osobe, objekti i prostori iz I. i II. kategorije ugroženosti
- neposredna tjelesna zaštita (zaštita osobnog integriteta osoba, obavljaju zaštitari specijalisti, drugim nazivom tjelohranitelji)

- osiguranje i pratnja distribucije novca, vrijednosnih papira i dragocjenosti, te transport osoba u prekograničnoj distribuciji
- osobe i imovinu u visokorizičnim okolnostima koje utvrđuje (25).

Zaštitari i zaštitari specijalisti moraju nositi kratko vatreno oružje kad je u pitanju distribucija novca i vrijednosnih papira, na način koji je propisan Zakonom o privatnoj zaštiti, a mogu koristiti i zaštitarskog psa kod obavljanja poslova tjelesne zaštite.

Osobe koje rade na poslovima tjelesne zaštite i kojima je izdano dopuštenje, imaju sljedeće ovlasti: provjeriti identitet osobe (prilikom ulaska, boravka ili izlaska iz štićenog objekta ili prostora, te unutar štićene površine, kada je osoba u vozilu koje ulazi ili izlazi iz štićenog objekta, odnosno prostora, na prostoru s privremeno ograničenom slobodom kretanja, ako je osoba zatečena u izvršenju kaznenog djela ili prekršaja i po nalogu policijskog službenika), davati upozorenja i naredbe (radi zaštite života i sigurnosti štićenih osoba, zaštite štićene imovine, sprječavanja kaznenih djela i prekršaja, hvatanja počinitelja i osiguravanja dokaza, održavanja i uspostavljanja reda i mira u štićenom objektu ili prostoru i radi sprječavanja pristupa ili zadržavanja na štićenom prostoru ili objektu), privremeno ograničiti slobodu kretanja (radi sprječavanja kaznenih djela ili prekršaja, hvatanja počinitelja istih i radi osiguranja svjedoka i dokaza), pregledati osobu, predmet i prometno sredstvo, osigurati mjesto događaja, uporabiti sredstava prisile, koja su prema članku 45., stavku 2.: „tjelesna snaga, raspršivači dozvoljenih neškodljivih tvari, sredstva za vezivanje, zaštitarski pas, vatreno oružje“ (25).

Osobe koje obavljaju poslove privatne zaštite postupaju na temelju naloga i nakon izvršenog posla moraju napisati izvješće o obavljenim poslovima (23).

Kako bi se osigurala sigurnosna zaštita gospodarskog subjekta, potrebno je uzeti u obzir ne samo sigurnost zaposlenika, kako na osobnoj razini, tako i u radnom okruženju, nego i sigurnost poslovanja, odnosno objekta koji se štiti, i to kroz osiguranje tehničke, mehaničke, informacijske i svih ostalih potrebnih vrsta sigurnosti. Kroz osiguranje gospodarskog subjekta na ovakav način, štiti se i poslovanje od rizika koji mu prijete.

4.3. Identifikacija sigurnosnih rizika koji mogu utjecati na gospodarski subjekt

Rizik predstavlja neizvjestan događaj koji bi svaki subjekt volio izbjeći. Međutim, to nije moguće, stoga je bitno biti svjestan rizika koji postoje i koji prijete poslovanju. U većini literature, rizici se dijele na unutarnje i vanjske (15, 26, 27). Unutarnji rizici su oni koji prijete iz samog objekta (ljudi, kvarovi strojeva, problemi sa softwareom itd.), dok vanjske rizike predstavljaju oni na koje organizacija nema utjecaja, poput vremenskih nepogoda, terorizma, hakerskih napada i sl.

Dakle, rizik se može podijeliti na unutarnje i vanjske (15). Prema prikazu Ivandić Vidić, Karlović, Ostojić (15) unutarnji rizici se dijele na:

- financijske – kao što su naplata potraživanja, likvidnost, valutni rizik, promjena kamatnih stopa, investicijski rizik
- operativne – kao što su ljudski potencijali, prodaja, organizacija poslovnog subjekta, inovacije, transportni, promjene u ponašanju potrošača itd.

S druge strane, vanjski rizici se dijele na:

- globalne (ekološki, klimatske promjene, rast siromaštva u nerazvijenim zemljama, terorizam, pojava i širenje zaraznih bolesti itd.)
- ostale (politički, socijalni, zakonodavni, tehnološki, tržišni, gospodarski) (15).

Svaki poslovni subjekt bi trebao za sebe odrediti svoje rizike, kako bi sama analiza rizika bila lakša za izradu i preciznija što se tiče potencijalnih prijetnji.

4.3.1. Unutarnji rizici

Iako se prije nije pridavalo toliko pažnje unutarnjim rizicima, danas je to drugačije jer su sigurnosni stručnjaci zaključili kako isti predstavljaju opasnost za poslovanje, koja lako može biti spriječena ako se obrati pozornost. Marko Cabric (26) unutarnje rizike dijeli u još dvije kategorije: tzv. „rizike činjenja“ i „rizike nečinjenja“. U „rizike činjenja“ ubraja one koji su namjerno učinjeni od strane npr. zaposlenika, ili su isplanirani (prijevare, pronevjere itd.). U drugu skupinu, u „rizike nečinjenja“ spadaju oni koji su proizvod nesavršenosti unutarnjih procesa bez dodatne namjere da se poboljšaju (26).

Unutarnji rizici obuhvaćaju kriminal protiv imovine, ali i reputacijski rizik, seksualno uznemiravanje, *mobbing*, konzumiranje nedozvoljenih supstanci te razne oblike protesta i sl. (26).

4.3.1.1. Reputacijski rizici

Reputacijski rizici predstavljaju ozbiljan problem koji najviše utječe na potrošače, a odnosi se, kako sam naziv kaže, na rizik koji je vezan uz reputaciju gospodarskog subjekta. U ovom slučaju nije riječ o reputaciji vezanoj uz proizvod, etikom subjekta i sl., već o riziku od gubitka dobre reputacije zbog lošeg ponašanja osiguranja ili npr. zaposlenika.

Kad je riječ o ponašanju osiguranja, odnosno zaštitara, treba uzeti u obzir da je prva osoba koju klijent susretne kada dođe u poslovni objekt upravo zaštitar, koji je u većini slučajeva vanjski suradnik. Cubric navodi kako je problem s vanjskim suradnicima taj što su ti zaštitari najčešće potplaćeni i samim time nisu motivirani za obavljanje posla. Također navodi kako se često događa da gospodarski subjekti budu meta napada medija zbog loše procjene ili ponašanja zaštitara koji u određeni prostor ili objekt nije pustio osobu na temelju neke njene značajke, kao što su dob, etnička pripadnost ili invaliditet. Međutim, razlog nepuštanja osobe u neki prostor najčešće nije zlonamjeran, već sa svrhom zaštite te osobe, primjerice u slučajevima nepuštanja trudnica na koncerte na kojima se očekuje velika gužva ili nepuštanja maloljetne osobe na događaj koji promovira alkohol ili cigarete (26).

S obzirom na to da svatko ima drugačiji pogled na istu situaciju, neki ljudi veliku količinu osiguranja mogu percipirati kao nepovjerenje prema klijentima, dok će drugima to biti plus jer će doživjeti da organizacija vodi brigu o sigurnosti svake osobe. Na temelju iste te činjenice će potencijalni kriminalci ili klijenti stvoriti sliku o određenom subjektu kao lakoj meti (26).

4.3.1.2. Pronevjera

Pronevjera predstavlja najučestaliju vrstu kriminala koju čine zaposlenici, i to na način da osoba „protupravno prisvoji tuđu pokretnu stvar ili imovinsko pravo koji su mu povjereni na radu“ (28). Kako bi se počinilo ovo kazneno djelo, trebaju biti ispunjena tri elementa:

1. motiv
2. prilika
3. način.

Kako zaposlenik već ima ispunjene elemente prilike i načina s obzirom na to da mu je željeno dobro povjereno na radu, lako je počiniti kazneno djelo pronevjere jer se treba ispuniti još samo

uvjet motiva. Motivi mogu biti različiti: otkaz, nezadovoljstvo plaćom ili radnim mjestom, dugovi i sl. (26).

4.3.1.3. Krađa

Prema Kaznenom zakonu (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24) (28), krađa je oduzimanje tuđe pokretne stvari s ciljem da je se protupravno prisvoji. Krađa je kazneno djelo koje se lako može zamijeniti za pronevjeru; kod pronevjere je bitan element da je osobi povjereno raditi s određenim dobrom, dok kod krađe osobi nije povjereno na rad ono što je ukrala. Primjerice, zaposlenik A (kojemu su povjerena dobra s odjela A) otuđenjem dobra s odjela B (inače povjerenom zaposleniku B) počini krađu, dok bi, da je istu stvar učinio na svom odjelu, zapravo počinio pronevjeru (26).

Krađa u gospodarskom subjektu može biti bilo koja krađa, bila ona usmjerena prema samom subjektu, zaposlenicima ili klijentima.

4.3.1.4. Prijevara

Prijevaru počini osoba koja „s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist dovede nekoga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da na štetu svoje ili tuđe imovine nešto učini ili ne učini“ (28). Najčešće vrste prijevara u poslovanju vezane su za krivotvorenje podataka na raznim ispravama (npr. vrijeme dolaska, pojedinosti napisane u izvještajima, podaci o zdravstvenom stanju u svrhu dobivanja bolovanja itd.), a uglavnom ih čine zaposlenici na nižim radnim mjestima. Međutim, i na višim se razinama unutar gospodarskog subjekta događaju takvi slučajevi, uz koje se dodatno lažiraju postignuća u određenom razdoblju kako bi se prikrili gubitci (26).

Uz ove prijevare Cabric (26) navodi prijevare vezane uz javnu nabavu (npr. favoriziranje jednog ponuditelja zbog prijateljstva) i putne naloge (npr. lažna putovanja i/ili veći troškovi od stvarnih), prijevare zaposlenika koji su na bolovanju ili rade od kuće, a zapravo obavljaju drugi posao, kao i iskorištavanje pristupa informacijama, kad zaposlenik iste prosljeđuje drugim osobama.

4.3.1.5. Protesti

Protesti predstavljaju nezadovoljstvo radnika koji jednim od načina protestiranja iskazuju svoje nezadovoljstvo prekidom rada ili barem djelomičnim prekidom rada. Štrajkovi, demonstracije i osobni protesti su najčešći u poslovnom svijetu, a zaposlenici se najčešće organiziraju u udruge i sindikate.

Štrajk je prestanak rada velikog broja ljudi, a uglavnom je organiziran od strane sindikata ili radnika koji su se okupili. Kad je u pitanju sigurnost povezana sa štrajkovima, treba biti na oprezu jer se mirni štrajk lako može pretvoriti u neku vrstu agresivne pobune. U takvim situacijama treba se pripremiti i stvoriti plan koji će minimizirati štetu i prevenirati da uopće dođe do takvog nečega. Cabric (26) navodi nekoliko elemenata koje treba imati plan koji se bavi štrajkom, a to su: razumjeti motiv, očekivati i predviđati što se sve može dogoditi, pripremiti radnje kojima će se umanjiti mogućnost nastanka neke veće štete te stvoriti strategiju u slučaju da događaj eskalira.

Demonstracije su političkog karaktera i odvijaju se neovisno, ali mogu biti dijelom štrajka. Sigurnost na takvim događajima je nešto osjetljivija jer ljudi posebno emotivno reagiraju kad je u pitanju politika ili kada se nađe netko suprotna mišljenja. Cabric (26) također navodi kako je preporučljivo imati neku „*low-profile*“ osobu koja će motriti situaciju „iznutra“, odnosno koja će biti dio te demonstracije kako bi se na vrijeme moglo upozoriti osiguranje ili policiju, koja mora biti obaviještena o događanju.

Što se tiče osobnih protesta, riječ je o različitim situacijama u kojima nezadovoljni pojedinci pokušavaju nešto promijeniti ili se izboriti za sebe. Često se događa da bivši zaposlenici namjerno izazivaju problematične situacije ili, primjerice, da osobe koje su na otkaznom roku, prije svojeg odlaska s radnog mjesta, unište opremu ili izbrišu informacije bitne za poslovanje. U planu je potrebno predvidjeti slične situacije kako bi se postavili zaštitni mehanizmi kojima će se onemogućiti takvo djelovanje ili kako bi se osiguralo da se, ako do takvog nečeg ipak dođe, situacija što prije stavi pod kontrolu.

4.3.1.6. Rizici osobne sigurnosti

O osobnoj sigurnosti je već bilo riječi, no za istu na radnom mjestu nije odgovoran samo pojedinac, već i poslodavac, koji u pojedinim situacijama treba reagirati kako sam pojedinac ne bi „uzeo pravdu u svoje ruke“. To se odnosi na situacije kao što su mobing, seksualno uznemiravanje i napadi.

Mobing je pojam s kojim se vrlo često susrećemo kad je u pitanju radno okruženje. Vjerojatno je većina ljudi doživjela neki oblik mobinga, a da toga možda u tom trenutku nije ni bila svjesna. Mobing je zapravo zlostavljanje na radnom mjestu, koje može biti umjereno, ali može biti i takvo da osoba jednostavno na kraju odustane i da otkaz ili počini nešto sebi nažao. U velikim organizacijama nije uvijek moguće vidjeti takve situacije, ali zaposlenike je potrebno upoznati s činjenicom da oni sami mogu prijaviti ako su žrtva ili ako znaju da je netko od kolega u takvoj situaciji, a sve s ciljem kako bi se problem riješio te, na kraju krajeva, kako bi se žrtvi osigurali uvjeti sigurnosti u svrhu postizanja boljih rezultata na poslu.

Jedna od „taboo“ tema je seksualno uznemiravanje na poslu, koje postoji oduvijek i koje se uglavnom ne prijavljuje iz raznih razloga (sram, pomisao da osobi nitko neće vjerovati, da postoji neki drugi razlog prijavljivanja itd.). Ovakav oblik uznemiravanja može biti prisutan na svim razinama, od najniže pa do onih najviših. Uglavnom je slučaj o uznemiravanju žena ili o odnosu nadređeni-podređeni. Kao u prethodnom slučaju, bitno je problem riješiti dok ne preraste u seksualni napad, silovanje ili bilo kakav oblik fizičkog odnosa. Nerješavanje ovakvih problema može dovesti do fizičkog napada.

Fizički napad je uglavnom produkt akumuliranog nezadovoljstva, osjećaja nepravde, mobinga ili seksualnog uznemiravanja/zlostavljanja.

Cabric (26) navodi kockanje i zlouporabu supstanci kao veliki problem u Americi, gdje 13 milijuna pojedinaca aktivno koristi neku supstancu na radnom mjestu (tu su uključeni alkohol, heroin, kokain, marihuana). Jedan od načina na koje se to može regulirati su nasumični pregledi prilikom dolaska na radno mjesto, informacije od drugih zaposlenika, nenajavljena testiranja alkotestom, testiranje urina, krvi i sl.

Kako bi se postigla sigurnost svakog zaposlenika, treba obraćati pažnju na odnose među ljudima i biti svjestan svih mogućih posljedica koje mogu nastupiti ako se ne reagira na vrijeme.

4.3.2. Vanjski rizici

Vanjskim smo rizicima okruženi stalno, isti predstavljaju konstantu u životu svake osobe, subjekta, države. Postoji mnogo rizika koji utječu na poslovanje i svakim danom nastaju neki novi. Kao neki od rizika se mogu navesti ekonomska kriza i recesija, koje za sobom povlače nezaposlenost, nesigurnost bankarskog sektora i politike, nesigurnost građana i siromaštvo, što

dovodi do osjetljive situacije na području koje je zahvaćeno. U takvim situacijama kriminal dolazi do izražaja.

Kriminal predstavlja najveći rizik zbog svoje raznolikosti. S obzirom na tu činjenicu, Cabric (26) kriminal dijeli na:

- kaznena djela protiv imovine – krađa, teška krađa, vandalizam, razbojništvo, pronevjera, ucjena itd.
- kaznena djela protiv tijela – tjelesna ozljeda, ubojstvo, silovanje, otmica itd.
- kaznena djela bez žrtava
- kaznena djela protiv države – špijunaža, prijevare vezane uz plaćanje poreza i sl.
- kaznena djela protiv gospodarstva – mito, korupcija, ometanje pravde i sl..

4.3.2.1. Krađa

Kako je ranije navedeno, krađa je kazneno djelo oduzimanja tuđe pokretne stvari. Kada je u pitanju krađa gledana kao vanjski rizik, najčešće se događa u maloprodajnim djelatnostima. Dobra koja se najučestalije kradu su hrana, alkohol, cigarete i skupi predmeti poput nakita, malih uređaja, parfema ili *brandirane* odjeće (26). Postoje razni elementi koji imaju preventivan utjecaj na potencijalne počinitelje, poput video nadzora, alarma i sl.

Nisu zanemarivi slučajevi krađa službenih automobila. Predstavljaju laku metu počiniteljima jer tvrtke najčešće imaju ista ili slična vozila za obavljanje određenih djelatnosti, tako da počiniteljima koji već imaju razvijene tehnike i alate za takve automobile krađa ne predstavlja veliki problem (26).

Gospodarski subjekti imaju veliki rizik krađe tereta, odnosno dobara u tranzitu. Današnje poslovanje je dinamično, a tržišta su sve zahtjevnija i sve se brže mijenjaju. Živi se konzumerističkim načinom života pa tako do izražaja dolazi i potreba za velikim količinama dobara koja svakodnevno putuju. Počiniteljima su posebno zanimljiva dobra koja mogu brzo i lako prodati, poput cigareta, alkohola, kućanskih uređaja i sl. Velika odgovornost se stavlja na vozače koji prevoze taj teret, čija vrijednost može biti i do nekoliko milijuna eura. Prestanak ili poremećaj opskrbnog lanca predstavlja veliki problem i velike gubitke, bilo da se radi o sirovinama potrebnim za proizvodnju ili o gotovim proizvodima.

4.3.2.2. Teška krađa

Teška krađa predstavlja kazneno djelo koje čini počinitelj:

1. „obijanjem, provaljivanjem ili svladavanjem većih prepreka da dođe do stvari iz zatvorenih zgrada, soba, blagajna, ormara ili drugih zatvorenih prostorija ili prostora,
2. na osobito opasan ili osobito drzak način,
3. iskorištavanjem stanja prouzročenog požarom, poplavom, potresom ili drugom nesrećom,
4. iskorištavanjem bespomoćnosti ili drugog osobito teškog stanja druge osobe,
5. ako je ukradeno oružje, streljivo, rakete, minskoeksplozivna sredstva, borbeno ili dio borbenog sredstva koje služi potrebama obrane,
6. ako ukradena stvar služi u vjerske svrhe ili je ukradena iz crkve ili druge zgrade ili prostorije koja služi za vjerske obrede,
7. ako je ukradeno kulturno dobro ili stvar od znanstvenog, umjetničkog, povijesnog ili tehničkog značenja ili se nalazi u javnoj zbirci, zaštićenoj privatnoj zbirci ili je izložena za javnost,
8. ako je počinitelj pri sebi imao kakvo oružje ili opasno oruđe radi napada ili obrane,
9. kao službena osoba u obavljanju službe ili odgovorna osoba u obavljanju javne ovlasti“ (28).

Kad je u pitanju teška krađa povezana s gospodarskim subjektima, najčešće se izvodi u malim grupama od dva ili tri počinitelja, a ponekad uz pomoć osobe iz subjekta. Organizirani počinitelji mogu ostvariti veći profit jer imaju bolji plan i više ljudi za izvršiti kazneno djelo.

Razlika između počinitelja krađe i teške krađe je u tome što je vjerojatnije da će se počinitelji teške krađe upustiti u neki oblik nasilnog ponašanja ako ih se uhvati u počinjenu kaznenog djela (26).

4.3.2.3. Razbojništvo

Prema hrvatskom Kaznenom zakonu (28), člankom 230. je propisano da je razbojništvo kazneno djelo koje počini osoba koja „uporabom sile protiv neke osobe ili prijetnjom da će izravno napasti na njezin život ili tijelo oduzme tuđu pokretnu stvar s ciljem da je protupravno prisvoji“. Bitan element kod razbojništva je sila ili prijetnja, što razlikuje ovo kazneno djelo od drugih sličnih kaznenih djela.

Kod planiranja aktivnosti za ovakva kaznena djela, potrebno je izraditi smjernice i prijedloge kojima će se objekt učiniti težom metom kako bi odvratilo potencijalne počinitelje, npr. tzv. *interlocking* vrata. Takva vrata se najčešće mogu vidjeti na ulazima u novčarske institucije, a sastoje se od duplih vrata. Rade na principu usporavanja ulaska, odnosno odlaska počinitelja u/iz objekta, na način da se prvo otvore samo jedna vrata, a druga se otvaraju tek kada su prva zatvorena, što zaposlenicima daje dovoljno vremena da procijene osobu koja ulazi. Također je bitno uzeti u obzir mogućnost napada na osobe koje se nalaze na određenom mjestu u određeno vrijeme, te je potrebno kroz obuku zaposlenika „usaditi" im da, ako se nađu u takvoj situaciji, nije bitna imovina koja se otuđuje, već da je bitnije da svi prisutni ostanu neozlijeđeni, čak ako to znači i pomoći počiniteljima da pobjegnu (26).

4.3.2.4. Vandalizam

Vandalizam je pojava u društvu koja je popularnija u mlađim generacijama, no nije isključivo vezana uz njih. Vandalizam predstavlja „(franc. *vandalisme*), oštećivanje, razaranje javne ili privatne imovine bez razloga ili povoda, bezobzirnost prema „kult." vrjednotama" (29).

Ovaj problem se može riješiti uz pomoć nekoliko jednostavnih metoda:

- odabir mjesta na kojem će biti ili će se izgraditi gospodarski subjekt – izbjegavati siromašnije četvrti, dijelove grada koji imaju visoku stopu kriminaliteta, mjesta koja su u blizini sportskih ustanova, klubova, kafića ili mjesta na kojima se odvijaju prosvjedi i demonstracije
- dobra osvijetljenost – iako mali trošak, može odvratiti puno počinitelja od počinjenja zbog osjećaja izloženosti
- postavljanje kamera na vidljiva mjesta ili označavanje da je objekt pod video nadzorom (26).

4.3.2.5. Kibernetički visokotehnološki kriminal

Kibernetički (enlg. *Cyber*) kriminal predstavlja sav kriminal povezan s računalima i mrežom, čija je svrha krađa financijskih i drugih osjetljivih poslovnih informacija (26). Ovakva vrsta kriminaliteta predstavlja veliku prijetnju kako gospodarskim subjektima, tako i nacionalnoj sigurnosti. Cabric dalje navodi kako se računalni kriminalitet dijeli u nekoliko kategorija:

- prijevare i financijski kriminalitet – iznuđivanje, pronevjera, ucjenjivanje itd.
- *cyber*-vandalizam – oštećenje *web* stranice, mijenjanje ili brisanje podataka

- kriminal protiv osoba – *cyber-stalking*, krađa identiteta, uznemiravanje, prijetnje, zlostavljanje (engl. *bulling*) itd.
- kriminal protiv države – špijunaža
- kaznena djela poput gledanja, distribuiranja i preuzimanja ilegalne pornografije (26).

Prednost ovakvog kriminala, za počinitelja, je što se čini iz udobnosti svog doma i lako se na takav način pošalje poruka svijetu, što predstavlja sve veću prijetnju.

Računalni kriminalitet organizacije pogađa financijski, izravnim financijskim gubitkom uzrokovanim kibernetičkom krađom, gubitcima uzrokovanim nefunkcioniranjem stranice, prekidom poslovanja zbog nefunkcioniranja stranica ili aplikacija uzrokovanih kibernetičkim napadom, gubitkom ugleda kod klijenata (npr. zbog krađe osobnih podataka), troškovima osiguranja od računalnog kriminaliteta (softveri, hardveri), troškovima oporavka itd. (26).

Kibernetički napadi su najčešće izvođeni pomoću zlonamjernih softvera, kao što su:

- zloćudni softver (engl. *malware)* – zlonamjerni računalni kod kojem je svrha uništavanje ili krađa informacija s računala
- virus – softver, odnosno program koji ima sposobnost reprodukcije, a „prilaže“ se uz datoteke ili računalne programe
- špijunski softver (engl. *spyware*) – vrsta *malware-a* koja „špijunira“ žrtvu, postoje razne vrste
- računalni crvi – vrsta programa koja se razmnožava i širi putem računalne mreže bez potrebe da ih se prilaže uz datoteke ili programe kao viruse
- napad uzastopnim pokušavanjem (engl. *brute-force attack*) – metoda uzastopnog pokušavanja, koja se koristi kod pokušaja probijanja lozinki na način da se isprobavaju kombinacije slova, brojeva i simbola
- napad rječnikom (engl. *dictionary attack*) – izvode hakeri koji koriste rječnik kako bi pogodili lozinku
- mreža robota (engl. *botnet*) – mreža računala koja se koristi za izvršenje napada poput napada uskraćivanja usluge (engl. *Denial of service* – DoS) i sl. (26).

Cabric (26) navodi kako je visokotehnološki kriminal (engl. *high-tech criminal*) onaj koji je počinjen pomoću novih tehnologija i zapravo *cyber*-kriminal predstavlja podvrstu *high-tech*-a. Navodi primjer *skimming*-a bankomata (postavljanje dodatnog čitača kartica na bankomat, kako bi se ukrali podaci o računu) te navodi kako je to *high-tech* kriminal, ali nije računalni.

4.3.2.6. Vanjske prijevare

Osim prijevara koje se mogu počiniti od strane zaposlenika kao vrsta unutarnjih prijevara, iste se mogu počiniti i prema gospodarskom subjektu od strane osoba koje nisu zaposlenici. Prijevare mogu biti usmjerene prema bilo kojem subjektu, a mogu biti i specifične za određene subjekte. Vrste prijevara s kojima se susreću gospodarski subjekti su:

- prijevare pri prijavama – ove vrste prijevara mogu biti počinjene pri prijavama radnika za posao (lažno prikazivanje diploma i postignuća), prijave za kredit (prikazivanje lažnih i krivotvorenih dokumenata)
- krađa financijskog identiteta – počinjeno s ciljem postizanja osobne dobiti, a uključuje i korištenje ukradene kartice, *skimming* kreditne kartice
- prijevare u osiguranju – prijevare protiv osiguravateljskih kuća prikazivanjem lažnih izvješća, te prijevare mogu biti „male“ (lažno prikazivanje stvari kako bi se ostvarila manja imovinska korist) i „velike“ (namjerno izazivanje događaja poput požara ili prometne nesreće kako bi se ostvarila velika imovinska korist, čak i slučajevi ubojstva ili lažiranja smrti)
- krivotvorine – namjerno krivotvorenje proizvoda, dokumenata, novca, diploma i sl.
- kružne prijevare s gospodarskim subjektima – ovakva se vrsta prijevare može počiniti u kratkom (subjekt je osnovan s ciljem prijevare odmah u kratkom periodu) ili u dugom periodu (subjekt osnovan radi pridobivanja povjerenja, na način da se prvo rade manje narudžbe koje se plate, a onda se naprave velike narudžbe koje se nikad ne plate)
- prijevare u nabavi – iako se mogu počiniti od strane zaposlenika koji nabavlja robu, isto tako ovu vrstu prijevare može počiniti prodavač, npr. isporukom lošije kvalitete robe od dogovorene ili sl.
- mito (davanje ili primanje određenog dobra za neku uslugu) i korupcija (primanje dobra kako bi se postigla ilegalna prednost, uz element iskorištavanja pozicije) (26).

4.3.2.7. Terorizam

Terorizam je postao sve prisutniji od događaja koji je promijenio svijet i pogled na sigurnost - 11. rujna 2001. Terorizam ne predstavlja samo prijetnju nacionalnoj sigurnosti, kako se prije vjerovalo, već i gospodarskim subjektima. Cabric navodi najučestalije vrste terorizma:

- religiozni terorizam – vjeruje se da je najopasniji zbog ideologija i vjerovanja ljudi, kao i zbog spremnosti da učine gotovo sve kako bi postigli svoj cilj (bombaši samoubojice), najpoznatija teroristička skupina ove vrste je Al-Qaeda
- desničarski terorizam – ekstremne nacionalističke grupe koje se bore protiv nacionalnih, rasnih, etničkih i seksualnih manjina, npr. *Neo-Nazi* grupe, Ku Klux Klan
- ljevičarski terorizam – imaju želju ponovno uspostaviti komunistički režim, najpoznatija takva skupina je Narodnooslobodilačka partija-fronta Turske (THKP-C)
- problemski orijentiran terorizam – koriste nasilje (palež, bombardiranje, vandalizam, potapanje brodova) kako bi istaknuli određene probleme, najčešće ekološke ili probleme vezane uz životinje, poput testiranja na životinjama ili lova na ugrožene vrste, takvim oblikom se bavi Fronta za oslobođenje životinja (ALF)
- separatistički terorizam – cilj im je osloboditi dio države koji je naseljen nekom etničkom i/ili religioznom manjinom i uspostaviti državu, kao što je ETA u Španjolskoj (26).

Gospodarski subjekti su pogođeni religioznim i separatističkim terorizmom jer predstavljaju financijsku snagu svojih država u kojima su osnovane, a također imaju veliki medijski potencijal. Desničarski terorizam može neki gospodarski subjekt izabrati kao metu napada iz raznih razloga, kao što je vlasništvo tvrtke u rukama etničke ili rasne manjine, dok ih ljevičarski terorizam percipira kao najveće neprijatelje jer su simbol kapitalizma. Problemski orijentirani terorizam ih vidi kao mete zbog utjecaja na okoliš i testiranja na životinjama (26).

4.3.2.8. Prirodni faktori

Na prirodne faktore se ne može utjecati, a poznato je koliku moć ima priroda i kako katastrofalne i razorne mogu biti vremenske nepogode, bilo da se radi o vremenskim uvjetima, potresima, požarima ili snažnim vjetrovima. Nedavno je cijeli svijet svjedočio pandemiji koja je utjecala na svaki segment života, a na našem su području značajan utjecaj imali i razorni potresi koji su pogodili unutrašnjost Republike Hrvatske.

Pozitivna strana prirodnih nepogoda je ta što se do neke mjere mogu predvidjeti, ovisno o kojem kraju svijeta je riječ. U Hrvatskoj se zna u kojim se razdobljima i na kojim područjima najčešće mogu očekivati poplave ili bura pa se, shodno tome, građani i/ili gospodarski subjekti mogu pripremiti. Loši vremenski uvjeti mogu na puno načina utjecati na poslovanje, od toga da zbog poplave zaposlenici ne mogu doći na posao do toga da dostava ne može doći zbog bure. S druge strane, tu je slučaj epidemije, kad je sve zatvoreno i kad je puno ljudi bolesno pa

nisu sposobni obavljati svoje svakodnevne zadatke. Svi ovi faktori imaju velik utjecaj na gubitke u poslovanju te je potrebno biti spreman odgovoriti na njih na adekvatan način.

4.3.2.9. Rizik poslovnog putovanja

U većini se poslova zaposlenici susreću s potrebom putovanja u druge gradove, ponekad i druge države, kako bi se proširila poslovna suradnja, unaprijedilo postojeće poslovanje ili, primjerice, zbog potrebe edukacije. Rizik poslovnog putovanja je usmjeren prema zaposlenicima koji putuju i njihovoj sigurnosti dok su na putovanju. Rizici su razni, od onih najgorih poput otmica, pa do onih koji se tiču bolesti, sanitetskih uvjeta, hrane, medicinske skrbi ili dostupnosti lijekova na području na koje se putuje. Tu je potrebno educirati zaposlenike koji putuju i osvijestiti ih o mogućim prijetnjama kako bi ih izbjegli na što bolji mogući način, te kako bi se pripremili na uvjete koji ih čekaju.

4.3.2.10. „Curenje“ podataka

Curenje podataka predstavlja još jedan rizik koji je vrlo vjerojatan, a vrlo bitan za poslovanje, pogotovo ako je riječ o gospodarskom subjektu koji ima unikatnu proizvodnju, proizvod, postrojenja ili sl. Curenje podataka se može dogoditi u bilo kojem dijelu poslovanja, na bilo kojoj razini, samo je potrebno malo nepažnje. Naravno, mogući su i slučajevi namjernog davanja podataka u neke druge svrhe. Kod ovog rizika ljudi predstavljaju najslabiju kariku (26).

Način na koji se mogu izbjeći ovakvi scenariji su jednostavni: držati radni stol čistim u slučaju posjeta, micati sve dokumente koji sadrže informacije koje predstavljaju poslovnu tajnu, ne stavljati previše informacija na *Web* stranicu, ugasiti računalo, ne ostavljati papire u automobilu okrenute tako da se vidi što na njima piše i sl.

4.4. Sigurnosna zaštita objekata, površina i pogona

Sigurnosna zaštita predstavlja sve mjere koje se poduzimaju kako bi se zaštito subjekt štićenja. Razlozi štićenja objekata, površina i pogona mogu biti različiti, od želje da se onemogući pristup neovlaštenim osobama, do toga da se sačuva proizvodni proces, ljudi koji se tamo nalaze i sl. Objekti, površine i pogoni se štite primjenom tjelesne, mehaničke i tehničke zaštite, koje se povezuju u smislenu i funkcionalnu cjelinu.

Potrebno je uspostaviti plan zaštite koji će obuhvatiti sve potencijalne rizike i načine njihova otklanjanja. Također se treba procijeniti objekt, površinu i prostor te ih svrstati u jednu od kategorija Pravilnika o uvjetima i načinu provedbe tehničke zaštite, prema kojima će se odrediti koje su sve mjere potrebne za postizanje efikasnog štićenja.

Tjelesna, odnosno fizička, zaštita se provodi kroz prisustvo zaštitara, bilo da je riječ o vanjskom zaposleniku ili zaposleniku subjekta koji se štiti. Poslovi i ovlasti zaštitara navedeni su ranije u radu. Kad je u pitanju tjelesna zaštita objekata, zaštitar bi trebao biti prva osoba na koju se nailazi u trenutku pokušaja stupanja u štićeni objekt. Primjenom svojih ovlasti, zaštitar identificira osobu koja ulazi te vodi knjigu ulazaka i izlazaka iz štićenog objekta. Zaštita površina tjelesnom zaštitom može predstavljati nešto veći problem jer za pokrivanje većih površina treba veći broj ljudi ili kombinacija mehaničke, tehničke i tjelesne zaštite.

Mehaničku zaštitu predstavljaju „specijalne ograde, rampe i barikade, protuprovalna vrata, brave sa serijskim brojem/kodom, specijalne građevne konstrukcije, neprobojna stakla, kase, trezori, naprave za detekciju metalnih predmeta, rendgenski uređaji za kontrolu prtljage i dr.“ (23). Pri zaštiti zatvorenih prostora mogu se koristiti rešetke na prozorima, protuprovalna vrata, okretne barijere, naprave za detekciju metalnih predmeta ili rendgenski uređaji, ovisno o vrsti prostora koji se štiti, dok se kod otvorenih prostora mehanička zaštita može vršiti postavljanjem ograda, rampi ili neke vrste barikada, a kako bi se postigla bolja zaštita, može se kombinirati sa tehničkom ili tjelesnom zaštitom. Zaštita pogona treba onemogućiti ulazak neovlaštenim osobama, što zbog njihove osobne sigurnosti, što zbog očuvanja tajne poslovnog procesa.

Kako je ranije navedeno u radu, osim fizičke zaštite, postoji i tehnička zaštita koja se upotrebljava u zaštiti objekata, površina i pogona. U tehničku zaštitu, kako je navedeno, spadaju mjere i radnje kako bi se od štićenog objekta odbilo:

- „protuprovalno djelovanje
- protuprepadno djelovanje i

- protusabotažno djelovanje“ (23).

Protuprovalno djelovanje se postiže primjenom tehničkih sredstava poput alarmnih sustava, video nadzora, sustava kontrole pristupa i sl. (30). Fajković (31) navodi kako u sustave tehničke zaštite spadaju:

1. „sustavi za detekciju ulaska u zatvoreni prostor,
2. sustavi za dojavu prepada,
3. sustavi za detekciju ulaska u otvorene prostore,
4. sustavi za nadgledanje štićenog prostora,
5. sustavi za detekciju nastanka požara,
6. ostali sustavi zaštite (detekcija koncentracije otrovnih plinova i sl.)“ .

Kad su u pitanju sustavi tehničke zaštite i video nadzora, isti mogu biti jednostavni (senzori pokreta, magnetni, kontaktni na prozorima ili vratima) ili složeni sustavi koji uključuju integraciju različitih sustava u jednu cjelinu (30).

Sustavi protuprovale su najčešće korišteni za zaštitu objekta, a svrha im je usporiti i detektirati neovlašteno kretanje unutar štićenog prostora. Želi se u što ranijoj fazi otkriti i usporiti počinitelja uzbuđivanjem alarma, a samim postavljanjem se pokušava i počinitelja odvratiti od počinjenja kaznenog djela. Sustavi protuprovale se sastoje od:

- alarmne centrale – obrađuje primljene signale s detektora i aktivira uređaj za signalizaciju i komunikaciju, te je povezano dodatno sa zvučnim ili svjetlosnim signalizatorima i upravljačkom tipkovnicom
- upravljača – najčešće tipkovnica blizu ulaznih vrata kako bi se prilikom ulaska/izlaska isključio, odnosno uključio alarmni sustav, a mogu biti i daljinski upravljači
- napajanja
- detektora (razne vrste) – jedan od najvažnijih dijelova sustava, koriste se za zaštitu unutrašnjosti objekta i vanjskog ruba, a mogu biti:
    - kontaktni detektori – mehanički ili magnetski prekidači, reagiraju kada se promijeni položaj, a postavljaju se na vrata ili prozore
    - detektori pokreta – detektiraju tijelo u pokretu koje se nalazi u štićenom prostoru, mogu biti ultrazvučni, mikrovalni i infracrveni
    - detektori loma stakla – prepoznaju karakteristične frekvencije lomljenja, a dijele se na: akustične (postavljaju se suprotno od prozora koji se nadzire), aktivne

(detektiraju promjene na samoj površini), pasivne (postavljaju se na prozor ili okvir prozora)
    - folije za zaštitu staklenih površina – aktivira ih razbijanje stakla na kojem je metalna folija kroz koju protječe struja
- uređaja za signalizaciju i komunikaciju – unutarnje ili vanjske sirene i/ili bljeskalice (30,31).

Osim alarmnih sustava, koristi se i video nadzor. Video nadzor je postao osnovni element u zaštiti objekata ili prostora koji su od važnosti, a sastoji se od jedne ili nekoliko kamera također povezanih centralnim uređajem koji šalje sliku na zaslon kako bi se pratile aktivnosti (30). Elementi sustava video nadzora su: kamera, uređaj za snimanje, uređaj za pristup sustavu, uređaj za upravljanje i nadzor sustava (30).

Nadzorne kamere koriste se u kombinaciji s drugim uređajima za snimanje te se prate preko monitora. Vrste kamera koje se danas koriste su:

- bežične kamere – manje upadljive, prenosive, jednostavne
- unutarnje kamere – široko vidno polje, postavljaju se na stropove i zidove kako bi bile izvan dometa ruku
- vanjske video kamere – otpornije na vremenske uvjete
- kamere s ugrađenim detektorom pokreta – prvo se uključuje detektor pokreta pa tek onda počinje snimanje, mogu biti: oklopne kupolaste, varifokalne kupolaste, infracrvene kupolaste
- podesive kamere za video nadzor – najviši stupanj kontrole i sigurnosti, funkcioniraju na daljinsko uključivanje (*zoom* opcija odlična za detaljan pregled objekta i osoba koje borave u njemu) (30).

Bitna funkcija kod protuprovalnih i protuprepadnih sustava je da alarmni signal stigne do zaštitarskog dojavnog centra putem posebnog prijemnika kojim operateru daje uvid u status štićenih prostora (30).

Kad je riječ o protuprepadnom djelovanju, najčešće se govori o tzv. panik tipki, koja se nalazi negdje skrivena te se aktivacijom iste šalje signal dojavnom centru, ali se ne uzbuđuje alarm gdje je aktiviran, što je vrlo korisno u situacijama poput razbojništva ili oružanih pljački u bankama i poštama. Također se koriste „šifre prisile“ koje služe za isključivanje alarma unutar štićenog objekta, dok s druge strane alarmiraju centralni dojavni sustav (30). Uz navedene

vrste, mogu se postaviti i nagazne pedale ili nagazne šine, koje imaju istu svrhu kao „panik tipka“ (31).

Protusabotažno djelovanje sprječava bilo kakav utjecaj na elemente zaštite štićenog objekta, bez obzira na to radi li se o fizičkom onesposobljavanju video nadzora ili napadu na programski dio zaštite (30).

Pod tehnička sredstva za osiguranje ubrajaju se i vatrodojavni sustavi. Postojanje ovakvog sustava je od izuzetne važnosti, pogotovo za proizvodne procese i pogone kod kojih lako može doći do požara, kako bi se što prije spriječilo nastajanje šteta velikih razmjera. Prema Zakonu o zaštiti od požara (NN 92/10, 114/22) (32), „požar je samopodržavajući proces gorenja koji se nekontrolirano širi u prostoru“. Sustav za gašenje požara se sastoji od:

- vatrodojavne centrale – glavni dio sustava vatrodojave gdje dolaze ulazne informacije, na temelju kojih se šalju upute izvršnim elementima
- javljača požara – razni detektori ili ručni prekidači
- signalizacije – zvučna ili svjetlosna
- izvršnih elementa – sustavi za gašenje ili usporavanje požara,

a tipovi vatrodojavnih sustava mogu biti:

- klasični – koriste se detektori porasta temperature ili dima koji imaju zvučnu i svjetlosnu signalizaciju (stanovi, kuće manjih kvadratura)
- adresabilni – svaki javljač ima jedinstvenu adresu u sustavu (točno utvrđivanje lokacije izvora požara)
- adresabilni s više stanja – prati promjenu požarne veličine (normalno stanje, predalarmno (vrijednost požarne veličine se približava alarmu) ili alarmno stanje)
- suvremeni analogno-adresabilni – javlja točnu lokaciju detekcije odgovornoj osobi, za profesionalnu namjenu u velikim građevinskim kompleksima (30).

Detektori požara predstavljaju važan dio sustava jer brzina detekcije ovisi o brzini reakcije na požar. Postoje razne vrste detektora, koje se postavljaju ovisno o vrsti. Postoje preporuke prema kojima se postavljaju detektori, kao npr. podjela u zone velikih zgrada i minimiziranje broja detektora u pojedinoj zoni; ako je ukupna površina veća od $300m^2$, svaki kat treba biti najmanje jedna zona, a ako je manje od $300m^2$, cijela zgrada može biti jedna zona (30). Ovisno o vrsti prostorije i vrsti požara koji može izbiti u štićenom prostoru, biraju se i detektori (otvoreni plamen, požar koji oslobađa velike količine dima i dr.) (31). Detektori se mogu podijeliti na:

- detektore dima – ionizacijski (pouzdani i osjetljivi, za detekciju brzih požara s plamenom, štetni za ljude), optički (najkorišteniji, detektiraju dim i produkte gorenja u ranoj fazi, mjeri količinu dima), s projiciranom zrakom (za velike prostore, veliki domet)
- detektore topline – fiksne temperature (naziva se i termomaksimalni, detektira požar na određenoj temperaturi (55-60°C), požari bez dima), porasta temperature (termodiferencijalni, koristi se u kombinaciji s fiksnim, detektira brzi rast), linijski temperaturni (tuneli, kabelski kanali), bimetalni obnovljivi
- detektore plamena – ultraljubičasti (u slučaju brzih požara zapaljivih tekućina i plinova, upozoravaju pri detektiranju ultraljubičaste komponente), infracrveni (za požare ugljikovodika, reagiraju na infracrveno zračenje požara)
- ručni javljač požara – ručno aktiviranje čovjeka (30).

Kako bi se utvrdila potrebna razina zaštite od požara, donesen je Pravilnik o razvrstavanju građevina, građevinskih dijelova i prostora u kategorije ugroženosti od požara. Razvrstavanje u četiri kategorije vrši se s „obzirom na vrstu zapaljivih tvari, namjenu građevine i prostora te površinu otvorenog prostora, a temelji se na sljedećim uvjetima, osnovama i kriterijima: instaliranom kapacitetu za proizvodnju ili preradu; kapacitetu nadzemnih spremnika ili građevina za zapaljive tvari; broju uposlenih.“ (33).

Još jedna od opasnosti koja prijeti u objektima i pogonima je plin pa je shodno tome potrebno imati i sustav plinodojave, koji se sastoji od: detektora, dojavne centrale i izvršnih elemenata (signaliziranje, alarmiranje, automatske akcije ventilacija i klimatizacije) (30). Detektori su najčešće specijalizirani za detektiranje samo jedne vrste plina, npr. ugljičnog monoksida, zemnog plina. Mogu biti i za veći spektar plinova, ali nisu toliko osjetljivi (30). Mogu biti: fiksni – učvršćeni na jednom mjestu, za detekciju jedne ili više vrsta plinova i prijenosni – za nadzor atmosfere oko zaposlenika. Za detekciju plinova razlikuju se: elektrokemijski, fotoionizacijski, infracrveni, poluvodički, ultrazvučni, holografski detektori plina (30).

Nadalje, kao element tehničke zaštite javlja se kontrola pristupa, kojom se ograničava i onemogućava pristup neovlaštenim osobama kako bi se zaštitili objekti ili dijelovi objekata koji su od posebnog značaja. Postoje dvije vrste kontrole pristupa:

- samostojeći uređaji – svrha im je isključivo kontrola pristupa putem čitača

- komunikacijsko vezani – ista namjena kao i samostojećih, ali ova vrsta još obrađuje podatke evidencije ulazaka i izlazaka (evidencija radnog vremena uz kontrolu pristupa) (30).

Kontrola pristupa se može obavljati i putem kartica; ovisno o vrsti kartice i čitaču, s različitih udaljenosti se može autentificirati kartica. Još jedan od načina je autentifikacija biometrijom, koja predstavlja siguran način identifikacije korisnika jer nije nešto što korisnik posjeduje, odnosno može izgubiti (poput kartice), već je to karakteristika koja je stalna, jedinstvena i nepromjenjiva (kada je riječ o otisku prsta).

Kod sustava na detekciju ulaska na štićene otvorene prostore, Fajković (31) navodi: mikrovalne i infracrvene, odnosno laserske barijere (sastoje se od predajnog i prijemnog dijela, zahtijevaju ravno tlo, bez trave, grmlja i sl.), sustavi za detekciju titranja žičanih i dr. ograda (prepoznaju se karakteristične vibracije rezanja, prelaženje i ostale nedopuštene radnje).

Najbolju zaštitu objekata, površina i prostora sigurno pruža kombinacija navedenih elemenata, kao što je postavljanje perimetra, odnosno osiguranje vanjskog dijela ili površina nekom od mehaničkih vrsta zaštite u kombinaciji sa tehničkom i/ili fizičkom, ovisno što se štiti na određenom prostoru. Ista je situacija kad je u pitanju zaštita objekata ili pogona. Ovim načinima zaštite nastoji se osigurati da poslovni procesi funkcioniraju nesmetano.

4.5. Sigurnosna zaštita poslovnog procesa

Poslovni proces predstavlja skup radnji i mjera koje međusobno djeluju, pretvarajući ulazne elemente u izlazne rezultate (15). Poslovni procesi mogu biti upravljački (razvoj misije, vizije i strategije poslovanja, nadzor i kontrola poslovanja), temeljni poslovni procesi (razvoj proizvoda/usluga, prodaja istih) i potporni (razvoj i upravljanje ljudskim potencijalima, računovodstvo i poslovno izvješćivanje, upravljanje rizicima, procesi korporativne sigurnosti itd.) (15). Potrebno je izraditi strategiju upravljanja poslovnih procesima, dizajnirati poslovni proces, implementirati te na kraju izvršiti kontrolu poslovnog procesa. Poslovnim procesima se prikupljaju razne informacije koje je potrebno zaštititi. Takve informacije se nazivaju poslovnim informacijama jer su potrebne za obavljanje poslovnih procesa i aktivnosti. Vrlo često je situacija da su poslovne informacije zapravo poslovna tajna.

O informacijskoj sigurnosti je već bilo riječi, no tu je potrebno naglasiti kako za sve informacije koje se prikupljaju (osobni podaci zaposlenika, poslovnih suradnika itd.) postoje normativne obveze subjekata da štite te podatke. Prema Ivandić Vidović i suradnicima (15), sustav planiranja informacijske sigurnosti sastoji se od četiri faze:

1. planiranje – postavljanje ciljeva, odabir sigurnosnih mjera
2. implementacija – provodi se isplanirano kroz izradu planova i njihovu implementaciju
3. nadzor i provjera – utvrđivanje ispunjavaju li rezultati postavljene ciljeve
4. održavanje i poboljšavanje – usavršavanje svega što je u prethodnoj fazi zabilježeno.

Tajna je nešto za što se želi osigurati da ostane skriveno, da nitko drugi ne sazna za to. Kako u privatnom, tako i u poslovnom svijetu postoje tajne. Tajnost podataka definirana je Zakonom o tajnosti podataka (NN 79/07, 86/12) (15), a predstavlja podatke i informacije koje se koriste u poslovanju, a subjektu donose prednost pred konkurencijom. Poslovna tajna mogu biti poslovne metode, proizvodni postupci, sastojci proizvoda, rezultati istraživačkog rada i sl. koji se ne smiju reći neovlaštenim osobama. Prema Zakonu o zaštiti tajnosti podataka (NN 108/96) (34), članku 20. „pravna osoba dužna je čuvati kao tajnu podatke:

1. koje je kao poslovnu tajnu saznala od drugih pravnih osoba,
2. koji se odnose na poslove što ih pravna osoba obavlja za potrebe oružanih snaga, redarstvenih vlasti Republike Hrvatske ili drugih javnih tijela, ako su zaštićeni odgovarajućim stupnjem tajnosti,
3. podatke koji sadrže ponude na natječaj ili dražbu - do objavljivanja rezultata natječaja odnosno dražbe,

4. podatke koji su zakonom, drugim propisom ili općim aktom doneseni na temelju zakona utvrđeni tajnim podacima od posebnog gospodarskog značenja“.

Poslovna tajna se može priopćiti drugima samo na temelju općeg akta i te su je osobe onda dužne čuvati, a unutar subjekta se određuje ovlaštena osoba ili posebno tijelo koje brine o poslovnim tajnama, uvidu, čuvanju i odlučivanju o tome koje osobe imaju pravo pristupa (34). Uz poslovnu tajnu, postoji i profesionalna, a odnosi se na podatke koje su u obavljanju svog posla saznali zdravstveni djelatnici, svećenici, odvjetnici i druge osobe u obavljanju svoje dužnosti. Postoje i drugi stupnjevi tajnosti koji se koriste u poslovanju, ovisno o djelatnosti subjekta. Vrste tajni, prema članku 5., mogu biti: vrlo tajno (podaci koji bi nanijeli nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima RH), tajno (podaci koji bi teško naštetili nacionalnoj sigurnosti i vitalnim interesima RH), povjerljivo (podaci koji bi naštetili nacionalnoj sigurnosti i vitalnim interesima RH) i ograničeno („neovlašteno otkrivanje bi naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova“) (35,36).

Kako bi se osigurala sigurnost informacija pri poslovnim suradnjama, Ivandić Vidović i suradnici (15) navode mjere informacijske sigurnosti poslovne suradnje:

- sklapanje klasificiranih ugovora – potpisivanje izjave o zaštiti klasificiranih podataka, ovisno o stupnju tajnosti klasificiranog ugovora potrebno je posjedovati certifikat poslovne sigurnosti
- certifikat poslovne sigurnosti – zahtjev za izdavanje se dostavlja Uredu Vijeća za nacionalnu sigurnost, provodi se sigurnosna provjera subjekta, a sami certifikat vrijedi 5 godina
- sigurnosni uvjeti za sklapanje klasificiranih ugovora – izrada naputaka i uputa o sigurnosnim mjerama
- prijevoz klasificiranog materijala – ovisno o stupnju tajnosti ovisi i potreba odgovarajućeg certifikata sigurnosne provjere osobe koja postupa s takvom pošiljkom
- pristup klasificiranim podacima prilikom međunarodnih posjeta – tijela koja šalju zaposlenike na takve posjete moraju prijaviti te zaposlenike nadležnom tijelu te države ili međunarodne organizacije preko Ureda Vijeća za nacionalnu sigurnost
- razmjena osoba u sklopu projekata ili programa.

Sklapanje ugovora predstavlja sastavni dio poslovnih procesa koji se najčešće održavaju na sastancima ili poslovnim putovanjima. Kako bi se, između ostalog, osigurala sigurnost poslovanja kroz poslovne procese, bitno je da su ljudi koji obavljaju te poslove sigurni. Kad je

u pitanju sigurnost poslovnog procesa na poslovnim sastancima, bitno je imati u vidu koje se osobe nalaze u prostoriji te prema tome prilagoditi sadržaj i teme koje će se prolaziti na sastanku, sve s ciljem sačuvanja integriteta poslovnog subjekta. Takvo stajalište vrijedi imati i pri razgovorima sa strankama ili bilo kojim drugim vanjskim osobama.

Posebnu pažnju treba posvetiti sigurnosti na poslovnim putovanjima, pogotovo ako je riječ o putovanjima van države, gdje uz segmente osobne i poslovne sigurnosti treba voditi računa o običajima i tradiciji države u koju se dolazi, posebno ako je riječ o državama koje nisu slične što se tiče vrijednosti, običaja i tradicije. O riziku poslovnog putovanja je bilo riječi ranije u radu.

Zbog osjetljivosti ovakvih podataka, potrebni su i drugi oblici zaštite, poput zaštite ranije navedenih objekata u kojima se takve informacije čuvaju, zaštite sigurnosti ljudi, pa i sustava i uređaja na kojima se takvi podaci pohranjuju, pogotovo zato što je u posljednje vrijeme opasnost od kibernetičkih napada sve veća. Subjekti koji su od značaja za RH predstavljaju posebno primamljivu metu zbog članstva Hrvatske u NATO i EU (37).

Kibernetička sigurnost predstavlja procese, mjere i standarde kojima se postiže pouzdanost u kibernetičkom prostoru, a zaštita mobilnih uređaja, podataka, računala, informatičke i informacijske infrastrukture pridonosti tome (38). U svrhu osiguranja sigurnosti informacijskog sustava i tajnosti podataka, o kojima je u ovom slučaju riječ, donesena je Uredba (EU) 2019/881, Nacionalna strategija kibernetičke sigurnosti i Akcijski plan, te Zakon o kibernetičkoj sigurnosti. Uz donesene pravne propise, osmišljen i osnovan je sustav, odnosno projekt Sigurnosno obavještajne agencije (SOA) i Zavoda za sigurnost informacijskih sustava (ZSIS) za zaštitu nacionalnog kibernetičkog prostora Republike Hrvatske, SK@UT, koji je namijenjen za rano otkrivanje, upozoravanje i zaštitu od državno-sponzoriranih kibernetičkih napada (APT – *Advanced Persistent Threat*) (39). Sama kibernetička sigurnost definirana je Uredbom (EU) 2019/811 (40) člankom 2. kao „sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu“, a „kiberprijetnja“ znači svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike tih sustava i druge osobe“. Kibernetičke prijetnje se mogu podijeliti u četiri kategorije:

1. kibernetički kriminal – kriminal koji uključuje računala (internet bankarstvo, prijevare u web trgovinama i sl.)

2. kibernetička špijunaža – dolaženje do tajnih informacija bez dopuštenja (tajne informacije vezane uz poslovanje i sl.)
3. kibernetički terorizam – planirani i politički motivirani napadi
4. kibernetički rat – rat pomoću računala i računalnih mreža (informacijski rat) (41).

Također je u smislu kibernetičke sigurnosti donesen i ISO standard 27032, koji pruža smjernice za poboljšanje kibernetičke sigurnosti kad je u pitanju sigurnost informacija, mrežna sigurnost, internet sigurnost i zaštita kritične informacijske infrastrukture (41).

4.6. Izrada plana sigurnosne zaštite gospodarskog subjekta

Plan sigurnosne zaštite predstavlja sveobuhvatnu cjelinu formaliziranih postupaka i izvora informacija koje gospodarski subjekti mogu koristiti pri oporavku, kako bi poslovanje i dalje funkcioniralo normalno, od negativnog događaja koji je planom predviđen kao rizik (42). Mnogi gospodarski subjekti imaju plan oporavka od katastrofe (engl. *disaster contingency recovery plan (DCRP)*) koji je reaktivan, tj. odnosi se na određivanje procedura kada dođe do neželjenog događaja. S druge strane, plan sigurnosne zaštite (*engl. Business continuity plan (BCP)*) predstavlja proaktivni, odnosno preventivan pristup jer sadrži pregled potencijalnih prijetnji i načina njihovog rješavanja prije nego do njih dođe, a također i postupanja prije, za vrijeme i nakon neželjenog događaja (27,43), što znači da je *DCRP* zapravo sastavni dio plana sigurnosne zaštite (engl. *Bussines continuity plan – BCP*). Ne postoji plan koji je univerzalan i primjenjiv na sve gospodarske subjekte, već je potrebno da svaki subjekt za sebe izradi sveobuhvatan plan baziran na specifičnoj situaciji; nije pitanje „ako“ se nešto dogodi, već „kada“ će se dogoditi. Također je potrebno stalno nadograđivati plan u skladu s promjenama koje su prisutne u poslovnom, tehnološkom i drugom okruženju.

Benyoucef i suradnici (42) navode kako kroz pet koraka napraviti plan sigurnosne zaštite:

1. izrada okvira za upravljanje projektima
2. identifikacija potencijalnih rizika te načina i vremena oporavka
3. uspostava akcijskog plana (resursi, proces donošenja odluka itd.)
4. pregled i testiranje te nadopuna plana (preporuka je svakih 6 mjeseci)
5. navesti neke druge potencijalne probleme, kao npr. preseljenje ureda.

Cerullo i Cerullo (27) navode tri glavna cilja koja bi trebao imati svaki plan:

1. identifikacija rizika
2. razvoj plana za oporavak
3. obuka zaposlenika i testiranje efektivnosti plana.

Prema istraživanjima iz 2004. godine, koja navode Cerullo i Cerullo (27), a u kojima je sudjelovalo 459 srednje velikih i velikih kompanija, prikazano je kako je samo 53% tih subjekata imalo plan sigurnosne zaštite, dok 21% subjekata nije provelo testiranje svog plana, a manje od 50% subjekata nije utvrdilo vrijeme oporavka, što može dovesti do velike razlike u očekivanjima između onoga što poslovanje treba i što plan nudi. Iako je istraživanje provedeno prije 20 godina, situacija se nije puno promijenila kad je u pitanju Hrvatska. U razgovoru sa

sigurnosnim ekspertima, koji se dugi niz godina bave izradom planova sigurnosne zaštite gospodarskih subjekata, luka, kritične infrastrukture i sl., potvrdili su kako veliki broj velikih subjekata, poput obrazovnih institucija i objekata kritične infrastrukture, nemaju adekvatno izrađene planove sigurnosne zaštite.

Prema Fani i Subriadi (43), struktura plana sigurnosne zaštite sastoji se od osam elemenata i 38 aktivnosti uz usvajanje PDCA (Planiraj-Uradi-Provjeri-Djeluj, engl. *Plan-Do-Check-Act*) kruga:

1. *plan* – planiranje i uspostavljanje ciljeva:
    a. utvrđivanje potrebe za menadžmentom kontinuiteta poslovanja (engl. *Business Continuity management*)
2. *do* – primjena procesa:
    a. analiza rizika – fokusira se na identifikaciju rizika, procjenu rizika i utjecaj na organizaciju
    b. analiza utjecaja na poslovanje (engl. *Business impact analysis*) – prepoznavanje i određivanje prioritetnih poslovnih funkcija
    c. strategija kontinuiteta poslovanja (engl. *Business continuity strategy*) – utvrđivanje odgovornosti utjecaja na poslovne procese
    d. plan oporavka od katastrofe (engl. *Disaster recovery plan (DRC)*
    e. obuka zaposlenika
3. *check* – nadzor i provjera
    a. testiranje plana sigurnosne zaštite
4. *act* – poduzimanje aktivnosti za unaprjeđenje plana
    a. pregled plana sigurnosne zaštite (44).

4.6.1. Analiza rizika

Rizik predstavlja neizvjestan događaj koji, ako se dogodi, može imati pozitivan ili negativan utjecaj na ciljeve poslovanja (42). Rizici mogu biti vanjskog i unutarnjeg tipa, kao što je ranije navedeno u radu (prirodne katastrofe, ljudske greške, virusi itd.).

Analiza rizika predstavlja kontinuirani proces koji se koristi kako bi se identificirale potencijalne opasnosti, odredili prioriteti i analiziralo što se može dogoditi ako se takva katastrofa ili opasnost dogodi (26,45). Puno je potencijalnih opasnosti, a sa svakom opasnošću (bile unutarnje ili vanjske) dolazi isto tako veliki broj mogućih scenarija. Ranije u radu navedena je i podjela rizika na unutarnje i vanjske, na što je potrebno skrenuti pozornost kod

izrade same analize rizika. Kako bi se rizične situacije što bolje i lakše predvidjele, postoje razni alati kojima se vrši analiza rizika.

Analiza rizika se naziva i majkom svih sigurnosnih analiza, a provodi se kroz četiri glavna koraka:

- identifikacija vrijednosti koja se štiti
- identifikacija opasnosti na temelju identificirane vrijednosti
- predviđanje vjerojatnog tijeka akcije
- predviđanje razine rizika (26).

Kad je riječ o identifikaciji vrijednosti, misli se na objekt napada koji za potencijalnog počinitelja predstavlja vrijednost ili neki od segmenata u poslovanju koji gospodarski subjekt percipira kao vrijednost te koji želi zaštititi od potencijalnih opasnosti. Prema Marku Cabricu (26) vrijednosti se dijele na primarne i sekundarne. Primarne su one od kojih ima koristi odmah (npr. proizvodi koji se mogu odmah koristiti ili lako prodati), dok sekundarne vrijednosti predstavljaju one koje trenutno nemaju vrijednost u tom obliku, ali se mogu dodati ili preraditi kako bi postale vrijedne.

Identifikacija opasnosti se bazira na privlačnosti i vrijednosti određenog zaštićenog dobra te se na temelju toga može i odrediti vrsta opasnosti koja prijeti. Kao primjer se mogu navesti dobra u malim količinama, primamljivija počiniteljima koji djeluju sami, dok su organizirane grupe fokusiranije na ono što je veće vrijednosti ili na ono za što je potrebno više ljudi kako bi se postigao željeni učinak.

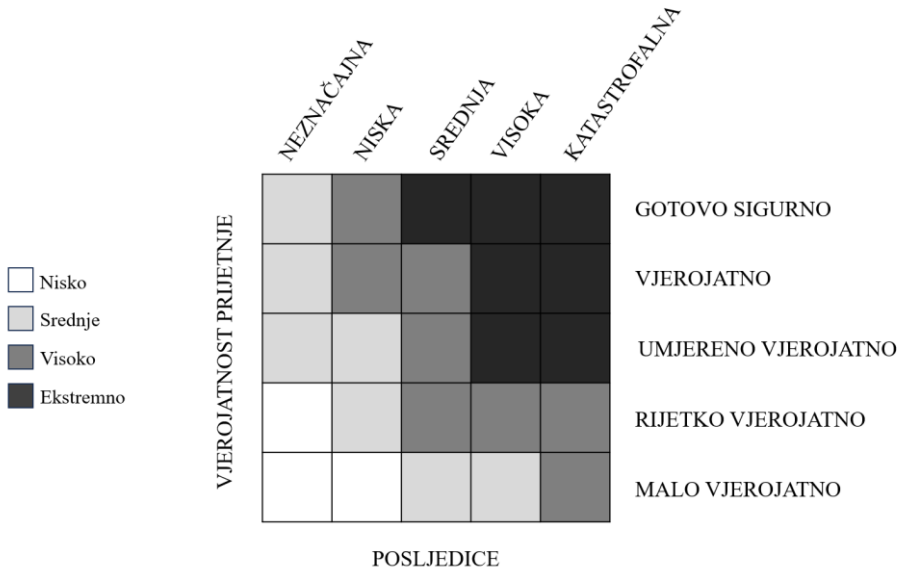
Predviđanje vjerojatnog tijeka akcije odnosi se na način kako određeno djelo može biti počinjeno, odnosno na predviđanje scenarija koji bi mogli predstavljati opasnosti za zaštićeno dobro.

Kao završni korak, vrši se predviđanje razine rizika za svaku utvrđenu opasnost. Potrebno je uzeti u obzir dva interaktivna elementa:

- vjerojatnost određene prijetnje – bazira se na prethodnim iskustvima, znanju i logici
- posljedice u najgorem slučaju – mjere se na temelju maksimalne moguće štete od određenog događaja (26).

Krmpotić (46) navodi kako se kao rezultat analize rizika može izraditi strategija za ublažavanje vjerojatnosti nekog rizika.

Razinu rizika je moguće prikazati i matricom kako bi bilo lakše razumljivo (Slika 1).

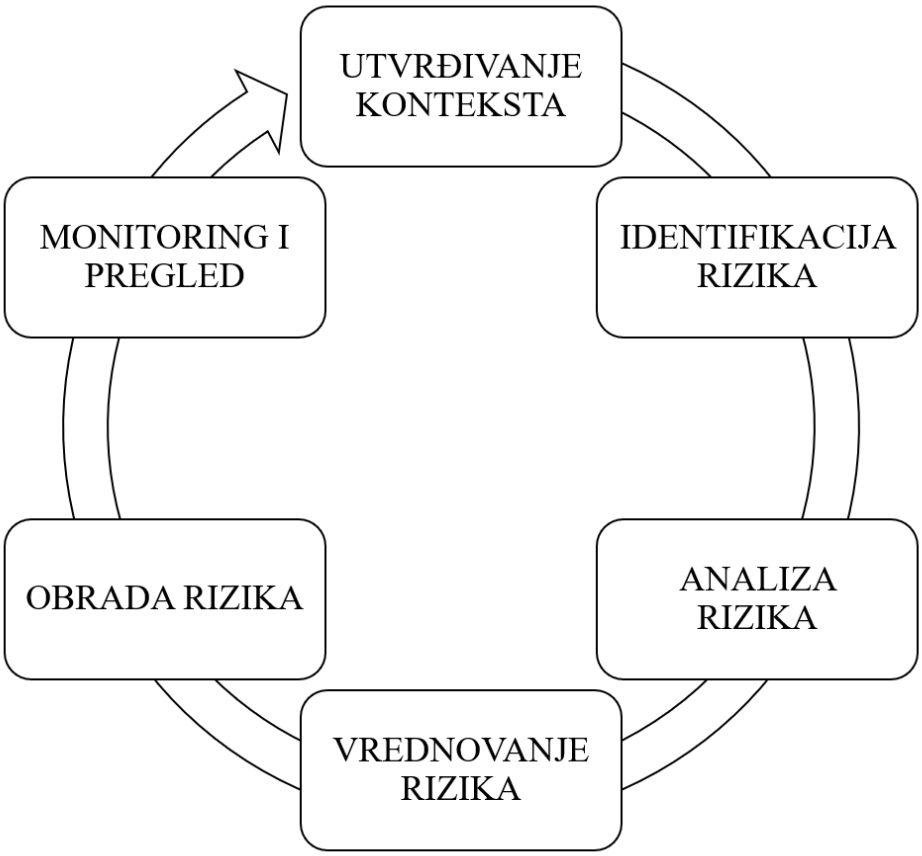


Slika 1. Matrica razine rizika

Izvor: (26)

Strateško planiranje sigurnosne strategije provodi se kroz pozicioniranje sigurnosti i analizu rizika. Pozicioniranje sigurnosti treba obuhvatiti ciljeve i poslovnu strategiju poslovanja te utvrditi resurse i imovinu subjekta, a sama sigurnost se treba uskladiti s upravljanjem rizicima. U svrhu boljeg upravljanja rizicima, donesen je međunarodni standard ISO 31000:2009 (engl. *Risk management – Guidelines on principles and implementation of risk management*) koji pruža smjernice za uspostavljanje i poboljšanje procesa upravljanja rizicima unutar organizacije. (15). Kod izrade procjene rizika, potrebno je identificirati rizike, analizirati ih, vrednovati i obraditi (15). Kad je riječ o identifikaciji rizika iz okoline, to uključuje ispitivanje svih rizika, vanjskih i unutarnjih, te ovom koraku treba posvetiti posebnu pažnju kako ne bi došlo do previđanja nekog potencijalnog rizika za koji poslije neće postojati način rješavanja. Tu spadaju rizici poput ekonomskih okolnosti, prirodnih pojava, ponašanja zaposlenika i suradnika, tehnoloških pitanja i sl. (15). Kod daljnje analize rizika dolazi do razdvajanja glavnih rizika od onih koji su nisu toliko bitni i koji nemaju toliki utjecaj na poslovanje, pri čemu se određuje i stupanj rizika (omjer vjerojatnosti i posljedica ako se rizik pojavi). Idući

korak koji je potrebno napraviti je vrednovati i rangirati rizike, nakon čega je moguće izraditi prioritetnu listu rizika. Prema prioritetnoj listi rizika se svaki rizik obrađuje za sebe te se definiraju postupci i planovi za odgovor na rizik implementacijom istih (15).



Slika 2. Shema procesa za upravljanje rizicima

Izvor: izradio autor prema Ivandić Vidović, Karlović, Ostojić (15)

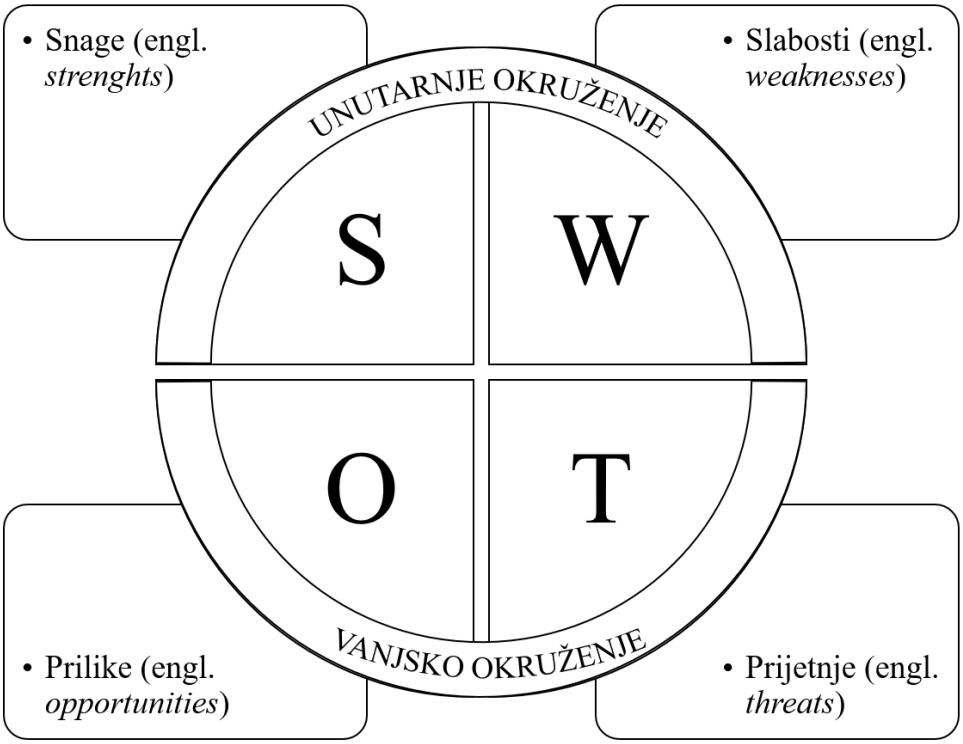
Međunarodna organizacija za normatizaciju je objavila ISO 31000:2018 (Upravljanje rizicima), što je novija verzija ISO 31000:2009 (47). ISO 31000:2018 (47) nudi smjernice za upravljanje rizicima, što pomaže organizaciji u postavljanju strategije, postizanju ciljeva i donošenju odluka. Smjernice su prilagodljive svim organizacijama jer pružaju univerzalni pristup upravljanja svim vrstama rizika, a isto tako se mogu primijeniti tijekom cijelog životnog ciklusa organizacije i na svim razinama donošenja odluka. Standardom su definirani pojmovi rizika, upravljanje rizikom (koordinirane aktivnosti za usmjeravanje i kontrolu organizacije u vezi s rizikom), sudionik (osoba ili organizacija koja može utjecati, biti pogođena ili sebe percipirati kao pogođenu odlukom ili aktivnošću), izvor rizika (element koji ima potencijal

izazvati rizik), događaj (pojava koja može imati više uzroka i posljedica), vjerojatnost (mogućnost da se nešto dogodi tijekom određenog razdoblja) i kontrola (mjere koje održavaju ili mijenjaju rizik, a uključuje procese, politike, uređaje, prakse i druge uvjete rada) (7). ISO 31000:2018 navodi načela za učinkovito i uspješno upravljanje rizicima, a koja predstavljaju temelj za uspostavljanje okvira i procesa upravljanja rizicima: „cjelovitost, strukturiranost i sveobuhvatnost, prilagodljivost, uključivost, dinamičnost, najbolja informiranost, ljudski i kulturni čimbenici te neprekidno poboljšavanje“ (47). Razvoj okvira upravljanja rizicima uključuje nekoliko elemenata:

- ovlaštenja i opredjeljenja – postavljanje jasnih ovlaštenja i obveza unutar organizacije
- integracija – integracija u sve poslovne procese i funkcije
- dizajniranje – kreiranje sustava koji odgovaraju organizaciji
- uspostavljanje – implementacija definiranih sustava i procesa upravljanja rizicima
- vrednovanje i poboljšavanje – redovito vrednovanje učinkovitosti upravljanja rizicima i njegovo kontinuirano poboljšavanje.

Strateško planiranje predstavlja ključ poslovne uspješnosti poslovnog subjekta (15). Za postizanje što uspješnijeg poslovanja, važno je pažljivo planirati i osmisliti kvalitetnu poslovnu strategiju. Poslovnu strategiju čini skup svih ostalih strategija i funkcija koje donose i obavljaju odjeli, kao što su strategije prodaje, upravljanja rizicima, upravljanja poslovnim procesima, sigurnosna strategija i strategija internih kontrola (15).

Korporativna sigurnost predstavlja stratešku funkciju, a samu strategiju korporativne sigurnosti treba razviti kroz faze strateškog planiranja, implementacije, kontrole i evaluacije sigurnosne strategije (15). U fazi strateškog planiranja izrađuje se analiza okruženja najčešće korištenjem metode SWOT analize (Slika 3.). Idući korak je procjena rizika, o kojoj je bilo riječi ranije u radu, nakon čega slijedi zadnji korak kontrole i vrednovanja sigurnosne strategije (15). Važnost kontrole i vrednovanja očituje se u mogućnosti strategije da identificirane rizike svede na prihvatljivu razinu i utvrdi je li došlo do promjena ili je li došlo do pojave novih rizika i sl. (15).



Slika 3. SWOT analiza

Izvor: autor

4.6.2. Analiza utjecaja na poslovanje

Poslovanje se sastoji od različitih sektora, odnosno poslovnih procesa koji čine cjelinu kako bi subjekt mogao nesmetano poslovati i obavljati svoje funkcije. Kako bi se što bolje odredilo na koje segmente poslovanja obratiti pažnju i bez kojih poslovanje ne bi bilo moguće, potrebno je izraditi analizu utjecaja na poslovanje. Kao primjer potrebe za analizom utjecaja na poslovanje može se navesti kako isti problem poslovanju ne predstavljaju pokvareni aparat za kavu i stroj za tiskanje u subjektu kojem je primarna djelatnost tiskanje knjiga.

Analiza utjecaja na poslovanje predstavlja kontinuirani proces koji identificira i procjenjuje moguće učinke prekida na ključne poslovne funkcije nastale zbog nesreće ili izvanredne situacije (46). Krmpotić (46) navodi kako nema formalnih standarda za analizu utjecaja, te kako iste mogu biti drugačije u pojedinom subjektu, a ističe sljedeće korake:

1. prikupljanje informacija najčešće na temelju upitnika
2. vrednovanje prikupljenih informacija

3. priprema izvješća s dokumentiranim nalazima s prioritetnim funkcijama
4. predstavljanje izvješća menadžmentu, koji izrađuje plan kontinuiteta poslovanja i strategiju za oporavak.

Cilj analize utjecaja na poslovanje je odrediti poslovne procese i sustave koji su potrebni za normalno djelovanje subjekta, kao i odrediti utjecaj pojedinog poslovnog procesa na financijski dio poslovanja subjekta. Analiza utjecaja na poslovanje također obuhvaća komponentu oporavka, vrijeme oporavka (engl. *Recovery time objective (RTO)*) (maksimalno dopušteno vrijeme u kojemu određeni poslovni proces ne funkcionira) i kontrolne točke ciljeva oporavka podataka (engl. *Recovery point objective (RPO)*) (najveća količina podataka koju gospodarski subjekt može izgubiti) (46, 48). Uz planiranje oporavka, o čemu će biti riječi kasnije, analiza utjecaja na poslovanje određuje prioritete i predlaže zahtjeve za resurse koji su neophodni, kao i vrijeme koje je potrebno.

Treba razlikovati analizu rizika od analize utjecaja na poslovanje. Analiza rizika se bavi identificiranjem potencijalnih opasnosti, načinima na koje može doći do neželjenog događaja i svrstavanjem, odnosno ocjenjivanjem rizika kroz vjerojatnost nastanka istog i kroz posljedice koje mogu nastati, dok se analiza utjecaja na poslovanje orijentira prema poslovnim funkcijama i sustavima i prema tome koje učinke na poslovanje, bilo financijske ili nefinancijske prirode, ima nastupanje nepoželjnog događaja.

4.6.3. Strategija kontinuiteta poslovanja

Strategija kontinuiteta poslovanja je temelj plana kontinuiteta poslovanja. Za izradu plana potrebno je imati strategiju, odnosno načine vođenja i rješavanje problema u svrhu postizanja ciljeva, kako bi se takvi strateški ciljevi implementirali u plan. Strategija kontinuiteta poslovanja usmjerava se prema određenim poslovnim funkcijama (49). Prema Fani i Subriadi (43), strategija kontinuiteta poslovanja sastoji se od određivanja preventivne strategije (engl. *Preventive Strategy Determination*), strategije za određene akcije (engl. *Determine strategies for actions*), strategije za oporavak (engl. *Recovery Strategy Determination*) i one koja će služiti za korekciju (engl. *Correction Strategy*).

Preventivna strategija bi bila ona koja se odnosi na načine vođenja prije nastanka neželjenog događaja i zapravo na pokušaje sprječavanja, odnosno izbjegavanja nastanka takvog rizika. Strategija za određene akcije bi se odnosila na znanja i vještine vođenja u situaciji kada nastane neželjeni događaj, te na što brže prebacivanje na strategiju za oporavak kako bi se osigurao

daljnji kontinuitet poslovanja gospodarskog subjekta. Također, potrebno je imati i strategiju koja će služiti za korekciju prije navedenih, kako bi se poboljšale i usavršile strategije.

4.6.4. Plan oporavka od katastrofe

Plan oporavka od katastrofe je zadnji u nizu od planova i analiza koje se rade unutar plana kontinuiteta poslovanja prema Cabricu i Rogersu (26). Nakon toga slijede aktivnosti povezane uz provjeru i unaprjeđenje plana. Ovaj plan je za upravljanje u hitnim situacijama, procesima i ljudima.

Plan oporavka od katastrofe osmišljen je za oporavak vitalnih poslovnih procesa nakon nepoželjnog događaja, odnosno katastrofe, unutar određenog vremenskog perioda za koji se želi da je što manji. Nakon osmišljavanja plana oporavka, nužno je u simuliranim uvjetima vidjeti kako funkcionira takav plan kako bi se isti mogao promijeniti u segmentima koji nisu dovoljno dobri i unaprijediti da bude što učinkovitiji.

Analiza utjecaja poslovanja je povezana s oporavkom od katastrofe jer planira oporavak od izvanrednog događaja tako da procjenjuje moguće troškove kvara i sl. (46). Najuspješnija strategija oporavka od katastrofe je ona koja se nikada neće ni implementirati/provoditi jer je ključan element u procesu oporavka od katastrofe upravo izbjegavanje iste (50).

4.7. Studija slučaja

Kad je u pitanju sigurnost gospodarskih subjekata, odnosno ranjivost istih, svakodnevno se mogu naći primjeri nekog oblika napada na segmente poslovanja. Razvojem tehnologije i važnosti očuvanja informacija, u posljednje vrijeme najčešće dolazi do različitih vrsta kibernetičkog napada.

Quader i P. Janeja (51) su 2021. godine izradili analizu koja je obuhvaćala 43 gospodarska objekta koji su bila meta kibernetičkog napada. U analizi su promatrali koji poslovni subjekt je doživio koju vrstu napada te kakve su bile posljedice i koji su mogući uzroci, tj. propusti zbog kojih je došlo do kompromitacije podataka (51). U analizu su uključeni veliki poslovni subjekti kao što su *Sony, Adobe, eBay*, Savezni istražni ured (engl. *Federal Bureau of Investigation*, FBI), razne baze, sveučilište, *Microsoft* i ostali (51). Najznačajniji zaključci istraživanja su bili:

- najčešći propusti su ljudski, odnosno nemar i neznanje zaposlenika
- glavne mete su financijske institucije, maloprodaja i industrija zabave, uz tehnologiju, zdravlje i energiju
- velik je utjecaj kibernetičkih napada na klijente i ugled poslovnog subjekta
- najveću opasnost za klijente predstavlja krađa biometrijskih podataka
- ključno je imati jaku politiku kibernetičke sigurnosti, ulagati u sigurnost i posvetiti se obuci zaposlenika (51).

Avio kompanije također predstavljaju metu hakera, a njihov prestanak rada može imati posljedice za cijeli svijet. Prema istraživanju Alohalia iz 2023. projicira se kako će u narednim godinama rasti cijene na tržištima za tehnologiju i informacijske sustave za avio kompanije (52). Također navodi probleme koji se mogu javiti u sektoru civilnog zrakoplovstva poput zrakoplovnih internet protokol mreža (engl. *internet protocol address*, IP), napada na operativne tehnologije (engl. *Operational Technologies*, OP) i sl., a kad je u pitanju broj napada na zrakoplovni sektor, malware napadi su narasli za 50% između listopada 2023. i siječnja 2024. godine (52). U 2020. godini bilo je 775 kibernetičkih napada na avio kompanije i 150 na zračne luke (52).

U ovom dijelu rada bit će prikazani slučajevi kibernetičkih napada na poslovne subjekte u Hrvatskoj i inozemstvu, kao i njihova postupanja u navedenim situacijama, te će se razmotriti što su potencijalno mogli drukčije napraviti kako bi se kvalitetnije pripremili, izbjegli napad ili bolje reagirali.

4.7.1. Zračna luka London City

Stranica Londonskog gradskog aerodroma je dana 28. svibnja 2023. godine bila pod napadom ruske hakerske grupe *NoName*. Pristup stranici je bio onemogućen te se pri pokušaju pristupanja stranici pojavljivala poruka greške. Službe su problem riješile u nekoliko sati, ali se podigla razina zabrinutosti jer je *NoName* organizacija bila poznata kao kibernetičko-teroristička organizacija (53, 54).

U vrijeme prije pada njihove stranice, *NoName* organizacija tvrdila je kako je ciljala stranice u Italiji, Škotskoj, Francuskoj i Velikoj Britaniji (53).

U slučaju ovog napada nije došlo do problema u radu zračne luke, a kako je navedeno, problem je saniran u kratkom vremenu. Glasnogovornik zračne luke je kazao kako je ujutro nakratko bio ograničen pristup stranici, ali da stranica radi te da njihov informatički tim radi na istrazi kako bi utvrdili što se dogodilo.

Kad je u pitanju reakcija službi zračne luke, brzo su riješili problem te su vratili stanje pod kontrolu. Hakerske napade teško je izbjeći zbog inovativnih metoda napadanja, kojih svakim danom ima sve više. U ovom slučaju došla je do izražaja reakcija djelatnika, koja je bila adekvatna, jer nije došlo do problema poslovanja zbog brzine saniranja štete. Ovaj primjer može sugerirati kako je zračna luka bila pripremljena te imala adekvatan plan što učiniti u slučaju takvog napada.

Sličan slučaj dogodio se i u Hrvatskoj, u Zračnoj luci Split.

4.7.2. Zračna luka Split

Dana 23. srpnja 2024. godine, Zračna luka Sveti Jeronim u Splitu bila je meta kibernetičkog napada. Zbog napada na sustav došlo je do kašnjenja i odgode letova. Ministar unutarnjih poslova izjavio je kako je bio slučaj o tzv. ucjenjivačkom softveru (engl. *ransomware*) kod kojeg napadači zaključavaju pristupljene podatke i traže neki oblik otkupnine, a najčešće riječ bude o novcu. U suradnji s Agencijom Europske unije za suradnju u provođenju zakona (EUROPOL), Saveznim istražnim uredom (FBI) i drugim službama, identificirana je skupina s euroazijskog područja. S počiniteljima se nije pregovaralo, već se kvar nastojao otkloniti na drugi način (55).

Sam ministar unutarnjih poslova je istaknuo kako bi se trebalo više ulagati u kibernetičku sigurnost (55). Bilo građani ili poslovni subjekti, bilo tko može biti meta kibernetičkog napada, no problem nastaje jer se često smatra kako će meta napada biti netko drugi. Predsjednik uprave

Zračne luke je rekao kako su, u dogovoru s drugim avio kompanijama, odlučili raditi kao nekad prije, preko liste putnika (56, 57).

Kako je ranije navedeno u radu, prevencija je ono na što bi se trebao staviti fokus, u ovom slučaju kroz konstantna ulaganja u kibernetičku sigurnost i edukaciju zaposlenika. Postojanje analize rizika i detaljno definiranje i predviđanje rizika neophodni su kako bi se mogla odrediti postupanja u slučaju nastupanja rizične situacije za poslovanje, a sve kako ne bi dolazilo do situacija sličnih ovoj u kojoj se našla zračna luka iz Splita. U radu je spominjan i plana oporavka od katastrofe kao bitan segment za najbrže moguće otklanjanje neželjene situacije kako ne bi dolazilo do prekida poslovanja, kao što je bio slučaj u Zračnoj luci Split s odgodom letova. Također, ranije spomenuta, analiza utjecaja na poslovanje može biti dobra motivacija poslovnim subjektima kako bi postali svjesniji gubitaka koji su mogući u slučajevima prestanka rada. U ovom slučaju nije samo riječ o financijskim gubicima, već i o onim koji se tiču povjerenja potrošača, pogotovo u slučajevima pristupa osobnim podacima, ali i o ugledu koji se promijenio kod putnika zbog odgode i čekanja.

4.7.3. Synnovis

Engleska organizacija za patološka istraživanja i obradu, Synnovis, bila je 3. lipnja 2024. godine žrtva kibernetičkog napada koji je imao velike posljedice za Nacionalnu zdravstvenu službu Engleske (engl. *the National Health Service* (*NHS*)) (58). U slučaju se radilo o *ransomware*-u, kao u slučaju splitske zračne luke, no tu su posljedice za zdravstvenu službu Engleske bile puno dugotrajnije. Prema izvješćima NHS-a, koja su izdavana svaki tjedan od napada, prikazani su brojevi slučajeva koji su se morali otkazati zbog poteškoća prouzrokovanih napadom. Napad je utjecao na rad nekoliko pružatelja zdravstvenih usluga u jugoistočnom Londonu, na način da su odgođene brojne operacije i pregledi pacijenata. Pružatelji usluga NHS su prema planu sigurnosne zaštite za ovakve slučajeve previdjeli pružanje uzajamne pomoći (58). Prema izvješću od dana 5. lipnja, NHS je rasporedio tim za odgovor na kibernetički napad kao podršku Synnovis-u i kako bi se što prije vratilo normalno funkcioniranje sustava. Dana 25. lipnja objavljeno je kako je zbog kibernetičkog napada odgođeno ukupno 1608 elektivnih zahvata te 8349 akutnih ambulantnih pregleda u samo dvije bolnice (59). U izvješću koje je objavljeno 8. kolovoza, vidljivo je da se potpuna obnova usluge transfuzije krvi planira za ranu jesen, a do tada je i dalje potreba uzajamna pomoć kako bi se smanjio utjecaj na pacijente. Također navode kako većina službi radi skoro pa normalno (60).

U slučaju je vidljivo kako je patološkoj službi trebalo više od dva mjeseca kako bi doveli situaciju pod kontrolu te ponovno mogli funkcionirati i pružati svoju uslugu za neophodnu djelatnost. Prema izvješćima, vidljivo je kako je postojao plan sigurnosne zaštite koji je pokrivao samo dio uzajamne pomoći, a tek je idući dan raspoređen tim za kibernetički napad. Kroz napad ovako velikih razmjera, iako je bio planiran kroz analizu rizika, vidljivo je kako je stručnjacima u području kibernetike potrebno iznimno puno vremena da oporave sustave kako bi bili funkcionalni. Potrebna su velika ulaganja u naprednije sustave obrane od kibernetičkih napada kako ne bi došlo do sličnih situacija u kojima je zbog sigurnosnog popusta velikom broju ljudi otkazan pregled, operacija, transplantacija i sl.

Napadi na zdravstvene sustave nisu novost jer zdravstvo predstavlja kritičnu infrastrukturu, koja je obvezna imati plan sigurnosne zaštite, koji je u ovom slučaju postojao, ali nije bio adekvatan. Kibernetički napad, ali manjih razmjera, usmjeren je bio i prema Kliničkom bolničkom centru u Zagrebu.

4.7.4. Klinički bolnički centar Zagreb – Rebro

Dana 27. lipnja 2024. godine došlo je do hakerskog napada na KBC Rebro, a zbog kojeg su djelatnici ugasili sustav bolnice kako ne bi došlo do veće štete za sustav ili podatke pacijenata. Prema izjavi pomoćnika ravnatelja za kvalitetu zdravstvene zaštite i nadzor, nije bilo pitanje hoće li se napad dogoditi, nego kada. Dakle, bili su svjesni mogućnosti dolaska do takvog slučaja te su izjavili kako su se na ovakvo nešto pripremali otprilike osam godina (61, 62). Dana 12. srpnja KBC Zagreb dao je priopćenje za javnost u kojem navodi kako na dan hakerskog napada nisu radili linearni akceleratori zbog sigurnosnih provjera, kako su idući dan u rad stavljena dva od pet, kako su se provodila hitna palijativna zračenja da pacijenti ne bi bili zakinuti za potrebna liječenja te kako su se pacijentima morali izrađivati novi planovi zračenja jer tri uređaja zbog sigurnosnih provjera nisu radila do 10. srpnja (63).

Što se tiče reakcije KBC-a, stručnjaci govore kako je odgovor na situaciju bio adekvatan te kako se dobro postupilo jer su u kratkom roku došle informatičke službe koje su radile na otklanjanju problema i dizanju sustava kako bi sve normalno funkcioniralo (64). Iz KBC-a su također zamolili pacijente da ne dolaze ako nemaju zaista hitan slučaj ili da, ako trebaju, odu u drugu bolnicu. Na taj se način dobro reagiralo i preusmjerilo pacijente kako bi im bila pružena adekvatna pomoć bez puno čekanja. Ministar zdravstva je uputio i ostale bolnice i bolničke sustave da provjere svoje informatičke sustave te da ih, ako je potrebno, nadograde kako bi se postigla bolja sigurnost (65), što u ovom slučaju za druge bolnice predstavlja preventivni

pristup ovakvom problemu. Iako su iz KBC-a bili pripremljeni na ovakvu vrstu napada, stopostotna sigurnost od kibernetičkih napada jednostavno nije moguća.

5. Zaključak

Poslovno okruženje suočeno je s brojnim izazovima, uključujući kibernetičke napade, fizičke prijetnje poput krađe ili vandalizma te organizacijske rizike, kao što su pronevjere ili curenje povjerljivih informacija. U tom kontekstu, ključno je razviti plan koji obuhvaća sve aspekte sigurnosti kako bi se minimizirali potencijalni gubici – plan sigurnosne zaštite gospodarskog subjekta. Razvojem svijesti o korporativnoj sigurnosti, došlo je do velikih pomaka u implementiranju sigurnosti u poslovno okruženje, kako je vidljivo kroz prikaz razvoja u radu.

Sigurnosna zaštita gospodarskog subjekta, neovisno o veličini istog, postiže se kroz sinergiju fizičke, tehničke i organizacijske zaštite. Jedan od ključnih elemenata u tom procesu je informacijska sigurnost, koja je danas usko povezana s kibernetičkom sigurnošću. S obzirom na to da u modernom poslovnom okruženju kibernetički napadi predstavljaju sve ozbiljniju prijetnju, prevencija i upravljanje istima postaju prioritet. U radu je kroz analizu studije slučaja jasno prikazano kako kibernetički napadi mogu nanijeti znatnu štetu gospodarskim subjektima, čime je potvrđena druga hipoteza (H2), koja tvrdi da takvi napadi imaju značajan negativan utjecaj na poslovanje. Rezultati pokazuju da je zaštita od kibernetičkih prijetnji ključna komponenta sveobuhvatne sigurnosne strategije, čime se dodatno naglašava važnost kontinuiranog praćenja i unaprjeđenja zaštitnih mjera.

Bilo bi poželjno da svi poslovni subjekti imaju razvijen plan sigurnosne zaštite. Međutim, kroz analizu istraživanja i razgovore sa stručnjacima koji su izradili veliki broj takvih planova, utvrđeno je da mnogi poslovni subjekti nemaju adekvatne sigurnosne planove, a neki ih uopće nemaju, čime je potvrđena prva hipoteza (H1). Ključni ciljevi sigurnosnog plana uključuju analizu rizika, izradu plana oporavka od katastrofe, obuku zaposlenika te redovito testiranje i ažuriranje plana kako bi se osigurala učinkovitost istog.

Proces procjene rizika ključan je za identificiranje specifičnih prijetnji s kojima se gospodarski subjekt može suočiti. Sama procjena rizika uključuje prikupljanje informacija o mogućim prijetnjama, analizu njihove vjerojatnosti i utjecaja te razvoj strategija za smanjenje rizika na prihvatljivu razinu. Također je istaknuta važnost uključivanja svih relevantnih sudionika unutar organizacije u proces planiranja i implementacije sigurnosnih mjera jer integrirani pristup povećava učinkovitost zaštite. Razlikuju se tri osnovne kategorije sigurnosnih mjera: tehničke, fizičke i organizacijske mjere. Tehničke mjere uključuju primjenu naprednih tehnologija za zaštitu informacija, poput enkripcije, firewall-a i antivirusnih sustava, dok fizičke mjere obuhvaćaju nadzor prostorija, kontrolu pristupa i zaštitu fizičke imovine. Organizacijske mjere

odnose se na definiranje sigurnosnih procedura, obuku zaposlenika i kreiranje sigurnosne kulture unutar organizacije.

Učinkovita sigurnosna zaštita je dinamičan proces koji zahtijeva stalno praćenje, evaluaciju i prilagodbu strategija u skladu s promjenama u poslovnom okruženju. Na temelju analize primjera iz prakse, pokazuje se da organizacije koje aktivno upravljaju svojim sigurnosnim rizicima, investiraju u modernizaciju svojih zaštitnih sustava te kombiniraju različite vrste mjera sigurnosti, koje pružaju višeslojnu zaštitu, imaju veću otpornost na incidente i brže se oporavljaju u slučaju kriznih situacija, čime je potvrđena i nulta hipoteza (H0) - da je sigurnosna zaštita od višestruke važnosti za gospodarski sustav.

Izrada plana sigurnosne zaštite predstavlja složen i kontinuiran proces koji ima mnogobrojne pozitivne učinke na poslovanje gospodarskog subjekta, ali i gospodarski sustav jer se smanjuje mogućnost financijskih gubitaka. Uvijek spominjani financijski gubici u nekim slučajevima nisu najgora posljedica koja je nastupila, ponekad je riječ i o ugledu gospodarskog subjekta, povjerenju potrošača, suradnika i sl. Ključ uspješne sigurnosne zaštite je integracija tehničkih, fizičkih i organizacijskih mjera unutar jedinstvenog sustava koji se kontinuirano prilagođava novim izazovima. Preporuka je da gospodarski subjekti ulažu u edukaciju zaposlenika, redovito ažuriraju sigurnosne politike i primjenjuju najnovije tehnologije kako bi bili korak ispred potencijalnih prijetnji. Osim toga, važno je razviti kulturu sigurnosti u organizaciji, gdje svaki zaposlenik prepoznaje svoju ulogu u održavanju sigurnosti te aktivno sudjeluje u unaprjeđenju iste.

6. Literatura

1. Nobilo M. Pojam sigurnosti u terminologiji međunarodnih odnosa. Politička misao: časopis za politologiju [Internet]. 1988. [citirano 25. lipnja 2024.]; 25(4). Dostupno na: https://hrcak.srce.hr/113633

2. Leksikografski zavod Miroslav Krleža. sigurnost. U: Hrvatska enciklopedija, mrežno izdanje [Internet]. 2021 [citirano 03. lipnja 2024.]. Dostupno na: https://www.enciklopedija.hr/Natuknica.aspx?ID=55892

3. Mihaljević B, Nađ I. Osnove korporativne sigurnosti. Hrvatska Udruga menadžera sigurnosti. Zagreb; 2018.

4. Martina Mihalinčić. Suvremena sigurnost, novi rizici i razvoj preventivnih modela kriznog upravljanja u Republici Hrvatskoj. Zagreb; 2020.

5. Tatalović S, Bilandžić M. Osnove nacionalne sigurnosti. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske; 2005.

6. Hrvatski jezični portal [Internet]. [citirano 03. lipnja 2024.]. rizik. Dostupno na: https://hjp.znanje.hr/index.php?show=search

7. ISO. ISO 31000:2018(en) Risk management — Guidelines [Internet]. 2018 [citirano 05. lipnja 2024.]. Dostupno na: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

8. Zakon o sigurnosnoj zaštiti pomorskih brodova i luka [Internet]. 2009 [citirano 05. lipnja 2024.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2009_10_124_3046.html

9. Zakon o javnoj nabavi [Internet]. 2023 [citirano 05. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/223/Zakon-o-javnoj-nabavi

10. Leksikografski zavod Miroslav Krleža. fizička osoba. U: Hrvatska enciklopedija, mrežno izdanje [Internet]. 2024 [citirano 05. lipnja 2024.]. Dostupno na: https://www.enciklopedija.hr/clanak/fizicka-osoba

11. Leksikografski zavod Miroslav Krleža. pravna osoba. U: Hrvatska enciklopedija, mrežno izdanje [Internet]. 2024 [citirano 05. lipnja 2024.]. Dostupno na: https://www.enciklopedija.hr/clanak/pravna-osoba

12. Barbić J. Osobe koje vode poslove kao odgovorne osobe i određenje predstavnika pravne osobe po Zakonu o odgovornosti pravnih osoba za kaznena djela. Hrvatski ljetopis za kazneno pravo i praksu [Internet]. 2003. [citirano 05. lipnja 2024.];10(2):779–842. Dostupno na: https://hrcak.srce.hr/87142

13. Leksikografski zavod Miroslav Krleža. korporacija. U: Hrvatska enciklopedija, mrežno izdanje [Internet]. 2021 [citirano 03. lipnja 2024.]. Dostupno na: https://www.enciklopedija.hr/natuknica.aspx?id=33256

14. Anthony McGee. 'Corporate Security's Professional Project: An examination of the modern condition of corporate security management and, the potential for further professionalisation of the occupation.' [Internet]. 2006 [citirano 04. lipnja 2024.]. Dostupno na: https://files.core.ac.uk/pdf/23/139759.pdf

15. Ivandić Vidović D, Karlović L, Ostojić A. Korporativna sigurnost. UHMS; 2011.

16. East Tennessee State University. Personal Safety [Internet]. [citirano 06. lipnja 2024.]. Dostupno na: https://www.etsu.edu/safety/personal_safety/

17. UCLA Police Department. Personal Safety Tips [Internet]. 2024 [citirano 06. lipnja 2024.]. Dostupno na: https://police.ucla.edu/prevention-education/personal-safety-tips

18. The Catholic University of America. Personal Safety Tips [Internet]. 2024 [citirano 06. lipnja 2024.]. Dostupno na: https://public-safety.catholic.edu/crime-prevention/personal-safety-tips.html

19. UNC Institutional integrity and risk management. Personal Safety [Internet]. [citirano 06. lipnja 2024.]. Dostupno na: https://campussafety.unc.edu/carolina-ready/take-action/personal-safety/

20. Wurtele SK, Saslawsky DA, Miller CL, Marrs SR, Britcher JC. Teaching personal safety skills for potential prevention of sexual abuse: A comparison of treatments. J Consult Clin Psychol. 1986.;54(5):688–92.

21. Zakon o informacijskoj sigurnosti [Internet]. 2024 [citirano 06. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti

22. Profozić M. Informacijska sigurnost u poslovanju [Internet]. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:128:078648

23. Pravilnik o uvjetima i načinu provedbe tehničke zaštite [Internet]. 2003 [citirano 06. lipnja 2024.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2003_12_198_3163.html

24. ECCOS. Mehanička zaštitna sredstva [Internet]. [citirano 06. lipnja 2024.]. Dostupno na: https://www.eccos.com.hr/tehnicka-zastita/mehanicka-zastitna-sredstva/

25. Zakon o privatnoj zaštiti [Internet]. 2023 [citirano 06. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/291/Zakon-o-privatnoj-za%C5%A1titi

26. Cabric M, Rogers M. Corporate security management : challenges, risks, and strategies. 2015.

27. Cerullo V, Cerullo MJ. Business continuity planning: A comprehensive approach. Information Systems Management. 2004.;21(3):70–8.

28. Kazneni zakon [Internet]. 2024 [citirano 07. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/98/Kazneni-zakon

29. Leksikografski zavod Miroslav Krleža. Hrvatska enciklopedija, mrežno izdanje. [citirano 09. lipnja 2024.]. vandalizam. Dostupno na: https://www.enciklopedija.hr/clanak/vandalizam

30. Mišković N. Tjelesna i tehnička zaštita na primjeru metaloprerađivačke tvrtke [Internet]. 2021. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:128:163021

31. Fajković I. Fizička i tehnička zaštita : za obrazovanje radnika fizičke i tehničke zaštite. Zagreb: Radničko i narodno sveučilište; 1986.

32. Zakon o zaštiti od požara [Internet]. 2023 [citirano 10. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/349/Zakon-o-za%C5%A1titi-od-po%C5%BEara

33. Pravilnik o razvrstavanju građevina, građevinskih dijelova i prostora u kategorije ugroženosti od požara [Internet]. 1994 [citirano 10. lipnja 2024.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/1994_08_62_1114.html

34. Zakon o zaštiti tajnosti podataka [Internet]. [citirano 11. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/748/Zakon-o-za%C5%A1titi-tajnosti-podataka

35. Zakon o tajnosti podataka [Internet]. 2007 [citirano 11. lipnja 2024.]. Dostupno na: https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka

36. Peran B, Goreta M, Vukošić K. Pojam i vrste tajni. Zbornik radova Veleučilišta u Šibeniku [Internet]. 2015. [citirano 11. lipnja 2024.];9(3–4). Dostupno na: https://hrcak.srce.hr/149944

37. Sigurnosno–obavještajna agencija. Kibernetička sigurnost [Internet]. [citirano 11. lipnja 2024.]. Dostupno na: https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/

38. Središnji državni ured za razvoj digitalnog društva. Kibernetička sigurnost [Internet]. [citirano 11. lipanj 2024.]. Dostupno na: https://rdd.gov.hr/kiberneticka-sigurnost/1436?lang

39. O sustavu SK@UT [Internet]. [citirano 11. lipnja 2024.]. Dostupno na: https://www.skaut.hr/#odluka

40. Službeni list Europske unije [Internet]. 2021 [citirano 11. lipnja 2024.]. Uredba (EU) 2019/881 Europskog parlamenta i Vijeća. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32019R0881

41. Zavod za informatičku djelatnost Hrvatske d.o.o. Upravljanje kibernetičkom sigurnošću [Internet]. 2022 [citirano 11. lipnja 2024.]. Dostupno na: https://zih.hr/konzalting/informacijska-sigurnost-i-kontinuitet-poslovanja/upravljanje-kibernetickom-sigurnoscu/

42. Benyoucef M, Forzley S. Business Continuity Planning and Supply Chain Management. Supply Chain Forum: An International Journal. siječanj 2007.;8(2):14–22.

43. Fani SV, Subriadi AP. Business continuity plan: Examining of multi-usable framework. U: Procedia Computer Science. Elsevier B.V.; 2019. str. 275–82.

44. Svijet kvalitete. PDCA krug (Demingov krug) [Internet]. [citirano 12. lipnja 2024.]. Dostupno na: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug

45. Ready. Risk Assessment [Internet]. [citirano 12. lipnja 2024.]. Dostupno na: https://www.ready.gov/business/planning/risk-assessment

46. Krmpotić G. Business Impact Analysis (BIA) ili Analiza utjecaja na poslovanje. 2019.

47. Svijet kvalitete. Upravljanje rizicima prema HRN ISO 31000:2018 [Internet]. [citirano 13. lipnja 2024.]. Dostupno na: https://www.svijet-kvalitete.com/index.php/normizacija/4106-upravljanje-rizicima-prema-hrn-iso-31000-2018

48. Šoštarić D. Upravljanje kontinuitetom poslovanja [Internet]. [citirano 10. lipnja 2024.]. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:122:708568

49. Kerla M. Implementacija BCP-a: CASES. Sarajevo; 2024.

50. Jorrigala V. Business Continuity and Disaster Recovery Plan for Information Security. 2017.

51. Quader F, Janeja VP. Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. Sv. 1, Journal of Cybersecurity and Privacy. Multidisciplinary Digital Publishing Institute (MDPI); 2021. str. 638–59.

52. Bashar Ahmed Alohali. Aviation Cybersecurity National Governance [Internet]. 2023 [citirano 07. kolovoza 2024.]. Dostupno na: https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/2.2%20Saudi%20Arabia%20-%20Aviation%20Cybersecurity%20National%20Governance.pdf

53. Simple Flying. Investigation Launched After London City Airport Website Hacked [Internet]. 2023 [citirano 07. kolovoza 2024.]. Dostupno na: https://simpleflying.com/investigation-launched-london-city-airport-website-hacked/

54. britishaviationgroup. Investigation Launched After London City Airport Website Hacked [Internet]. 2023 [citirano 07. kolovoza 2024.]. Dostupno na: https://www.britishaviationgroup.co.uk/knowledge/investigation-launched-after-london-city-airport-website-hacked/

55. Vlada Republike Hrvatske. Hakerski napad na zračnu luku je slučaj ransomwarea [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://vlada.gov.hr/vijesti/hakerski-napad-na-zracnu-luku-je-slucaj-ransomwarea/42774

56. Lider. IT stručnjaci: Do napada na splitski aerodrom ne bi došlo da je bilo osnovne sigurnosne kontrole [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://lidermedia.hr/tvrtke-i-trzista/it-strucnjaci-do-napada-na-splitski-aerodrom-ne-bi-doslo-da-je-bilo-osnovne-sigurnosne-kontrole-158243

57. Dnevnik.hr. Ministar Božinović komentirao hakerski napad na splitsku zračnu luku [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://dnevnik.hr/video/ministar-bozinovic-komentirao-hakerski-napad-na-splitsku-zracnu-luku---62870108

58. NHS England — London. NHS London statement on Synnovis ransomware cyber attack – Tuesday 4 June 2024 [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://www.england.nhs.uk/london/2024/06/04/nhs-london-statement-on-synnovis-ransomware-cyber-attack/

59. NHS England — London. Update on cyber incident: Clinical impact in south east London – Thursday 25 July [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://www.england.nhs.uk/london/2024/07/25/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-25-july/

60. NHS England — London. Update on cyber incident: Clinical impact in south east London – Thursday 8 August [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://www.england.nhs.uk/london/2024/08/08/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-8-august/

61. Dnevnik.hr. KBC Zagreb i dalje pod opsadom, iz bolnice poručuju: „Podaci pacijenata nisu došli u krive ruke“ [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://dnevnik.hr/vijesti/hrvatska/sustav-kbc-a-zagreb-jos-ne-funkcionira-dio-pacijenata-mozda-ce-seliti-u-druge-bolnice---856107.html

62. Dnevnik.hr. Novi detalji s Rebra nakon napada hakera: „Nitko neće biti poslan doma. Nije došlo do curenja podataka pacijenata“ [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://dnevnik.hr/vijesti/hrvatska/kbc-rebro-na-meti-hakera-iz-bolnice-objavili-kakva-je-situacija---855976.html

63. KBC Zagreb. Nastavljeni protokoli zračenja u KBC-u Zagreb [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://www.kbc-zagreb.hr/nastavljeni-protokoli-zracenja-u-kbc-u-zagreb.aspx

64. RTL danas. [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://d20lr2ntorbqvd.cloudfront.net/ea7a6b12-355b-11ef-977c-72780b90502a/original

65. Dnevnik.hr. Beroš pozvao bolnice da provjere svoje sustave: Omogućena je i nadogradnja [Internet]. 2024 [citirano 08. kolovoza 2024.]. Dostupno na: https://dnevnik.hr/vijesti/hrvatska/beros-bolnicama-provjerite-sigurnosni-status-informatickih-sustava---856276.html

7. Sažetak

SIGURNOSNA ZAŠTITA GOSPODARSKOG SUBJEKTA

U ovom radu naglašava se ključna uloga izrade plana sigurnosne zaštite za gospodarske subjekte, koji značajno utječe na kontinuitet i uspješnost poslovnih procesa i funkcija. Rad se u prvom dijelu fokusira na razumijevanje osnovnih pojmova sigurnosne zaštite, uključujući fizičku, tehničku i mehaničku zaštitu. Fizička zaštita odnosi se na fizičke barijere i nadzor prostora, tehnička zaštita uključuje tehnologije poput enkripcije i vatrozida, dok mehanička zaštita obuhvaća sigurnosne sustave kao što su zaključavanje i alarmni sustavi.

Analiza u radu pokazuje da je za učinkovitu sigurnost nužno uspostaviti i implementirati detaljan plan sigurnosne zaštite. Ovaj plan uključuje analizu rizika i razvoj dodatnih planova i strategija za upravljanje prijetnjama. Iako izrada plana sigurnosne zaštite i analiza rizika nisu zakonski obavezni za sve gospodarske subjekte, oni su ključni dokumenti koji pomažu gospodarskim subjektima u identifikaciji potencijalnih prijetnji i razvoju učinkovitih strategija za njihovo upravljanje.

Studija slučaja kibernetičkih napada u Republici Hrvatskoj i svijetu ističe ozbiljnost prijetnji koje takvi napadi mogu predstavljati za poslovne sustave, kao i posljedice napada. Ova studija naglašava važnost adekvatne prevencije i razvoja plana oporavka od kibernetičkih napada, koji su sve češći. Implementacija preventivnih mjera i planova oporavka ključna je za minimiziranje štete i osiguranje otpornosti poslovnih procesa i funkcija na nepredviđene incidente, čime se povećava sigurnost i stabilnost poslovanja.

Ključne riječi: *sigurnosna zaštita, gospodarski subjekt, plan sigurnosne zaštite, analiza rizika, plan oporavka od katastrofe*

8. Summary

SECURITY PROTECTION OF THE ECONOMIC ENTITY

This paper emphasizes the key role of creating a security protection plan for business entities, which significantly affects the continuity and success of business processes and functions. In the first part, the paper focuses on understanding the basic concepts of security protection, including physical, technical and mechanical protection. Physical protection refers to physical barriers and space surveillance, technical protection includes technologies such as encryption and firewalls, while mechanical protection includes security systems such as locking and alarm systems.

The analysis in the paper shows that for effective security it is necessary to establish and implement a detailed security protection plan. This plan includes risk analysis and the development of additional plans and a threat management strategy. Although the creation of a security protection plan and risk analysis are not legally mandatory for all economic entities, they are key documents that help economic entities identify potential threats and develop effective strategies for their management.

The case study of cyber-attacks in the Republic of Croatia and the world highlights the seriousness of the threats that such attacks can represent for business systems, as well as the consequences. This study highlights the importance of adequate prevention and development of a recovery plan from cyberattacks that are becoming more common. The implementation of preventive measures and recovery plans is essential for minimizing damage and ensuring the resilience of business processes and functions to unforeseen incidents, thereby increasing business security and stability.

***Keywords**: security protection, business entity, security protection plan, risk analysis, disaster recovery plan*

9. Životopis

Osobni podaci:

Ime i prezime:	Elena Leško
Adresa:	Novo brdo 33b, Husain, 44320 Kutina, Hrvatska
Mobitel:	+358 99 591 1003
e-mail:	elenalesko@gmail.com
Datum i mjesto rođenja:	03.11.1999., Zagreb, Hrvatska
Vozačka dozvola:	B kategorija
Strani jezik:	Engleski jezik

Obrazovanje:

2014.-2018. Srednja škola Tina Ujevića, Kutina (ekonomistica)

2018.-2021. Stručni studij kriminalistike, Zagreb, prvostupnica kriminalistike (bacc. crim.)

2022.-2024. Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti – Diplomski studij forenzike, modul Forenzika i nacionalna sigurnost

Iskustva:

Nakon završetka preddiplomskog stručnog studija, zaposlila sam se u maloprodajnoj trgovini u Kutini, „Pinky“, gdje sam radila 6 mjeseci kao prodavačica do upisa na diplomski studij. U sklopu studija na Sveučilišnom odjelu za forenzične znanosti, sudjelovala sam na događajima „*13th ISABS Conference on Applied Genetics and Mayo Clinic Lectures in Translational Medicine*“, „*International scientific-expert Maritime security Conference 2023*“, te na događaju u organizaciji RACVIAC-a, „*Course of Non-proliferation and Disarmament law*“.

Vještine:

Dobre komunikacijske vještine stečene tijekom školovanja, dobro funkcioniranje pod pritiskom, spremna preuzeti odgovornost, sklonost timskom radu, strpljivost, snalažljivost

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, **Elena Leško**, izjavljujem da je moj diplomski rad pod naslovom **Sigurnosna zaštita gospodarskog subjekta** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ničija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u nijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 23. rujna 2024.

Potpis studenta/studentice: 

Popis slika