

VIŠJA STROKOVNA ŠOLA ACADEMIA
MARIBOR

VARNOSTNI SISTEMI V FINANČNIH INSTITUCIJAH

Kandidatka: Nika Lamut

Vrsta študija: študentka izrednega študija

Študijski program: varovanje

Mentor predavatelj: Jakob Demšar, univ. dipl. prav.

Mentor v podjetju: Marko Golež

Lektorica: dr. Petra Kunc, prof. slov.

Selnica ob Dravi, 2022

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Nika Lamut sem avtorica diplomskega dela z naslovom Varnostni sistemi v finančnih institucijah, ki sem ga napisala pod mentorstvom Jakoba Demšarja, univ. dipl. prav.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel/a, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Selnica ob Dravi, maj 2022

Podpis študenta:

ZAHVALA

Specifičnost teme, zaupnost podatkov in težje pridobivanje relevantnih virov je bila stalnica pri pripravi in izdelavi mojega diplomskega dela. Tudi zaradi tega mi je bila med pisanjem diplomske naloge zelo dobrodošla in bistvena velika podpora ter pomoč, ki mi je bila nudena, za kar se iskreno zahvaljujem.

Posebej bi se rada zahvalila svojemu mentorju Jakobu Demšarju, ki me je ob izbrani temi pravilno usmerjal do uspešnega zaključka.

Zahvaljujem se Zdravku Podgorniku, Denisu Podgorniku ter Marku Goležu iz podjetja Protect infra, d. o. o., ki so me ob izvajanju praktičnega usposabljanja vodili tudi po neizhojenih poteh zasebnega varovanja v Republiki Sloveniji, mi odpirali oči in omogočili poglede na zasebno varovanje skozi realno izvedbo nalog.

Posebej se zahvaljujem Miranu Vačovniku, ki mi je nudil pomoč pri pridobivanju strokovne literature, ki predstavlja temelj varnostnih ukrepov v bankah in hranilnicah, s katerimi se zagotavlja neprekinjeno in varno okolje finančnega poslovanja v bankah in hranilnicah. Brez njegove pomoči diplomsko delo ne bi imelo takšne vsebine.

Iskrena hvala tudi Đaniju Begiču iz banke Intesa Sanpaolo Bank, d. d, za svoj prispevek k vsebinskemu delu moje diplomske naloge z opravljenim intervjujem.

Zahvaljujem se družini za potrpljenje in spodbudo, še posebej očetu, ki mi je podal koristne informacije in poskrbel za spodbudne razprave.

Zahvaljujem se prijateljici Kristini Mlakar za vso nudeno pomoč in podporo.

POVZETEK

Sodobne demokratične države vse bolj prepuščajo nekatere segmente družbene varnosti zasebnim varnostnim družbam, ki ponujajo storitve varovanja oseb in premoženja. S tem namenom so zasebne varnostne družbe zakonsko predvidene tudi pri varovanju finančnih institucij. Za zakonito in strokovno ter učinkovito izvedbo nalog je zakonodajalec podelil posebna pooblastila varnostnikom in predpisal pogoje, ki jih morajo zasebne varnostne družbe izpolnjevati, da bi lahko prevzemali naloge varovanja ljudi in premoženja. Zakonodajalec je med področja, na katerih je obvezno izvajati organizirano varnostno službo po zasebnih družbah, uvrstil tudi del tako imenovane kritične infrastrukture. Finančne institucije, kot so banke, hranilnice ter pošte, prav tako spadajo pod kritično infrastrukturo. Varovanje finančnih institucij v Republiki Sloveniji je z zakoni in podzakonskimi akti prepuščeno v izvajanje zasebnim varnostnim družbam. Posledično je bilo treba nujno podeliti pooblastila varnostnemu osebju in zagotoviti strokovno usposabljanje za varnostni management, da lahko zasebna varnostna družba zakonito in uspešno ukrepa ob tveganih dogodkih. Sistemi varovanja finančnih institucij obsegajo fizično varovanje in tehnično varovanje. Skupaj tvorijo varovanje, ki zagotavlja neprekinjeno poslovanje v objektih in po spletnem bančništvu. Razvoj IT, prenos poslovanja na splet ter uporaba negotovinskih plačilnih sredstev imajo za posledico, da se vse več varnostnih tveganj odvija v teh okoljih, zato je tako za finančno institucijo kot tudi za uporabnika bistveno večje tveganje pri poslovanju po spletu. V finančnih institucijah se osnova varnostnega sistema vzpostavlja že ob načrtovanju gradnje in se nato dopolnjuje in nadgrajuje v celovito varnostno rešitev, ki bistveno omejuje varnostna tveganja. Pri izvajanju poslovanja finančnih institucij in njihovih uporabnikov po spletu pa je treba varnostni sistem nenehno nadgrajevati in v realnem času odkriti vedno nova varnostna tveganja, jih omejiti pri vstopu in preprečiti negativno delovanje v bančnem sistemu. Trenutno so največjemu varnostnemu tveganju izpostavljeni uporabniki spletnega bančništva, predvsem iz razloga opuščanja varnostnih ukrepov, kar ima lahko negativne posledice tudi za finančno institucijo. Razlog je verjetno v tem, da v 21. stoletju uporabnik lahko spletno bančništvo uporablja ne samo po stacionarnem in prenosnem računalniku, temveč z uporabo mobilnih telefonov, ki so zaradi delovanja različnih aplikacij zelo izpostavljeni delovanju računalniških kriminalcev – t. i. »računalniškimi hekerjem«, ki izkoriščajo nezakonito pridobljene podatke za pridobivanje premoženjske koristi.

Ključne besede: finančne institucije, varnostni management, varovanje, varnostna tveganja in varnostno osebje

ABSTRACT

"SECURITY SYSTEMS IN FINANCIAL INSTITUTIONS"

Private companies in modern democracies are increasingly leaving certain segments of social security to private security companies, which offer protection services for people and properties. These private security companies are legally required to protect financial institutions. For legal, professional, and efficient performance of tasks, the legislator grants special powers to security guards and prescribes the licenses that private security companies must meet to protect people and properties. Amongst the areas in which it's obligatory to provide an organized security service by private companies, the legislator also included certain critical infrastructures. Financial institutions, banks, and post offices are also a part of the critical infrastructure. In the Republic of Slovenia, the protection of such institutions is left to private security companies through laws and regulations. As such, it's essential to empower the security staff and provide professional training in security management. The security company can take effective legal actions in events of risky events. Physical and technical security is included in the security systems of financial institutions, which are implemented by several internal and external contractors. They ensure uninterrupted operations in branches and ATMs as well as online banking. More and more security risks take place in these online environments, because of the shifts towards online business, and the use of non-cash payments. There is a significantly higher risk for online financial institutions and users when doing online business. In financial institutions, the basis of the security system is established at the time of construction planning and then supplemented and upgraded into a comprehensive security solution, which significantly limits security risks. When conducting operations of financial institutions and their users online, the security system must be constantly upgraded and new security risks must be detected in real-time. Upon entry, they must be limited and negative operations in the banking system must be prevented. Due to the abandonment of security measures, the users of online banking are currently the greatest security risk, which can have negative consequences for the financial institution. In the 21st century, the user can use online banking from multiple devices such as desktops, laptops, and mobile phones. Due to the different ways the applications operate, they are very exposed to computer criminals (hackers), who exploit and illegally obtain data for material gain.

Key words: financial institutions, security management, security, security risks and security staff

KAZALO VSEBINE

1	UVOD	9
1.1	Opis področja in opredelitev problema.....	10
1.2	Namen, cilji in osnovne trditve.....	11
1.3	Predpostavke in omejitve	11
1.4	Uporabljene raziskovalne metode.....	12
2	SLOVAR POJMOV	13
3	FINANČNE INSTITUCIJE V REPUBLIKI SLOVENIJI.....	16
3.1	Banka Slovenije	16
3.1.1	Naloge Banke Slovenije	16
3.1.2	Ključna področja delovanja in naloge Banke Slovenije	18
3.1.3	Vizija Banke Slovenije.....	19
3.1.4	Cilji Banke Slovenije.....	20
4	PRAVNA UREDITEV PODROČJA VAROVANJA FINANČNIH INSTITUCIJ. 21	
4.1	Zakoni in podzakonski akti.....	21
4.1.1	Zakon o Banki Slovenije	21
4.1.2	Zakon o bančništvu	21
4.1.3	Zakon o gospodarskih družbah.....	22
4.1.4	Basel II	22
4.1.5	Uredba o varovanju tajnih podatkov	22
4.1.6	Zakon o varstvu osebnih podatkov.....	22
4.1.7	Zakon o varstvu pred požarom	22
4.1.8	Pravilnik o požarnem varovanju.....	23
4.1.9	Pravilnik o študiji požarne varnosti	23
4.1.10	Zakon o zasebnem varovanju	24
4.1.11	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih	24
4.1.12	Pravilnik o načinu prevoza in varovanja denarja ter drugih vrednostnih pošiljk.....	25
4.1.13	Zakon o varnosti in zdravju pri delu.....	25
5	IZVEDBA VAROVANJA FINANČNIH INTITUCIJ PO ZASEBNI VANOSTNI DRUŽBI.....	26

5.1 Načrt varovanja.....	26
5.1.1 Ocena stopnje tveganja.....	26
5.1.2 Program varovanja	27
5.1.3 Načrt varovanja za finančne institucije	27
5.1.4 Načrt fizičnega varovanja.....	28
5.2 Tehnično varovanje.....	28
5.2.1 Tehnično varovanje v finančnih institucijah	29
5.2.2 Mehanska zaščita.....	29
5.2.3 Gradbeno-tehnična priporočila.....	30
5.2.4 Sistemi požarnega varovanja.....	30
5.2.5 Sistemi tehnične zaščite za zaznavo razlitja tekočin ali uhajanja plinov	31
5.2.6 Sistemi za zaznavanje in javljanje vloma ali ropa in klica v sili	32
5.2.7 Sistemi pristopne kontrole.....	32
5.2.8 Sistem za prenos alarmnih signalov	32
5.2.9 Videonadzorni sistem	33
5.2.10 Varnostno-nadzorni centri	33
5.3 Fizično varovanje	33
5.3.1 Prevoz in prenos gotovine ter vrednostnih pošilk	34
5.4 Sodelovanje z varnostnimi službami in policijo	36
5.4.1 Sodelovanje z varnostnimi službami	36
5.4.2 Obveščanje in sodelovanje s policijo.....	37
5.4.3 Sodelovanje z drugimi institucijami	38
 6 PRIMERI IZVEDBE NAPADOV NA VARNOSTNE SISTEME V FINANČNIH ISTITUCIJAH Z UPORABO IT.....	 39
6.1 Delovanje storilcev z uporabo črnega spleta.....	39
6.2 Izvrševanje spletnih goljufij	40
 7 NAJODMEVNEJŠI PRIMERI NAPADOV NA FINANČNE INSTITUCIJE IN VARNOSTNO OSEBJE PRI PREVOZU GOTOVINE	 42
7.1 Rop SKB – bančni sefi in trezorji.....	42
7.2 Izvršitev devetih ropov finančnih institucij na območju Slovenije s strani srbske kriminalne združbe 43	
7.3 Izvršitev štirih ropov finančnih institucij s strani enega storilca ob uporabi pištole in kolesa z motorjem	43
7.4 Izvršitev ropa vozila za prevoz denarja zasebne varnostne družbe	44

7.5	Izvršitev dveh ropov poslovalnice Pošte z uporabo strelnega orožja in smrtjo uslužbenke Pošte	45
8	STATISTIKA KAZNIVIH DEJANJ, POVEZANIH Z NAPADI NA FINANČNE USTANOVE IN DENAR.....	46
9	SKLEP.....	51
10	VIRI IN LITERATURA.....	54
11	PRILOGE.....	6
11.1	Priloga 1: Intervju – Dani Begić, vodja službe varnosti Intesa Sanpaolo Bank	6

KAZALO SLIK

Slika 1: Področja delovanja in naloge Banke Slovenije 1	18
Slika 2: Področja delovanja in naloge Banke Slovenije 2	19

KAZALO TABEL

Tabela 1: Kazniva dejanja rop, roparske tatvine in velike tatvine na prizoriščih bank (bankomati), hranilnice in pošte.....	46
Tabela 2 : Kazniva dejanja uporaba ponarejenega negotovinskega plačilnega sredstva	47
Tabela 3: Primerjava števila kaznivih dejanj, kjer je predmet napada objekt bank ali hranilnic ter pošt, s številom, kjer je sredstvo storitve kaznivega dejanja spletno bančništvo	48
Tabela 4: Primerjava petletnega obdobja kaznivih dejanj, kjer je predmet napada finančna institucija ali spletno bančništvo	49

KAZALO GRAFIKONOV

Graf 1: Kazniva dejanja rop, roparske tatvine in velike tatvine na prizoriščih bank (bankomati), hranilnice in pošte.....	47
Graf 2: Kazniva dejanja uporabe ponarejenega negotovinskega plačilnega sredstva.....	48
Graf 3: Primerjava petletnega obdobja kaznivih dejanj, kjer je predmet napada finančna institucija ali spletno bančništvo	49
Graf 4 : Primerjava petletnega obdobja kaznivih dejanj, kjer je predmet napada finančna institucija ali spletno bančništvo	50

1 UVOD

V diplomskem delu bom predstavila varovanje v finančnih institucijah, kakršnega trenutno poznamo na območju Republike Slovenije (RS). Izbran izraz finančne institucije je posledica dejstva, da je to izraz, ki ga je uporabil zakonodajalec in z njim zakonsko obvezal različno poimenovane družbe (banke in hranilnice), katerim je med ostalim skupno tudi to, da imajo za izvedbo svoje dejavnosti dovoljenje Banke Slovenije, ki je regulator bančnega sistema v Sloveniji, med katerega spadajo tudi hranilnice. Zaradi dostopnosti bančnih storitev na območju celotne Slovenije se bančne storitve opravljajo tudi na poslovalnicah Pošte Slovenije.

Varovanje v finančnih institucijah je zaradi posebnega statusa le-teh zakonsko urejeno, kompleksno in zahtevno, tako za izvajalce in upravljalce varnostnih sistemov kot tudi za neposredne uporabnike varnostnih sistemov. Varovanje v finančnih institucijah je naloga, ki se opravlja konstantno in se vodi na različnih nivojih in s strani različnih, posebej za to usposobljenih kadrov in zato skupek vseh udeleženih poimenujemo varnostni sistem. Vsi varnostni sistemi morajo delovati najprej neodvisno eden od drugega in skupaj nudijo najboljšo možno zaščito pred morebitnimi varnostno obremenjujočimi dejanji. Izpostavljenost finančnih institucij je s tem najmanjša in odzivanje na varnostna tveganja najhitrejše. Zaradi razumljivosti in preglednosti bom predstavila s tem povezano zakonodajo glede izvedbe varovanja.

Izgradnja celotnega varnostnega sistema v finančni instituciji se začne s pripravo varnostnega načrta kot prvi korak k zagotavljanju varnosti. Varnostni sistemi zaradi specifičnosti in kompleksnosti vključujejo subjekte, ki niso del finančne institucije v smislu organizacijske strukture, zato je njihovo delovanje neizogibno povezano z delovanjem t. i. notranjega varnostnega sistema, kar bo predmet obravnave v diplomskem delu. Prav tako bo predmet obravnave izpostavljenost finančne institucije v elektronskem delovanju, še posebej v okviru poslovanja po internetu. Podrobno bom predstavila sisteme varovanja v finančni instituciji, pri čemer bom poskusila z raziskovalno metodo pridobiti dovolj kakovostnih podatkov tudi za ponazoritev informacijskih varnostnih rešitev. Informacijske varnostne rešitve so namreč v času nenehnega razvoja informacijske tehnologije izredno varovan podatek, saj ima lahko napad na informacijski varnostni sistem finančne institucije nepopravljivo premoženjsko škodo. Prav gotovo imamo svojo vlogo pri delovanju varnostnega sistema po spletnem delovanju finančne institucije tudi uporabniki, posebej s svojim premišljenim in priporočenim ravnanjem. S poglobljeno obravnavo zastavljenih vprašanj glede varnostnih sistemov v finančnih institucijah

bom potrjevala postavljene hipoteze oziroma trditve in v največji možni meri usvojila poznavanje metod in tehnik varovanja finančnih institucij v povezavi s pravočasnim predvidevanjem možnih varnostnih tveganj pri izvedbi varovanja kot celote. Za potrjevanje trditve bom uporabila tudi javno objavljene statistične podatke slovenske policije glede obravnavanih kaznivih dejanj, kjer je predmet napada finančna institucija v kateri koli obliki. V diplomskem delu se bom dotaknila tudi medijsko najodmevnejših primerov napadov na finančne institucije in s tem povezanimi varnostnimi sistemi, kar bo prav tako predmet potrjevanja postavljenih hipotez diplomskega dela.

1.1 *Opis področja in opredelitev problema*

Področje raziskovanja bo delovanje varnostnih sistemov v povezavi z delovanjem zasebnih varnostnih družb v slovenskih bankah in hranilnicah, ki je urejeno z zakonskimi, podzakonskimi in internimi predpisi finančnih institucij, ki delujejo na območju RS, ne glede na lastniško strukturo in model upravljanja.

Problem, ki ga ob raziskovanju želim spoznati in razumeti, je organiziranost sistema varnosti v bankah in hranilnicah. Zavedam se namreč, da varnostni problem ne predstavlja zgolj tveganje za neposreden fizičen napad na finančno institucijo in s tem delno prekinjeno poslovanje finančne institucije na eni lokaciji. Varnostna tveganja namreč obstajajo ves čas poslovanja finančne institucije tudi po spletnem bančništvu, ki je vse pogostejši način opravljanja bančnih storitev. Problem obvladovanja teh varnostnih tveganj pa zaenkrat ni v domeni zasebne varnostne službe, saj gre za specifična tveganja, pri katerih je za preprečevanje in obvladovanje tveganj potrebno visoko kvalificirano in specifično znanje. Kako zagotoviti celovito obvladovanje vseh varnostnih sistemov glede na to, da pri tem sodeluje več izvajalcev, ki med sabo niso neposredno povezani, je problem, s katerim se spopada varnostni management vsake posamezne finančne institucije. Ob zavedanju, da se delovanje varnostnega sistema (vključeni izvajalci in razdelitev nalog) opredeljuje kot varovan podatek, bom z raziskovanjem, intervjujem in vpogledom v dokumentacijo, ki ureja varovanje bančnega poslovanja, ugotavljala, kako se varnostni sistemi med seboj dopolnjujejo in so hkrati neodvisni eden od drugega, pri čemer so vsakodnevno izpostavljeni problemu varnostnega tveganja iz različnih vzrokov (zunanji vplivi ali notranji dejavniki). Glede na dejstvo, da se vse več plačilnega prometa opravlja brezgotovinsko in po spletnem bančništvu, je pričakovan problem obvladovanje varnostnih tveganj, ki nedvomno pri tem nastajajo in jih je z razvojem informacijske tehnologije vse več. Razsežnost varnostnih tveganj in razširjenost problema

ogroženosti po spletnem poslovanju je izziv za varnostni management in tudi za odločevalce ter lastnike.

1.2 *Namen, cilji in osnovne trditve*

Namen mojega diplomskega dela je predstaviti obvladovanje varnostnih tveganj v okviru poslovanja finančne institucije v RS, njihovo pravno ureditev ter umestitev v področje varovanja ter izvedbo varovanja finančnih institucij po zasebni varnostni službi.

Cilj diplomskega dela je dokazati, da je varnost finančnih institucij najranljivejša po spletnem poslovanju in je zato treba varnostne sisteme v okviru informacijske tehnologije ves čas spremljati, preverjati, ocenjevati in nadgrajevati. Uvajanje novih tehničnih rešitev pri izvedbi sistema varovanja mora biti načrtovano in premišljeno. Zagotovljeno mora biti vključevanje različnih strokovnjakov, in sicer s ciljem čim bolj zmanjšati možnost negativnih varnostnih dogodkov za bančno poslovanje.

V diplomskem delu bom skušala ob raziskavi področja izvedbe varovanja v finančnih institucijah potrditi, da je varovanje finančnih institucij najbolj izpopolnjeno pri varovanju objekta, v katerem se dejavnost opravlja.

Z raziskavo in ob uporabi uradnih statističnih podatkov o izvršenih kaznivih dejanjih, pri katerih je predmet napada finančna institucija in denar, bom skušala potrditi, da je največ negativnih varnostnih dogodkov povezanih s poslovanjem po spletu.

Z raziskavo in intervjujem bom skušala potrditi trditev, da je za varnost finančne institucije zelo pomembna tudi visoka varnostna zavest in usposobljenost uslužbencev.

Na podlagi teh raziskav bomo preverili pravilnost naslednjih trditev:

- **H1:** varovanje finančnih institucij je najbolj izpopolnjeno pri varovanju objekta
- **H2:** največ negativnih varnostnih dogodkov je povezano z delovanjem finančne institucije po spletu
- **H3:** finančna institucija mora graditi visoko varnostno zavest uslužbencev

1.3 *Predpostavke in omejitve*

Večina informacij, ki so uporabljene v diplomskem delu, prihaja od preverjenih virov ali oseb, ki se z dejavnostjo ukvarjajo. Pri pisanju diplomskega dela sem bila omejena pri pridobivanju

literature in konkretnih podatkov, ki se nanašajo na celovit sistem varovanja v bankah in hranilnicah, saj so podatki, ki se nanašajo na obravnavano tematiko, večinoma poslovna skrivnost. Raziskovanje po javno dostopnih objavah in literaturi, s ciljem pridobiti konkretne podatke za obravnavan problem celovitega varnostnega sistema v finančnih institucijah, je bilo uspešno zgolj za teoretični del, prav tako iz razloga varovanja tajnih podatkov. Pri pripravi vprašanj za izvedbo intervjuja sem morala upoštevati omejitve, postavljene s strani odgovorne osebe banke; prav tako sem bila zaradi nepripravljenosti sodelovanja primorana v diplomsko delo vključiti intervju odgovorne osebe ene od bank, ki delujejo v slovenskem bančnem sistemu.

1.4 *Uporabljene raziskovalne metode*

Delo je sestavljeno iz teoretičnega in praktičnega dela. Teoretični del vsebuje vire iz zakonodaje, priročnikov, knjig in internega gradiva finančne institucije. Praktični del pa je sestavljen iz intervjuja, raziskave obravnavanega področja po spletnih objavah in javno dostopnih virih ter iz analize statističnih podatkov, ki so pridobljeni z raziskavo javno objavljenih statističnih podatkov Policije, ki po uradni dolžnosti obravnava opredeljena kazniva dejanja, s katerimi sem med ostalim potrjevala postavljene trditve v diplomski nalogi.

2 SLOVAR POJMOV

V tem poglavju bodo predstavljeni temeljni pojmi, ki bodo v diplomski nalogi omenjeni in so pomembni za lažje razumevanje celotne vsebine.

BANKA/HRANILNICA – izraz se uporablja za kreditno institucijo, ki ima sedež v RS in ima dovoljenje za opravljanje bančnih storitev v skladu z zakonom.

ALARM – zvočni znak, ki opozarja na prisotnost nevarnosti lastnine. Alarm, ki ga sproži ali avtomatska naprava ali oseba, zahteva ukrep.

ALARMNI SISTEM – PROTIROPNI – sprožitveni sistem za javljanje ropov v finančnih institucijah.

ALARMNI SISTEM – PROTIVLOMNI – sistem za javljanje vloma v finančnih institucijah. Je sistem za zgodnje odkrivanje prisotnosti vstopa vlomilca ali poskusa v nadzorovane prostore finančne institucije.

ALARMNI SISTEM – POŽARNI SISTEM – naloga požarnega sistema je odkrivanje in javljanje požara z zvočno, svetlobno in pa drugo obliko signalizacije.

FIZIČNO VAROVANJE – varovanje finančne institucije s fizično prisotnostjo varnostnika.

TEHNIČNO VAROVANJE – varovanje finančne institucije z alarmi, video-nadzornim sistemom ter mehansko zaščito.

MEHANSKO VAROVANJE – mehanska zaščita, kot so sefi, trezorji, cilindrični vložki, vratna in okenska varovala, zapornice ipd.

INTERVENCIJA – odziv pooblaščenih oseb na kraj dogajanja.

JAVLJALNIK – element, ki odkriva nepravilne ter nezaželene nenavadne okoliščine, ki pomenijo prisotnost nevarnosti.

NAČELO »4 OČI« – dejavnost, ki ga istočasno izvajata dve osebi.

LICENCA – dovoljenje za opravljanje dejavnosti varovanja.

NAČRT VAROVANJA – je obvezen dokument, v katerem mora finančna institucija opredeliti vsa tveganja v okviru svojega delovanja.

NAČRTOVANJE VARNOSTNIH SISTEMOV – tehnična dokumentacija, ki je pomembna za pravilno delovanje varnostnih sistemov.

PREVOZ IN VAROVANJE GOTOVINE TER VREDNOSTNIH POŠILJK – prevoz s prilagojenimi, posebnimi prevoznimi sredstvi ter varnostniki od točke A do točke B.

SAMOPOSTREŽNA NAPRAVA – bankomati, avtomatski sefi, naprave za štetje kovancev, dnevno-nočni trezorji ipd.

SEF – je omarica, ki je namenjena strankam za varno hranjenje predmetov z ustrezno varnostno zaščito.

SENZOR – zazna spremembo stanja, ki bi lahko pomenila prisotnost nevarnosti.

SISTEM ZA OBARVANJE GOTOVINE – trajno obarva gotovino ob sprožitvi.

TREZOR – poseben prostor, ki je namenjen shranjevanju gotovine ter drugih vrednosti; vstopanje skozi ustrezna posebna in prilagojena vrata.

TREZORSKA BLAGAJNA – shranjevalna enota, izdelana v skladu s standardi, namenjena hranjenju gotovine ter ostalih vrednosti; hramba v posebnem varovanem prostoru.

VNC – varnostni nadzorni center.

TVEGANJE – verjetnost, da se bo zaradi nekih dejavnikov zgodila škoda ali drug negativen izid.

VARNOST – stanje, ko smo obvarovani pred negativnimi dogodki in stanji.

VARNOSTNA FUNKCIJA – dejavnost, ki se ukvarja z rešitvijo in pa z organiziranjem varovanja.

VARNOSTNO OSEBJE – osebje s pooblastili, ki opravljajo naloge v skladu z zakonom.

VAROVANJE LJUDI IN PREMOŽENJA – varovanje ljudi, premičnega in nepremičnega premoženja, ki se nahaja na varovanem območju, pred poškodovanjem, uničenjem, tatvino ter drugimi negativnimi vplivi z varnostniki in drugimi sistemi za varovanje.

VAROVANO OBMOČJE – to je območje, na podlagi ocene stopnje tveganja razporejeno v varnostne razrede.

VIDEONADZORNI SISTEM – sistem, ki omogoča vidno nadziranje gibanja v varovanem območju in njeni okolici.

ZASEBNO VAROVANJE – gospodarska dejavnost, ki je namenjena za varovanje ljudi in premoženja na varovanem območju pred nezakonitimi dejanji, z varnostnim osebjem ter tehnično/mehanskimi sistemi varovanja.

FINANČNE INSTITUCIJE – so banke in hranilnice, ki dejavnost opravljajo z dovoljenjem Banke Slovenije in so s tem zavezane k izvedbi vseh potrebnih ukrepov varovanja.

3 FINANČNE INSTITUCIJE V REPUBLIKI SLOVENIJI

3.1 *Banka Slovenije*

Banka Slovenije je centralna banka RS. Ustanovljena je bila 25. 6. 1991 s sprejetjem Zakona o Banki Slovenije. Je pravna oseba javnega prava, ki samostojno razpolaga s svojim premoženjem. Banka Slovenije je v državni lasti na finančni in upravljavski avtonomiji, računovodske izkaze le-te pa revidira neodvisni mednarodni revizor.

Banka Slovenije ter člani njenih organov odločanja so neodvisni in pri opravljanju svojih nalog po Zakonu o Banki Slovenije niso vezani na sklepe, stališča, navodila državnih ali katerih koli organov, se ne smejo nanje niti obračati za navodila in usmeritev.

Banka Slovenije je postala del Evropskega sistema centralnih bank (ESCB) s časom, ko je RS postala članica Evropske unije (EU), in sicer 1. 5. 2004. Banka Slovenije je postala del Evrosistema, ko je RS uvedla evro, na katerega je bila hkrati prenesena pristojnost za vodenje denarne politike, in sicer 1. 1. 2007.

Pri uresničevanju nalog Banke Slovenije se z dnem uvedbe evra kot valute RS upoštevajo določila Statuta ESCB in Evropske centralne banke (ECB) (Banka Slovenije Evrosistem, 2017).

3.1.1 *Naloge Banke Slovenije*

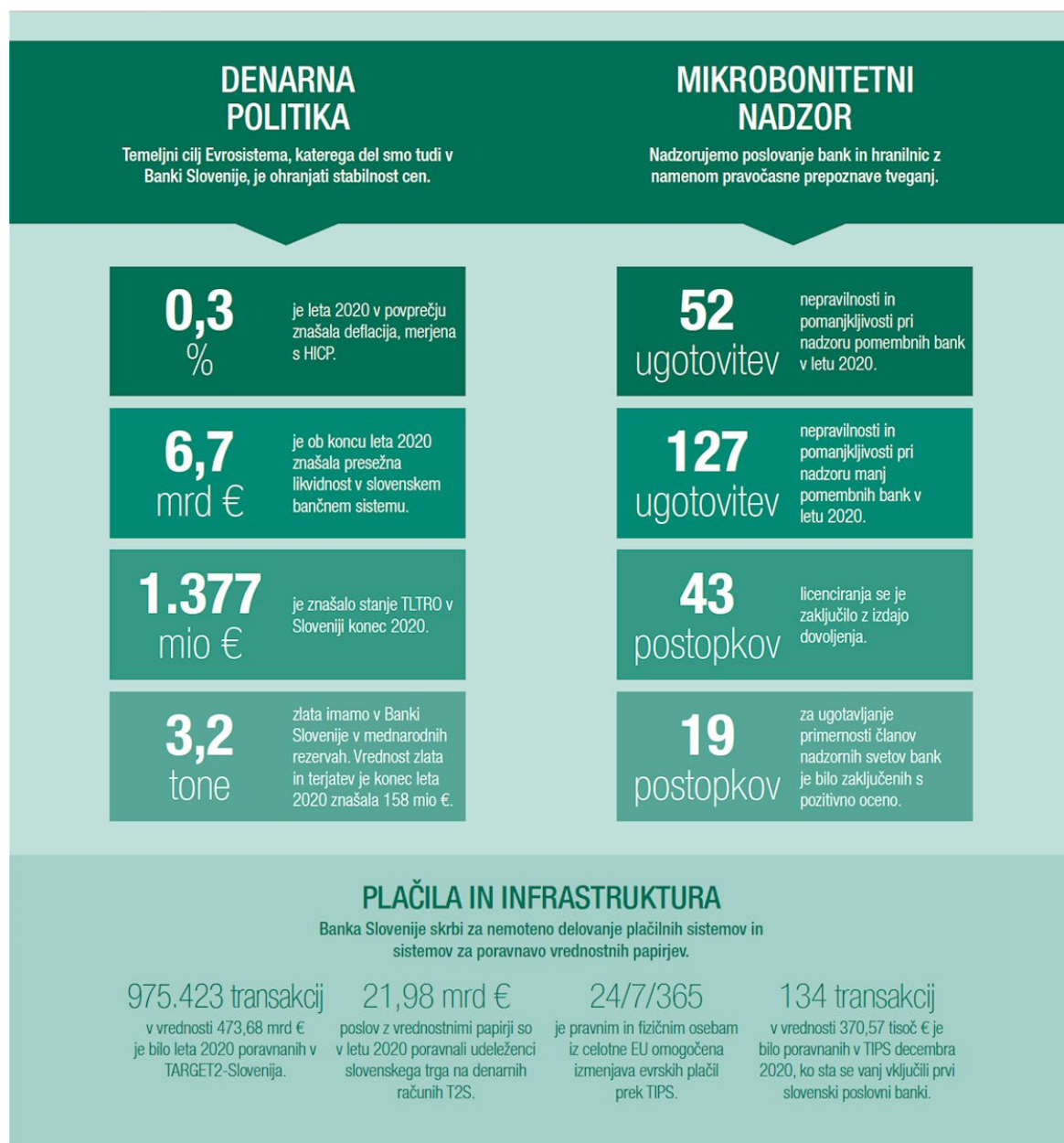
Banka Slovenije opravlja naslednje naloge (kot članica Evrosistema skladno s Pogodbo o delovanju EU in Statutom ESCB in ECB):

- izvaja skupno denarno politiko Evrosistema;
- upravlja uradne devizne rezerve;
- skrbi za nemoteno delovanje plačilnih sistemov;
- izdaja evrobankovce.

Med drugim pa opravlja tudi druge zakonsko določene naloge:

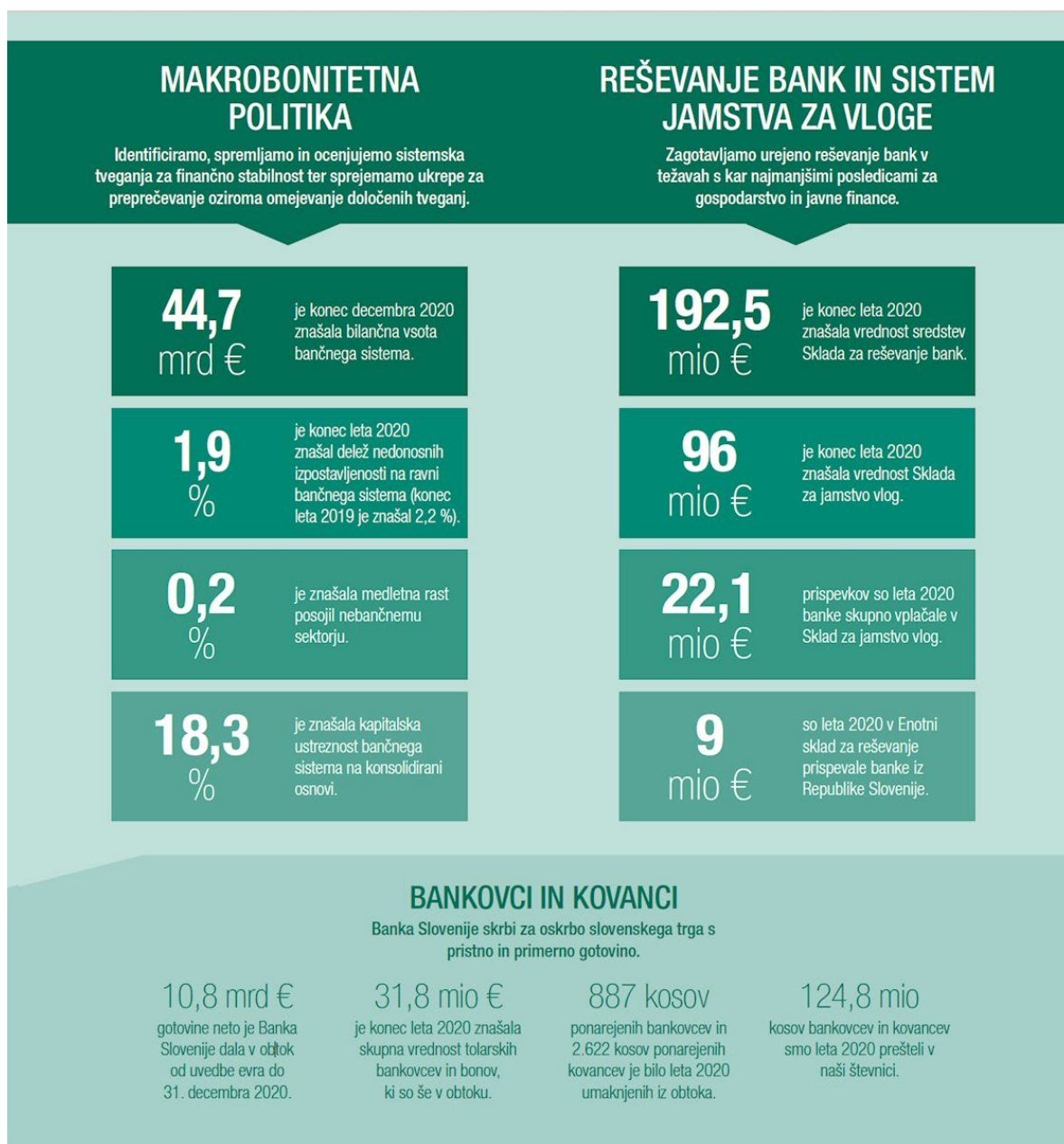
- nadzira banke in sodeluje pri ohranjanju finančne stabilnosti;
- upravlja osrednjo nacionalno zbirko podatkov o zadolženosti fizičnih oseb in poslovnih subjektov – Centralni kreditni register;
- skrbi za varnost depozitov in reševanje bank;
- skrbi za oskrbo območja RS z gotovino;
- vodi račune ter opravlja plačilni promet za RS, državne organe in osebe javnega prava ter banke;
- zbira, obdeluje in izkazuje statistične podatke, ki so pomembni za delovanje denarnega in finančnega sistema (Banka Slovenije, 2022).

3.1.2 Ključna področja delovanja in naloge Banke Slovenije



Slika 1: Področja delovanja in naloge Banke Slovenije 1

(Banka Slovenije Evrosistem, 2017)



Slika 2: Področja delovanja in naloge Banke Slovenije 2

(Banka Slovenije Evrosistem, 2017)

3.1.3 Vizija Banke Slovenije

V prihodnost usmerjena in proaktivna centralna banka s predanimi strokovnjaki, z visokimi etičnimi standardi, ki sodelujejo pri oblikovanju in izvajanju denarne politike v smeri ohranitve cenovne stabilnosti ter skrbijo za nadzor bank z namenom zagotavljanja stabilnosti finančnega sistema (Banka Slovenije, 2022).

3.1.4 Cilji Banke Slovenije

Strategija Banke Slovenije je temeljni dokument o njenih ciljih, vrednotah in razvoju. Veljavna strategija kot pet strateških ciljev v obdobju 2015–2020 določa:

1. okrepljen nadzor bančnega in finančnega sistema;
2. poglobljeno poznavanje ključnih makroekonomskih izzivov ter pravočasno sprejemanje ukrepov, opozoril in predlogov;
3. bolj prepoznavna vloga Banke Slovenije v Evrosistemu in EU;
4. uspešno ter učinkovito delovanje in poslovanje – s prožno organizacijo in z motiviranimi sodelavci;
5. večji ugled in zaupanje javnosti (Banka Slovenije, 2022).

4 PRAVNA UREDITEV PODROČJA VAROVANJA FINANČNIH INSTITUCIJ

4.1 *Zakoni in podzakonski akti*

Predmet obravnave v diplomski nalogi so izključno finančne institucije (banke in hranilnice), ki imajo za izvajanje svoje dejavnosti dovoljenje Banke Slovenije (ne glede na lastništvo) in so iz tega razloga obvezane izpolnjevati predpisane naloge in aktivnosti. Med drugimi kriteriji, ki jih morajo izpolnjevati, so tudi aktivnosti s področja varovanja. Področje varovanja bank in hranilnic je med ključnimi nalogami za ohranjanje varnosti in stabilnosti finančnih institucij in je tudi iz tega razloga zajeto v več zakonskih in podzakonskih predpisih, ki jih bom v nadaljevanju predstavila.

4.1.1 *Zakon o Banki Slovenije*

Zakon o Banki Slovenije ZBS-1 (sprejet 19. 6. 2002) med ostalim opredeljuje pojem bank in hranilnic in v 23. členu nadzor nad poslovanjem bank in hranilnic s ciljem zagotavljanja standardov varnega poslovanja bank in hranilnic. Zakon o Banki Slovenije je bistven tudi zato, ker brez dovoljenja Banke Slovenije finančna institucija na območju RS ne sme izvajati dejavnosti bank in hranilnic (Zakon o Banki Slovenije, 2002).

4.1.2 *Zakon o bančništvu*

Zakon o bančništvu ZBan-3 (sprejet 27. 5. 2021) ureja pogoje za ustanovitev, poslovanje in redno prenehanje kreditnih institucij s sedežem v RS. Ta zakon se ne uporablja za storitve, ki jih opravlja banka Slovenije v skladu z zakonom, ki ureja banko Slovenije, ali drugim aktom, ki ureja pristojnosti in naloge banke Slovenije. V 14. členu opisuje obveznosti varovanja zaupnih informacij. Kaj pa so zaupni podatki, pa ureja 145. člen tega zakona. V 146. členu pa je zapisano o dolžnostih o varovanju zaupnih podatkov (Zakon o bančništvu, 2021).

4.1.3 Zakon o gospodarskih družbah

Ta zakon je začel veljati že leta 1993, večje spremembe zakona pa so se zgodile leta 2006, ko je Slovenija vstopila v EU. Zakon določa temeljna pravila ustanovitve in poslovanja gospodarskih družb, samostojnih podjetnikov itd. (Zakon o gospodarskih družbah, 2006).

4.1.4 Basel II

Basel II (kapitalski sporazum) je priporočilo za oblikovanje politik v zvezi z obvladovanjem tveganj. Določa, koliko kapitala mora imeti banka ali druga finančna institucija glede na nivo finančnih in operativnih tveganj, s katerimi se sooča. Sporazum ni zavezujoč, vendar je mednarodno uveljavljen in se uporablja po vsem svetu. Oblikovan je leta 2004, sprejet pa leta 2006 (Basel II, 2013).

4.1.5 Uredba o varovanju tajnih podatkov

Uredba določa načine in oblike označevanja tajnih podatkov, fizične, organizacijske in tehnične ukrepe ter obvezne sestavine postopkov za varovanje tajnih podatkov, ki jih morajo pri vzpostavitvi sistema ukrepov in postopkov varovanja tajnih podatkov upoštevati in zagotoviti vsi organi in organizacije (Uredba o varovanju tajnih podatkov, 2005).

4.1.6 Zakon o varstvu osebnih podatkov

Zakon določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neopravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Obravnava načela obdelave, varstva in shranjevanje osebnih podatkov (Zakon o varstvu osebnih podatkov, 2004).

4.1.7 Zakon o varstvu pred požarom

Zakon ureja sistem varstva pred požarom. Obsega organiziranje, načrtovanje, izvajanje, nadzor ter financiranje dejavnosti in ukrepov varstva pred požarom. Dejavnost opravljajo fizične in pravne osebe, samostojni podjetniki, ki samostojno opravljajo dejavnost, v kolikor izpolnjujejo predpisane pogoje. Dejavnost po zakonu so raziskovanje, izobraževanje in usposabljanje, načrtovanje ukrepov varstva pred požarom, nadziranje, požarno zavarovanje, gasilstvo, tehnični

nadzor vgrajenih sistemov požarne zaščite, dimnikarstvo, požarno varovanje premoženja in drugo (Zakon o varstvu pred požarom, 1993).

4.1.8 *Pravilnik o požarnem varovanju*

S pravilnikom se določa pogoje in način izvajanja požarnega varovanja premoženja ter nadzor nad izvajanjem požarnega varovanja, ki ga opravljajo pravne osebe, in merila za požarno pokrivanje določenih vrst objektov, ki jih lahko požarno varujejo požarne enote. V pravilniku se uporabljajo naslednji pojmi:

- a) POŽARNO VAROVANJE – je varovanje premoženja objekta pred požarom. Vključuje tehnično in fizično požarno varovanje.
- b) TEHNIČNO POŽARNO VAROVANJE – obsega nadzor prenosa signalov od vgrajenega sistema aktivne požarne zaščite v varovanem objektu do VNC.
- c) FIZIČNO POŽARNO VAROVANJE – obsega preventivni pregled varovanega objekta med obhodom, preverjanja stanja v objektu po prejetem signalu, obveščanje pristojne gasilske enote ob požaru, gašenje začetnega požara in drugo ustrezno ukrepanje. Opravlja ga varnostnik, ki je trajno, občasno, med obhodom ali po prejetem signalu, navzoč v varovanem objektu.

V 9. členu pravilnika je obrazložen pomen pojma varnostnik. Oseba, ki izpolnjuje osebne pogoje za varnostnika, ki so določeni v zakonu, ki ureja zasebno varovanje, mora opraviti tudi preizkus znanja oziroma usposobljenost iz varstva pred požarom. Varnostnik, ki pa pri svojem delu vstopa v eksplozijsko ogrožene prostore, pa mora opravljati redna periodična usposabljanja in preizkuse znanja, za katere pa je odgovoren imetnik pooblastila za izvajanje požarnega varovanja. Usposabljanja in preizkuse znanja iz varstva pred požarom izvajajo izvajalci, usposobljeni na področju varstva pred požarom (Pravilnik o požarnem varovanju, 2007).

4.1.9 *Pravilnik o študiji požarne varnosti*

Pravilnik o študiji požarne varnosti določa vrsto in vsebino študije požarne varnosti, pogoje za pridobitev ter odvzem pooblastila tistim, ki izdelujejo študije ter objekte, pri katerih se mora izdelati študija. Študija je sestavljena iz splošnega dela, ki mora vsebovati podatke o naročniku in izdelovalcu študije, podatke o objektu, pomemben je podpis izdelovalca študije in pa

vsebovati mora tudi seznam upoštevanih predpisov, standardov in druge specifikacije ter strokovne literature. Splošnemu delu sledi strokovni pisni del študije, ki pa mora vsebovati opis objekta, oceno požarne nevarnosti in ogroženosti, kakšni so načrtovani ukrepi varstva pred požarom in pa oceno ustreznosti načrtovanih ukrepov. Grafična priloga študije pa vsebuje rešitve pred predvidenimi požarnovarnostnimi ukrepi (evakuacijske in intervencijske poti, lokacije naprav ter sredstev za osnovno gašenje, požarna odpornost, meje požarnih/dimnih sektorjev ipd.) (Pravilnik o študiji požarne varnosti, 1998).

4.1.10 Zakon o zasebnem varovanju

Zakon o zasebnem varovanju (ZZasV-1) ureja pravice in obveznosti gospodarskih družb, samostojnih podjetnikov posameznikov, državnih organov, zavodov ..., in sicer na področju varovanja, ki ga ne zagotavlja država. Zakon določa zasebno varovanje, oblike varovanja, pristojnosti, pogoje, standarde, usposabljanje, ukrepe in dolžnosti varnostnika, delovno obleko, nadzor itd.

Zakon določa zasebno varovanje, oblike varovanja, pristojnosti, pogoje za upravljanje zasebnega varovanja, standarde, strokovna usposabljanja, ukrepe ter dolžnosti varnostnika, evidence in kazenske določbe, nadzor ... Zakon navaja tudi pristojne organe za izvajanje nalog s področja zasebnega varovanja. Ta organa sta ministrstvo, ki je pristojno za notranje zadeve, ter zbornica na področju zasebnega varovanja. Zakon opredeljuje tudi pogoje za opravljanje zasebnega varovanja ter vrste licenc, opredeljeni so postopki za pridobitev licence, spremembo licence ter pogoji za začetek opravljanja zasebnega varovanja (Zakon o zasebnem varovanju, 2011).

4.1.11 Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih

Ta zakon ureja način, organizacijo, infrastrukturo in izvedbo zajema ter hrambe dokumentarnega gradiva v elektronski in fizični obliki. Opredeljuje temeljna načela, arhivsko javno službo, zagotavljanje infrastrukture ... (Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih, 2006).

4.1.12 Pravilnik o načinu prevoza in varovanja denarja ter drugih vrednostnih pošilk

Pravilnik določa način prevoza in varovanje gotovine ter drugih vrednostnih pošilk z namenom, da se zmanjšajo in preprečijo nevarnosti odtujitve ter se poveča varnost oseb, ki take pošiljke prevažajo. Določa tudi, kdo lahko opravlja prevoze in varovanje gotovine ter pogoje za to delo. Pravilnik opredeljuje pojme in posamezne izraze v zvezi z vsebino pravilnika (prevoz pošiljke, tveganje, neprebojno vozilo, komunikacijski sistem, nadzorni sistem ...). Pravilnik določa tudi:

- vrste varnostnih ukrepov pred prevozom vrednostnih pošilk;
- načine za zmanjšanje tveganja;
- preventivne varnostne ukrepe;
- načrt prevoza;
- usposabljanje za imetnike licenc;
- vsebino operativnega načrta za pošiljke tretjega, četrtega in petega razreda in
- način za opravljanja vozil za prevoz ali spremstvo varovanih pošilk – to so razni pregledi, vzdrževanja in pa nadzor (Pravilnik o načinu prevoza in varovanja gotovine ter drugih vrednostnih pošilk, 2016).

4.1.13 Zakon o varnosti in zdravju pri delu

Zakon o varnosti in zdravju pri delu (Ur. I. 43/2011) je začel veljati s 4. 12. 2011 – prinesel je spremembe za delodajalce in zaposlene. Zakon se usklajuje z okvirno direktivo s področja varnosti in zdravja pri delu, odpravo administrativnih bremen in z njimi povezanih stroškov za delodajalca. Zaostruje pa tudi dosledno izvajanje ukrepov za zmanjšanje ogroženosti zdravja delavcev, obveznost za pripravo pisnih ocen tveganja, katerim so izpostavljeni uslužbenci. Zaostrujejo pa se tudi kazenske določbe za delodajalca (Zakon o varnosti in zdravju pri delu, 2011).

5 IZVEDBA VAROVANJA FINANČNIH INSTITUCIJ PO ZASEBNI VARNOSTNI DRUŽBI

Banka je dolžna zagotoviti varovanje ljudi in premoženja v skladu z varnostno politiko banke, skrbeti mora, da so varnostna oprema in naprave ustrezno certificirane. Vse pogodbe, ki se nanašajo na izvajanje nalog varovanja, morajo natančno definirati medsebojne obveznosti in odgovornosti, načine komuniciranja in obveščanja, naštetih morajo biti tudi vsi morebitni podizvajalci. Za varovanje finančnih institucij se ne sme najemati izvajalcev, ki ne izpolnjujejo določil Zakona o zasebnem varovanju (Vačovnik, Interno gradivo, 2022).

5.1 Načrt varovanja

Načrt varovanja je dokument, ki določa način in obseg varovanja z varnostnim osebjem in s sistemi tehničnega varovanja ter ukrepi za varovanje. Izdela se za zagotavljanje strokovnega, učinkovitega in stopnji tveganja prilagojenega varovanja. Kakšno varovanje bo organiziral nek subjekt, je odvisno od njega, od tveganj, ki so prisotna v njegovi dejavnosti, od odnosa vodstva do varnosti in strokovnega znanja tistih, ki so pri subjektu odgovorni za varnost. Sestavni deli načrta varovanja so ocena stopnje tveganja, program varovanja, načrt fizičnega varovanja (Vačovnik, Interno gradivo, 2022).

5.1.1 Ocena stopnje tveganja

Ocena stopnje tveganja je ocena nevarnosti oziroma ogroženosti, ki temelji na varnostnih potrebah varovanega območja, izpolnjevanju zahtev predpisov, zmogljivostih in drugih okoliščinah ter verjetnosti nastanka posledic, ki bi lahko vplivale na varnost, ter je podlaga za izdelavo načrta varovanja. Obvezni elementi ocene stopnje tveganja so podatki o zavezancu, opis varovanega območja, analiza ranljivosti, analiza ogroženosti, analiza tveganj, splošna ocena o stopnji tveganja z oceno verjetnosti nastanka posledic.

Ocena tveganja se določa v treh stopnjah – nizka stopnja (verjetnost tveganja je manjša – poslovanje je normalno), srednja (verjetnost tveganja obstaja – poslovanje je lahko moteno) in visoka (verjetnost za nastanek škodnih dogodkov je večja – poslovanje je ogroženo) (Vačovnik, Interno gradivo, 2022).

5.1.2 Program varovanja

Program varovanja predstavlja varnostno politiko nekega subjekta. Gre za dokument, v katerem so opredeljeni namen varovanja, pregled pravnih podlag, zahtev, meril, pristojnosti in dolžnosti pri varovanju ter izhodišča za varovanje in drugi ukrepi za izvedbo učinkovitega varovanja. Obvezni elementi programa varovanja so opredelitev namena varovanja, pregled pravnih podlag, zahteve, merila, pristojnosti in službe varovanja, izhodišča in drugi ukrepi za izvedbo učinkovitega varovanja (Vačovnik, Interno gradivo, 2022).

5.1.3 Načrt varovanja za finančne institucije

Načrt varovanja za finančne institucije je dokument, v katerem vsaka finančna institucija opredeli:

- organizacijo varovanja premoženja;
- prevoz gotovine in drugih vrednostnih pošiljk;
- upravljanje z varnostnim operativnim centrom in
- načrtovanje in izvajanje varnostnih sistemov.

Načrt o varovanju premoženja finančne institucije zajema tudi analizo operativnega tveganja in načrt varovanja, ki ima podlago v analizi operativnega tveganja. V načrtu se izpostavi tudi t. i. krizni načrt in načrt neprekinjenega poslovanja finančne institucije.

Tveganja pri poslovanju finančnih institucij razumemo kot možnost dogodkov, ki so drugačni od sicer predvidenih aktivnosti. Ravno zato je treba izhajati iz dobrega predvidevanja škodnih dogodkov in s tem povezanega obvladovanja. Predvidevanja so vključena v krizni načrt in se z njimi obvladujejo odstopanja od normalnih aktivnosti v poslovanju finančnih institucij.

Med posebno področje, zajeto v načrtu varovanja premoženja finančne institucije, spada tudi področje upravljanja tveganja, ki opredeljuje operativno tveganje, ki se nanaša na možnost izgube zaradi neuspelega ali nezadostnega izvajanja notranjih procesov, ravnanj ljudi, delovanja sistemov ali zaradi zunanjih dejavnikov ali dogodkov. Finančna institucija mora vsaj enkrat letno zagotoviti ugotavljanje in ocenjevanje pomembnih operativnih tveganj. V kolikor so operativna tveganja nedvomno zaznana, je treba izvesti takojšnjo analizo vzrokov za nastalo realizirano tveganje (Vačovnik, Interno gradivo, 2022).

5.1.4 Načrt fizičnega varovanja

Načrt fizičnega varovanja je dokument, ki obsega varovanje z varnostnim osebjem in s sistemi tehničnega varovanja. Zavezanec mora zagotavljati, da se načrt fizičnega varovanja ažurira sproti, glede na spremenjene varnostne razmere in ocene stopnje tveganja.

Načrt fizičnega varovanja mora biti pripravljen tako, da so varnostni ukrepi prilagojeni posamezni oceni stopnje tveganja glede na to, ali gre za nizko, srednjo ali visoko stopnjo tveganja (Vačovnik, Interno gradivo, 2022).

5.2 Tehnično varovanje

Sistemi tehničnega varovanja so posamezna ali funkcionalno povezana tehnična sredstva in mehanske naprave za protivlomno in protiropno varovanje, kontrolo vstopa, izstopa ali gibanja, pregled oseb, prevoznih sredstev, tovora in prtljage, preprečevanje nasilnega vstopa, samodejno odkrivanje in javljanje nepooblaščne prisotnosti, prenos alarmnih sporočil ter sredstva za obdelavo in arhiviranje teh sporočil, električne, elektromagnetne ali biometrične naprave za pristopno kontrolo ter drugi sistemi in naprave, ki so namenjeni varovanju po Zakonu o zasebnem varovanju.

Med tehnično varovanje sodijo naslednji sistemi:

- mehanske zaščite;
- sistemi protivlomnega varovanja;
- sistemi protipožarnega varovanja;
- sistemi za detekcijo in merjenje eksplozivnih ter strupenih plinov;
- videonadzor;
- pristopna kontrola;
- evidenca delovnega časa;
- industrijski alarmi;
- centralno-nadzorni sistemi;
- sistemi varnostnega dima.

Sistemi tehničnega varovanja v kombinaciji s fizičnim varovanjem zmanjšujejo odvisnost od človeškega faktorja. Z uvedbo sistema se zmanjša tudi število varnostnikov, ki so potrebni za varovanje objekta (Vačovnik, Interno gradivo, 2022):

5.2.1 Tehnično varovanje v finančnih institucijah

Tehnično varovanje je funkcionalno povezano delovanje več tehničnih sredstev in mehanskih naprav za varovanje v koordinirano celoto, kar se poimenuje v sistem tehničnega varovanja. Sistemi tehničnega varovanja v finančnih institucijah morajo biti skladni z Zakonom o zasebnem varovanju in so lahko medsebojno povezani ali samostojno delujoči (Vačovnik, Interno gradivo, 2022).

5.2.2 Mehanska zaščita

Vloga sistemov mehanske zaščite je predvsem v onemogočanju dostopa nepooblaščenim osebam v varovana območja, zato imajo izrazit preventivni značaj. Uspešnost mehanske zaščite se meri s časom, ki ga potrebuje vlomilec za premostitev ovire. Daljši, kot je, uspešnejše je varovanje.

Z mehanskim varovanjem se nepooblaščenim osebam in vlomilcem prepreči dostop na neko območje ali v prostore. Sama mehanska zaščita ni dovolj, ampak jo je treba dopolniti in povezati še z drugimi sistemi tehničnega varovanja.

Med mehanska varovanja sodijo varnostne ograje in vrata, mehanska zaščita oken, mehanska zaščita vrat, protivlomna vrata, sistemi zaklepanja, protivlomni roloji, rešetke, varnostni trezorji ipd.

V finančnih institucijah se z mehansko zaščito s posebej izdelanimi mehanskimi napravami za varovanje (posamezne ali funkcionalno povezane) preprečuje dostop, vstop, odpiranje delovnih prostorov, naprav in se z njimi tudi omejuje gibanje. Najuporabnejše mehanske naprave za varovanje so ograje, vrata, stekla, ključavnice, zapahi, gradbene ovire ter elementi in zaporni sistemi, ki so nameščeni na blagajnah, sefih, trezorjih in na depojih gotovine. Vse mehanske naprave, uporabljene pri varovanju finančne institucije, morajo upoštevati naslednje gradbeno tehnične zahteve:

- SIST EN 1143-1 – ta standard razvršča varnostne shranjevalne enote, med katere spadajo blagajne in prostori. Standard ima štirinajst varnostnih protivlomnih razredov. Varnostni

razredi z oznako 0, I, II, III, IV, V, VI so namenjeni za klasifikacijo varnostnih omar, blagajn in oklopnih blagajn. Varnostni razredi z oznako V, VI, VII, VIII, IX, X, XI, XII IN XIII pa so namenjeni za klasifikacijo varnostnih oklopnih in prostorov s trezorji.

- SIST EN 1303:2005 je standard, ki razvršča profilne cilindre za ključavnice v šest varnostnih razredov proti vlamljanju.
- SIST EN V1627:2000 je standard, ki določa šest protivlomnih razredov za protivlomno odpornost vrat in oken glede na način ter čas vlamljanja (Vačovnik, Interno gradivo, 2022).

5.2.3 Gradbeno-tehnična priporočila

Kot sem že omenila, mora biti pri načrtovanju izgradnje objekta, v katerem bo delovala finančna institucija, že od začetka (od same idejne zasnove objekta naprej) varnostna funkcija vključena v proces izgradnje. Zato se pred načrtovanjem gradnje ali adaptacije objektov ali poslovnih prostorov finančne institucije presodi tveganje poslovanja in izdela varnostna ocena. To mora biti o predpisih in priporočilih upoštevano tako pri načrtovanju kot izvedbi gradnje ali obnove. S tem se doseže, da so upoštewane posebnosti bančnega poslovanja in omejitve, vse z namenom zmanjšanja tveganja nenormalnih situacij, protipožarne zaščite in ostalega. Od načrtovalca se upravičeno pričakuje, da dajejo prednost varnosti in funkcionalnosti, ki bo predvsem omogočala zagotavljanje in izvedbo varnostnih rešitev, s katerimi bodo uspešno izpolnjene zahteve varnosti z najmanjšimi vplivi na vsakdanji proces poslovanje banke oziroma hranilnice. Varnost in zanesljivost se zagotavlja torej od samega začetka ter v nadaljevanju skozi nadzor gradnje in vzdrževanje tega istega objekta (Vačovnik, Interno gradivo, 2022).

5.2.4 Sistemi požarnega varovanja

Požarno varovanje je urejeno v Pravilniku o pregledovanju in preizkušanju vgrajenih sistemov aktivne požarne zaščite. Glede na dejstvo, da spada požar med nenormalne situacije, je v finančnih institucijah vključenih več sistemov aktivne požarne zaščite, katerih namen je preprečiti, odkriti in omejiti morebitni požar. Sistemi požarne zaščite so:

- sistemi za odkrivanje in javljanje požara ter alarmiranje;
- naprave za odkrivanje, javljanje in gašenje v transportnih cevovodih;
- naprave za odkrivanje in javljanje prisotnosti gorljivih plinov ali par v zraku;

- vgrajeni gasilni sistemi s tekočimi gasili, plini ali praški;
- naprave za požarno vodno hlajenje s polivanjem ali škropljenjem;
- vgrajene naprave za znižanje koncentracije kisika;
- avtomatski sistemi za nadzor nad dimom in produkti zgorevanja ter odvod dima in toplote;
- sistemi za vzpostavljanje nadtlaka zraka v prostorih, katerih osnovni namen je aktivna požarna zaščita;
- varnostna razsvetljava v celotnem objektu;
- naprave in oprema, ki služi za pogon in krmiljenje požarnih dvigal.

Tudi za sisteme aktivne požarne zaščite je predpisano, da morajo ustrezati seriji standardov SIST EN 54 (odkrivanje požara, javljanje, alarmiranje in avtomatsko krmiljenje sistema požarne zaščite, v katero sodi gašenje, ločevanje požarnih in dimnih sektorjev, sistemi za odvod dima in toplote, klimatizacijske in prezračevalne naprave, dvigala, varnostna razsvetljava in drugo). Razen ustrežanja standardov morajo sistemi za avtomatsko gašenje požara ustrezati tudi predpisom in uredbam, ki urejajo to področje. Da bi se izvedlo tehnično brezhibno protipožarno varovanje, je v osnovi treba izdelati študijo požarne varnosti, na osnovi katere se izvedejo vsi sistemi protipožarnega varovanja (Vačovnik, Interno gradivo, 2022).

5.2.5 Sistemi tehnične zaščite za zaznavo razlitja tekočin ali uhajanja plinov

Med nenormalne situacije v okviru delovanja finančne institucije spadajo tudi tveganja razlitja tekočin ali ohlajanja plinov, ki so lahko nevarni (eksplozivni in/ali strupeni) za ljudi in premoženje. Med te tekočine in pline spadajo kurilno olje, zemeljski plin, utekočinjen naftni plin, CO, ogljikov dioksid, metan, mestni plin in butan. Sistemi za eksplozijsko varovanje morajo ustrezati standardov SIST EN 50054, SIST EN 50055, SIST EN 50056, SIST EN 50057 in SIST EN 50058. Razlitje tekočine, kot je voda, pa pomenijo nevarnost predvsem za premoženje, zato so sistemi za razlitje namenjeni predvsem opozarjanju zaposlenih in pristojnih služb.

Za kotlovnice, garaže, za zaščito pred napetostmi in strelovodno zaščito se v okviru izgradnje sistemov za varovanje uporabljajo določila Zakona o graditvi objektov (Vačovnik, Interno gradivo, 2022).

5.2.6 Sistemi za zaznavanje in javljanje vloma ali rop in klica v sili

Namen teh sistemov je, da zaznajo in javijo vlom, rop in klic v sili z za storilca nezaznavnim alarmiranjem pooblaščenih varnostnih služb. Sistem je izgrajen na način, da ga lahko sprožijo uslužbenci finančne ustanove sami ali tudi roparji s svojim delovanjem. Med te sisteme sodijo tudi naprave, ki obarvajo gotovino in roparja, ki je v stiku z njo. Tudi za tako imenovano protivlomno varovanje s sistemi za zaznavanje in javljanje vloma so predpisana izhodišča s standardom SIST EN 50131-1 za varnostne sisteme bank in hranilnic. Banke in hranilnice morajo navedeni standard uporabljati ob prvi namestitvi sistema ali ob prenovi, v kolikor ta sistem niso že uporabljale (Vačovnik, Interno gradivo, 2022).

5.2.7 Sistemi pristopne kontrole

Sam sistem pristopne kontrole je namenjen predvsem nadzoru nad varovanim območjem, pri čemer mora zagotavljati spoštovanje načel nadzorovanega, omejenega in selekcioniranega dostopa/vstopa. Poglavitne naloge tega sistema zaščite so krajevno in prostorsko omejevanje vstopov in izstopov iz varovanega objekta finančne institucije. Izpolnjevati je treba cilj doslednega evidentiranja vstopov in izstopov ter takojšnje obveščanje morebitnih kršitev pravic vstopa in izstopa. V sistem je vključena konstrukcijska in mehanska zaščita (zgradbe, opreme, vrata, mehanski omejevalniki, zapore), elektronsko podprti elektromagnetni sistemi za mehanske zapore, računalniško in/ali elektronsko nadzorovana in vodena tehnologija sistema elektromagnetnih ključavnic video sistemov domofona, video nadzornih in biometričnih komponent. Pri namestitvi in uporabi sistemov pristopne kontrole je treba upoštevati veljavni Zakon o varstvu osebnih podatkov s smiselno uporabo serije standardov SIST EN 50133 (Vačovnik, Interno gradivo, 2022).

5.2.8 Sistem za prenos alarmnih signalov

Naloga sistemov za prenos alarmnih signalov je, da omogočajo neposreden prenos stanj alarmnih sistemov iz varovanega objekta finančne institucije do VNC zasebne varnostne službe. Tudi za prenos teh alarmnih signalov je opredeljen standard, in sicer SIST EN 50131. Sistemi za prenos alarmnih signalov se uporabljajo za nadzor na bančnih avtomatih (Vačovnik, Interno gradivo, 2022).

5.2.9 Videonadzorni sistem

Pri vzpostavitvi videonadzornega sistema je treba upoštevati določila Zakona o varstvu osebnih podatkov in minimalne zahteve za videonadzorni sistem, ki jih določa serija standardov SIST EN 50132. Pomembni parametri pri zagotavljanju uporabne vrednosti videonadzornega sistema so:

- optimalna kakovost slike;
- optimalno snemanje;
- prilagojena osvetljenost ob upoštevanju minimalne osvetlitve;
- nameščenost videonadzornega sistema v posebnem varovanem prostoru ali pohoštvu;
- minimalen čas hranjenja posnetkov je 14 dni.

Banka ali hranilnica si kot nadstandardno storitev lahko zagotovi oddaljen dostop do posamezne ali več videosnemalnih naprav (Vačovnik, Interno gradivo, 2022).

5.2.10 Varnostno-nadzorni centri

Zadnji in najobčutljivejši ter najpomembnejši člen v sistemu tehničnega varovanja so VNC. V te centre se v realnem času (trenutnem) stekajo alarmna sporočila iz vseh priklopljenih, povezanih alarmnih sistemov, se obdelajo in shranijo. Iz VNC-ja se obveščajo ustrezne intervencijske in varnostne službe. Banke in hranilnice morajo od zasebnih varnostnih služb zahtevati, da jim zagotovijo mesečna poročila o razpoložljivosti VNC-ja. Za morebitno odločitev o sekundarnem VNC-ju morajo biti banke in hranilnice obveščene in s tem soglašati (Vačovnik, Interno gradivo, 2022).

5.3 Fizično varovanje

Fizično varovanje je varovanje življenja in premoženja ter osebne varnosti na varovanem območju. Izvaja se v skladu z Zakonom o zasebnem varovanju in pod zakonskimi predpisi, ki urejajo to področje.

Izvajanje nalog zasebnega varovanja temelji na uporabi ukrepov in pooblastil ter drugih sredstev varnostnih oseb, ki jih je treba podrobno poznati in biti izurjen za njihovo uporabo. Ukrepi in uporaba drugih sredstev se navezuje na vsa področja dela v zasebnem varovanju. Z

uporabo ukrepov in drugih sredstev se posega na področje varovanja temeljnih človekovih pravic in svoboščin, zato je še toliko pomembnejše znanje in izurjenost.

Varnostno osebje mora pri izvajanju ukrepov in drugih sredstev dosledno upoštevati načelo zakonitosti, strokovnosti, sorazmernosti, humanosti in etičnosti, vse z namenom, da bi z najmanjšimi možnimi posledicami dosegli izvedbo zadane naloge.

Kot posebnost izvedbe fizičnega varovanja v finančnih institucijah moram omeniti, da vidno oboroženi varnostniki niso primerni za delo v prostorih, kjer je v neposredni bližini večje število ljudi, kjer se opravlja delo s strankami. Izjemoma se vidno oboroženi varnostniki v poslovnih prostorih finančne institucije pojavijo takrat, ko drugi predpisi to izrecno zahtevajo (dostava gotovine, intervencije, prevzem gotovine in drugo).

Pri izvajanju fizičnega varovanja varnostnik uporablja naslednja zakonsko predpisana pooblastila, in sicer:

- opozorilo;
- ustna odredba;
- ugotavljanje istovetnosti;
- površinski pregled;
- preprečitev vstopa;
- zadržanje osebe;
- uporaba fizične sile;
- uporaba sredstev za vklepanje in vezanje;
- uporaba drugih sredstev – uporaba plinskega razpršilca in nošenje ter uporaba strelnega orožja (Savski, Rozman, Velički, Polutnik & Hartman, 2017).

5.3.1 Prevoz in prenos gotovine ter vrednostnih pošilk

Prevozi gotovine in prenos vrednostnih pošilk ter gotovine je ena iz med najpogostejših nalog, ki jih opravlja zasebna varnostna služba v okviru varovanja finančnih institucij. Sama izvedba je opredeljena v podzakonskem aktu Pravilnik o načinu prevoza in varovanje denarja ter drugih vrednostnih pošilk. Bistveno za uspešno izvedbo naloge je:

- pot od vozila, s katerim se upravlja prevoz, do trezorja, kjer se opravlja primopredaja, naj bo čim krajša;
- primopredaja gotovine ali vrednostnih pošiljk mora biti opravljena v varnem prostoru (prostor, ki ni viden iz prostora za stranke);
- čas primopredaje in prenosa do vozila mora biti čim krajši;
- postopek primopredaje mora biti ustrezno dokumentiran.

Primopredaja gotovine ter drugih vrednostnih pošiljk je postopek, pri katerem se opravi predaja oziroma prevzem gotovine iz varnega prostora (trezorja) v roke za to posebej opremljenim in usposobljenim varnostnikom ali obratno. Primopredaja je zaključena, ko je gotovina ali druga vrednostna pošiljka zaklenjena v trezorju ali predana varnostniku. Finančna institucija skladno z možnostmi zagotovi parkirno mesto, namenjeno specialnemu vozilu za prevoz gotovine ter drugih vrednostnih pošiljk, ki naj se nahaja v neposredni bližini vhoda v objekt, kjer bo potekala primopredaja. Zasebna varnostna služba kot prevoznik gotovine ter drugih vrednostnih pošiljk je finančni instituciji dolžna zagotoviti ažurne sezname delavcev, ki dejansko opravljajo dela in naloge varovanja in prevoza le-teh. Seznami morajo vsebovati identiteto varnostnika, podjetje in številko službene izkaznice. Zaposleni v finančni instituciji so dolžni preverjati istovetnost oseb s seznama s pomočjo službenih izkaznic.

Znotraj objekta banke ali hranilnice se vrši prenos gotovine, vrednostnih pošiljk in plemenitih kovin nemoteno v delu objekta, ki je fizično (mehansko) povsem ločen od dela objekta, v katerem se gibljejo stranke. Glede oskrbovanja bančnih avtomatov z gotovino, kar prav tako zagotavljajo varnostniki, je pravilo, da se oskrbujejo zunaj obratovalnega časa. Izjema je v primerih, ko se bankomati ne nahajajo v varnem prostoru. V primerih prenosa gotovine znotraj banke po t. i. pnevmatski (zračna cevna pošta) pošti se posebni ukrepi varnostnika ne pričakujejo, saj gre za prenos v okviru delovnih procesov in so v tej zvezi izpolnjeni vsi dokumenti. Kadar se pri prenosu gotovine ni možno izogniti križanju poti, v katerih se nahajajo stranke, se varnostno tveganje zmanjša z uporabo prirejenih kovčkov. Kot posebnost velja omeniti še, da mora biti vsak dvig večje količine predhodno najavljen (znesek določi banka ali hranilnica z internim aktom). V teh primerih se primopredaja gotovine izvede v za to namenjenem zaprtem prostoru in ne na blagajniškem delovnem mestu. V kolikor gre za dvig izredno velike količine gotovine, znesek določi banka ali hranilnica z internim aktom, vodja banke ali hranilnice pa mora o tem predhodno obvestiti svojega neposrednega nadrejenega

delavca in varnostnega managerja, ki zagotovi potrebne dodatne varnostne ukrepe in aktivnosti (Vačovnik, Interno gradivo, 2022).

5.4 Sodelovanje z varnostnimi službami in policijo

Finančne institucije spadajo med subjekte, za katere je predpisano obvezno organiziranje varnostne službe iz razloga, ker se na posameznem objektu banke ali hranilnice neposredno posluje z gotovino ter drugimi vrednostmi v protivrednosti najmanj 200.000 evrov. Obveznost organiziranja varovanja je določena v javnem interesu zaradi varovanja ljudi in premoženja, zaradi preprečevanja škodnih dogodkov in zaradi dejstva, da je varnost teh institucij v interesu države. Za zagotavljanje varnosti morajo banke in hranilnice same prepoznati obveznost organiziranja varnostne službe. Pri tem varnostni management zagotavlja sodelovanje z varnostnimi službami in policijo. Prav tako se z vidika varnosti lahko dogovori in izvede sodelovanje z drugimi državnimi ali zasebnimi službami v cilju izboljšati varnost (Vačovnik, Interno gradivo, 2022).

5.4.1 Sodelovanje z varnostnimi službami

Banke in hranilnice po prepoznani obveznosti organiziranja varovanja sklenejo pogodbo o sodelovanju z vidika varnosti z zasebno varnostno službo. Iz pogodbe morajo biti razvidne vse dolžnosti in pravice obeh pogodbenih strank. Kot najpomembnejša podlaga za sklenitev pogodbe med banko ali hranilnico in zasebno varnostno službo je licenca za opravljanje storitev varovanja, skladna z določili Zakona o zasebnem varovanju. Običajno takšna pogodba vsebuje tudi določilo o obveznem rednem mesečnem poročanju o vseh izrednih dogodkih v finančnih institucijah. Posebej se določi obveznost sprotnega obveščanja varnostnega managementa banke ali hranilnice o vseh nepredvidenih dogodkih. Obveščanje mora biti takojšnje in je lahko glede na čas nepredvidenega dogodka izvedeno po kateri koli obliki komunikacije (telefon, mail, ustno in podobno). Zasebna varnostna služba zagotavlja tudi obveščanje o rednih dogodkih v banki ali hranilnici, katere razlogi so razna vzdrževalna dela, servisi, popravila in drugo. Naloga varnostnega managerja banke ali hranilnice, ki ni zaposlen v zasebni varnostni službi, je redno opravljanje kontrole dela zasebne varnostne službe. V kolikor takšnega nadzora ni mogoče izvajati zadovoljivo, se varnosti manager lahko obrne na strokovno usposobljeno zunanjo institucijo (Vačovnik, Interno gradivo, 2022).

5.4.2 Obveščanje in sodelovanje s policijo

Pri varovanju finančnih institucij, kar izvaja zasebno varnostno podjetje, je po zakonskih določilih treba obveščati policijo v primerih, ko varnostnik uporabi katera od v nadaljevanju navedenih pooblastil. Ključno je, da varnostnik zasebnega varnostnega podjetja pooblastila uporabi v skladu z zakonom in le takrat, ko je to nujno potrebno, da se zavaruje premoženje, življenje ter ohrani varnost na varovanem območju.

Varnostnik je o uporabi ukrepov in drugih sredstev dolžan takoj obveščati policijo v primerih, če:

- osebo zadrži;
- uporabi fizično silo;
- uporabi sredstva za vklepanje in vezanje;
- uporabi plinski razpršilec;
- uporabi strelno orožje;
- je oseba pri uporabi ukrepov varnostnika telesno poškodovana (hkrati pa ji je dolžan nuditi prvo pomoč oziroma mora poskrbeti, da oseba dobi ustrezno strokovno pomoč).

Varnostnik tako o uporabi ukrepov oziroma o navedenih primerih obvešča policijo takoj, ko mu okoliščine to dopuščajo – policijo obvešča neposredno po telefonu ali pa posredno prek VNC. Preden pa varnostnik začne z obveščanjem policije, si pridobi podatke o osebah, zoper katere je uporabil ukrep, podatke o kraju in času izvedenega ukrepa, posledice in druge podatke.

Po zaključenem postopku je varnostnik v poročilo o dogodkih dolžan zapisati vse podatke o uporabi ukrepa ali drugega sredstva, opisati mora postopek obveščanja policije in njihovega ukrepanja.

Varnostni menedžer družbe za zasebno varovanje oziroma imetnik licence, pri katerem je varnostnik zaposlen, je dolžan oceniti zakonitost in strokovnost izvedenega ukrepa in v roku 48 ur na pristojno policijsko postajo pisno poročati o izvedenem ukrepu.

Zasebna varnostna družba obvešča policijo tudi o vseh varnostno tveganih dogodkih, med katere spadajo tudi aktivacije tehničnih alarmnih sistemov (protivlomna, protipožarna, »panik« tipke) in ob zaznanem kaznivem dejanju ali prekršku. Primer formalnega sodelovanja zasebne

varnostne družbe, ki upravlja naloge v finančni instituciji, je obveščanje policije v primerih izvajanja prevoza gotovine 5. razreda (višina gotovine, ki se prevaža, je višja od 4 000 000 evrov).

Posebej pa je opredeljeno varovanje t. i. kritične infrastrukture, ki se izvaja tako po zasebni varnostni družbi in hkrati s tehničnim varovanjem neposredno po alarmnem obveščanju na policiji.

V primeru čezmejnih prevozov gotovine je nujno potrebno formalno sodelovanje policije in zasebne varnostne družbe, ki sicer opravlja varovanje.

Velja pa omeniti, da varnostni management zasebnih varnostnih družb, ki opravljajo varovanje bank in hranilnic, vseskozi tudi na neformalni ravni sodeluje s policijo (Vačovnik, Interno gradivo, 2022).

5.4.3 Sodelovanje z drugimi institucijami

Banke in hranilnice lahko za izvedbo zakonsko predpisanih nalog pooblastijo tudi zunanje organizacije za konkretno opravljanje določenih nalog. Največkrat banke in hranilnice pooblastijo zakonsko pooblaščen zunanje organizacije s področja Zakona o varstva o požaru in Zakona o varnosti in zdravja pri delu. Banke in hranilnice sodelujejo tudi z drugimi organizacijami za zagotavljanje čiščenja, servisiranja, vzdrževanja in podobno. Za vse zunanje organizacije velja, da morajo pri opravljanju nalog v bankah in hranilnicah spoštovati vse zakonske, podzakonske, interne pravne akte, vključno s posebnimi navodili, ki veljajo za varnostno ogrožena območja. Pri nadzoru tega ima bistveno vlogo varnostni manager banke ali hranilnice (Vačovnik, Interno gradivo, 2022).

6 PRIMERI IZVEDBE NAPADOV NA VARNOSTNE SISTEME V FINANČNIH ISTITUCIJAH Z UPORABO IT

V novejšem času se z razvojem informacijske tehnologije (IT) ter množične uporabe spletnega poslovanja vedno pogosteje z uporabo vrhunskih računalniških znanj ter orodij »napada« neposredno IT bank in hranilnic z namenom pridobivanja protipravne premoženjske koristi. Del teh napadov so banke in hranilnice s svojimi notranjimi varnostnimi sistemi uspele omejiti. Nekaj primerov napadov pa se zaradi neprimernih ravnanj uporabnikov uspešno izvede na škodo komitentov. Banke in hranilnice v takšnih primerih sicer ne utrpijo večje škode, vseeno pa gre za varnostno tvegan dogodek, ki mora biti nemudoma ustrezno obravnavan (Bobovnik, 2020).

6.1 *Delovanje storilcev z uporabo črnega spleta*

Internet, kot ga poznamo, bi lahko razdelili na tri dele, in sicer:

- površinski splet,
- globoki splet,
- črni splet oziroma »dark net«.

Storilci običajno za izvrševanje napadov na banke in hranilnice ter njihove uporabnike uporabljajo predvsem črni splet. Črni splet je nastal okoli leta 1970 z ločitvijo od omrežja Agencije za napredno raziskovalno dejavnost (Arphanet). Črni splet je omrežje v internetu, do katerega lahko dostopamo le s posebno programsko opremo. Dostop je enostaven z uporabo spletnega brskalnika TOR. TOR za zagotavljanje anonimnosti uporablja vrste povezav s končnico .onion. Bistveno pri delovanju temnega spleta je, da vsebuje naslove, ki se ne pojavljajo na seznamu omrežij in ne odgovarjajo na zahteve poizvedb prek veljavnih IP naslovov. Ravno zaradi navedenega se črni splet pogosto uporablja za kriminalne aktivnosti (hekerje), deljenje datotek nelegalne programske vsebine in za ponudbo ter prodajo vseh vrst sicer prepovedanih predmetov. Ponudbe za prodajo in posredovanje se vršijo na t. i. »dark net market« oziroma ilegalnih spletnih trgovinah. Na črnem spletu je trenutno več ilegalnih spletnih trgovin, pri čemer moraš za dostop do njih imeti izklopljen program JavaScript. Za dodatno varnost uporabnikov je nujna uporaba šifriranja PGP. Trenutno so najpopularnejše ilegalne spletne trgovine TORREZ market, WORLD market in Dark0D Reborn Market. Za dodatno

varnost se za kupovanje prepovedanih stvari uporabljajo samo t. i. kriptovalute, kot so Bitcoin, Litecoin, Monero in druge.

Na črnem spletu se prodaja izredna velika količina ukradenih kreditnih kartic, kreditnih računov in tudi PayPal računov. Vsi ti podatki so ukradeni z vdori v IT sisteme bank, hranilnic, ponudnikov spletnih predplačniških računov in drugo. Na črnem spletu se je možno naučiti tudi, kako uporabiti ukradene podatke za nakupe.

Glede na množico ukradenih bančnih podatkov lahko sklepamo, da kriminalne aktivnosti t. i. hekerjev potekajo ves čas in da pri tem niso predmet napada samo banke in hranilnice, ampak tudi druge organizacije, katere tako ali drugače razpolagajo s podatki o bančnih računih, geslih, transakcijah (Temni splet, 2021; Bobovnik, 2020)

6.2 Izvrševanje spletnih goljufij

V diplomski nalogi bom omenila oblike izvrševanja t. i. spletnih goljufij, pri katerih storilci izkoristijo podatke o bančnih računih ter v nadaljevanju izvrševanja kaznivega dejanja iz napadenih bančnih računov pridobijo denarna sredstva, do katerih seveda niso upravičeni. Finančna institucija pri tem s svojim varnostnim sistemom (IT) izvršitev goljufije nikakor ne more preprečiti kakor tudi ne zaznati. Vsa odgovornost za ravnanje oziroma poslovanje po bančnem računu je na strani odgovornih oseb v podjetjih ali fizičnih oseb, ki so imetniki bančnih računov. Vse finančne institucije svoje uporabnike pri elektronskem bančnem poslovanju nenehno opozarjajo na nujna samozaščitna ravnanja. Za opustitev teh ravnanj finančne institucije ne morejo odgovarjati.

V nadaljevanju predstavljam oblike izvršitev spletnih goljufij, pri katerih storilci uporabijo bančne podatke oziroma jih pridobijo pred izvršitvijo kaznivega dejanja:

- vdori v poslovno elektronsko pošto (storilci prestrežejo elektronsko dopisovanje poslovnih subjektov in nato s spremembami obstoječih predloženih računov zagotovijo, da poslovni subjekt nakaže denarna sredstva na bančni račun, za katerega je prepričan, da je od poslovnega subjekta, s katerim sodeluje);
 - vdor v računalnik uporabnika v obliki nujenja lažne tehnične pomoči družbe Microsoft (storilci z lažnim prikazovanjem v telefonskem pogovoru uporabnika zavedejo, da mu omogoči tako imenovan oddaljen dostop do njegovega računalnika in s tem tudi pridobijo bančne podatke, s katerimi nato pridobijo denarna sredstva z bančnega računa uporabnika)
- in

- zloraba bančnih podatkov, pridobljenih po spletu (pri tej obliki storilci pri pripravljanju izvedbe spletnega nakupa kupca zavajajo tako, da svoje bančne podatke vnese v polja za plačilo, pri čemer se bančni podatki dejansko vnašajo v polja, ki jih je pripravil storilec, ki v nadaljevanju izvede spletni nakup z uporabo bančnega računa uporabnika, ki pa seveda kupljenega blaga nikdar ne dobi).

Iz opisanega izhaja, da morajo banke in hranilnice ves čas ocenjevati varnostna tveganja pri spletnem bančništvu iz razloga morebitnih napadov na IT in s tem odtujitvijo bančnih računov ter podatkov o uporabnikih teh računov (temni splet – »dark net«). Nenehno obveščanje, poučevanje in ozaveščanje bančnih uporabnikov glede možnosti zlorab pri elektronskem bančnem poslovanju in poslovanju na spletu pa lahko bistveno omeji možnosti spletnih zlorab z uporabo bančnih podatkov (Temni splet, 2021; Bobovnik, 2020).

7 NAJODMEVNEJŠI PRIMERI NAPADOV NA FINANČNE INSTITUCIJE IN VARNOSTNO OSEBJE PRI PREVOZU GOTOVINE

Predstavitev najodmevnejših primerov napadov na finančne institucije in/ali varnostno osebje pri prevozu gotovine za poslovanje finančnih institucij bo skupaj s statističnimi podatki bistven pokazatelj varnostnih tveganj pri delovanju finančnih institucij. Predstavitev bomo omejili na časovno obdobje od leta 2005 naprej, s tem da bomo predstavili samo odmevne oziroma posebne primere napadov, saj bomo tudi z manjšim številom predstavljenih primerov zadostili namenu predstavitve. Med medijsko objavljenimi primeri bom opravila izbor glede na predmet napada, delovanje storilcev in morebitno vpletenost varnostnega oziroma drugega osebja finančne institucije.

7.1 *Rop SKB – bančni sefi in trezorji*

31. 10. 2005 v poznih večernih urah je več storilcev vstopilo v del objekta SKB, d. d., v Ljubljani, kjer je imela banka trezorje in sefe, v katerih je hranila premoženje komitentov banke. Pri tem so storilci delovali na varnostno osebje, in sicer na način, da so oba varnostnika fizično onemogočili. Celo noč so nato odpirali in izpraznili več kot 427 sefov banke SKB in nato ob 6. uri z ukradenimi predmeti neovirano zapustili kraj dejanja. Sam način dostopa v prostore banke s sefi in trezorji je nedvomno izkazovala, da so storilci imeli t. i. notranje informacije tako glede prostega dostopa do sefov (uporabniški dostop) kot tudi glede izvedenega varovanja v objektu in zunaj njega. Rop sefov SKB banke še danes ni dokončno pojasnjen, prav tako ukradeni predmeti niso bili najdeni in vrnjeni banki oziroma komitentom banke. SKB, d. d., je oškodovanim komitentom banke izplačala odškodnine.

Mediji so z javnimi objavami več let spremljali policijsko preiskavo ter prav tako sojenje storilcem, ki so bili med večletno preiskavo identificirani. Dejstvo, da je v navedenem primeru šlo nedvomno za sodelovanje t. i. notranjega kadra, potrjuje tudi časovna eksponenta in izostanek materialnih dokazov (ukradeni predmeti).

Z vidika varnosti finančnih institucij pa je zgoraj predstavljen primer izkazal več varnostnih tveganj, ki niso bila pravočasno prepoznana in z ustreznimi ukrepi odpravljena (Roparja SKB banke v priporu – informacija z novinarske konference, 2012).

7.2 Izvršitev devetih ropov finančnih institucij na območju Slovenije s strani srbske kriminalne združbe

V časovnem obdobju od 9. 6. 2011 do vključno 20. 7. 2012 je na območju celotne Slovenije v krajših časovnih presledkih delovala kriminalna združba državljanov Republike Srbije, ki so izvrševali rope finančnih institucij z neposredno uporabo strelnega orožja na uslužbence finančnih institucij. Kriminalna združba je organizirano prihajala na območje RS, in sicer izključno z namenom izvršiti tudi do tri rope na finančno institucijo in z ukradenim denarjem takoj zapustiti območje RS. V kriminalni združbi je sodelovalo enajst mlajših oseb, ki so se pri izvrševanju ropov izmenjevali. Premoženjska škoda za finančne institucije, glede na javno objavljene podatke Policije, ni bila izrazito velika, in sicer iz razloga, ker so neposredno delovali na uslužbence finančnih institucij v času obratovanja in so rop morali izvršiti v zelo kratkem času. Ravno to pa je imelo za posledico, da so pri tem uspeli odtujiti zgolj omejeno količino denarnih sredstev (trenutno razpoložljivo pri uslužbencu).

Kriminalna združba je izvršila rope v poslovalnico Raiffeisen banke v Ljubljani, poslovalnico Pošte Slovenije v Mariboru, poslovalnico SKB, d. d., v Mariboru, poslovalnico Pošte Slovenije v Ljubljani, poslovalnico Pošte Slovenije v Kranju, poslovalnico Pošte Slovenije v Mariboru in poslovalnico Raiffeisen banke v Ljubljani. Kriminalna združba je prav tako izvršila rop v poslovalnici Pošte Slovenije v Semedeli in še en rop poslovalnice Pošte Slovenije v Mariboru, pri čemer pa je ostalo pri poskusu zaradi nedvomno strokovnega in učinkovitega delovanja varnostnega osebja, zaposlenih in ob veliki pomoči občanov – očividcev (Policija uspešno preiskala deset poštnih in bančnih ropov, 2013).

7.3 Izvršitev štirih ropov finančnih institucij s strani enega storilca ob uporabi pištole in kolesa z motorjem

V letih 2017 in 2018 je slovenski državljan izvršil štiri rope nad finančnimi ustanovami, pri čemer je deloval sam, pri izvršitvi uporabljal prevozno sredstvo kolo z motorjem in pištolo. Finančne ustanove je napadal v obratovalnem času z neposrednim delovanjem na zaposleno osebje, od katerih je s podkrepljeno grožnjo s pištolo zahteval izročitev gotovine. Zaradi uporabe motoristične čelade v času izvršitve dejanja in uporabe kolesa z motorjem za pristop in pobeg s kraja dejanja je bila identifikacija storilca težavna. Pri četrtem ropu v časovnem obdobju petih mesecev je bil storilec 8. 3. 2018 neposredno po izvršitvi ropa prijet s strani očitveca – policista v civilu, ki se je v času ropa slučajno – v prostem času nahajal v poslovalnici

finančne institucije Delavske hranilnice na Dunajski cesti v Ljubljani. V preiskavi se je izkazalo, da je isti storilec izvršil rop poslovalnice Delavske hranilnice v Ljubljani 20. 10. 2017, 5. 1. 2018 izvršil rop poslovalnice SKB na Dunajski cesti v Ljubljani in tudi rop poslovalnice Delavske hranilnice na Novih Fužinah 22. 1. 2018 v Ljubljani. Kot izhaja iz posredovanih podatkov medijem, je specialni storilec povratnik dejanja izvrševal sam, pri čemer je očitno predhodno z ogledi finančnih ustanov ugotovil, da so za izvedbo njegovega načina ropa najprimernejše poslovalnice finančne ustanove Delavske hranilnice, d. d., in SKB, d. d.

Glede na opisan način njegovega delovanja v prostoru finančne ustanove je bilo pomembno dejstvo višina steklenih pregrad pri bančnih okencih in neposreden dostop do njih.

Pri predstavljenem primeru velja izpostaviti, da pri izvršitvi ropa ni bilo uporabljeno strelno orožje in telesne poškodbe niso nastale. Reakcije zaposlenih in očividcev pa so temu pripomogle. Seveda je pri zaposlenih, ki so bili predmet neposrednega delovanja storilca, nastala tudi posledica predvsem na psihičnem zdravju, kar pa je mogoče s pravim pristopom tako v okviru finančne ustanove (premeščanje na delovnih mestih) kot ob nudenju psihosocialne podpore bistveno hitreje in z manj škodljivimi posledicami učinkovito sanirati (Pogumni ljubljanski policist ujel storilca, ki je oropal že več bančnih poslovalnic, 2018).

7.4 Izvršitev ropa vozila za prevoz denarja zasebne varnostne družbe

Pri pregledu primerov ropov na finančne ustanove in varnostno osebje pri prevozu denarja sem se odločila v predstavitev vključiti primer, ki se je zgodil v letu 2019. 21. 10. 2019 sta dva oborožena storilca nekaj pred 6. uro zjutraj, pred uvozom na avtocesto v bližini kraja Ljubečno pri Celju, oropala kombinirano vozilo zasebne varnostne službe, ki je v tem času prevažalo večjo vsoto gotovine. Pri izvršitvi ropa varnostno osebje ni bilo poškodovano. Storilca sta kraj dejanja zapustila z osebnim vozilom, ki sta ga sama ali ob sodelovanju morebitnih sotorilcev na območju Ljubljane uničila. Glede na samo izvedbo ropa in v nadaljevanju uničenje uporabljenega vozila, lahko sklepamo, da gre za načrtovan in dobro organiziran rop, pri čemer obstaja velika verjetnost, da sta storilca ali storilci razpolagali tudi z notranjimi informacijami glede izvedbe prevoza gotovine s strani zasebne varnostne službe ter vsoto gotovine, ki se prevažala. Čas, lokacija in način izvedbe kaznivega dejanja ropa je bil torej dobro premišljen in izveden v kratkem časovnem okviru. Pri tem varnostno osebje zasebne varnostne službe očitno ni povzelo nobenih aktivnosti za preprečitev ropa. Pridobljeni podatki pa očitno niso bili dovolj konkretni za takojšnje ukrepanje policije in izsleditev storilcev. V tem predstavljenem primeru

se izpostavi vprašanje, ali so prevozi gotovine s strani zasebne varnostne službe optimalno organizirani glede na oceno tveganja in ali je varnostno osebje dovolj dobro usposobljeno, da v primerih ropov uspešno uporabi tehnične oblike varovanja in s svojim pasivnim ukrepanjem podaljša časovni okvir izvrševanja ropov in s tem omogoči pridobitev bistveno več konkretnih podatkov za odkritje storilcev, z najmanjšimi možnimi posledicami za življenje in telo (Lopova zažgala BMW takoj po oboroženem ropu vozila za prevoz denarja, 2019).

7.5 Izvršitev dveh ropov poslovalnice Pošte z uporabo strelnega orožja in smrtjo uslužbenke Pošte

Kot zadnjega bom predstavila primer ropov dveh poslovalnic Pošte Slovenije, ki sta ju izvršila ista storilec istega dne. Pri izvršitvi drugega ropov je storilec uporabil strelno orožje – pištolo in z njo ustrelil uslužbenko Pošte, ki je zaradi tega umrla.

Oba ropov sta bila izvršena 21. 6. 2011, in sicer sta ista storilec najprej z uporabo strelnega orožja oropala poslovalnico Pošte v Divači. V nadaljevanju istega dne sta načrtovala in izvedla še ropov poslovalnice Pošte v Kresnicah, pri čemer je eden od storilcev od neposrednega delovanja odstopil, drug storilec pa je pri izvršitvi kaznivenga dejanja uporabil strelno orožje – pištolo in uslužbenko Pošte med prerivanjem smrtno poškodoval. Kot izhaja iz javnih objav v medijih, je uslužbenka Pošte potem, ko je navedeni ob grožnji s pištolo zahteval denar, njegovo zahtevo ignorirala in v nadaljevanju poskušala storilcu z glave sneti t. i. maskirno kapo, s katero je storilec prikrival svojo identiteto. Ob njenem aktivnem delovanju zoper storilca je storilec med prerivanjem sprožil strel in pri tem uslužbenko smrtno ranil.

Izpostaviti velja, da se je pri tem odmevnem in tragičnem primeru še enkrat več izkazalo, da je za omilitev posledic pri izvrševanju kaznivih dejanj ropov ob uporabi kakršnih koli pripomočkov (orožje, orodje, naprave, hladno orožje) bistvenega pomena ravnanje zaposlenih. Prav tako je nedvomno pomembno zagotavljanje prisotnosti več zaposlenih v poslovalnici in uporaba kakovostnega tehničnega varovanja, kar ima tudi pozitiven psihološki učinek na zaposlene ob morebitnem ropu. Protokol ravnanja zaposlenih ob takšnih primerih mora biti usmerjen v varovanje njihovih življenj, uporaba sistemov varovanja pa mora biti preprosta za zaposlene in v največji možni meri koristna za preiskovanje morebitnih varnostno ogrožajočih dogodkov (Roparjema pošte v Divači in Kresnicah nižja kazen, 2012).

8 STATISTIKA KAZNIVIH DEJANJ, POVEZANIH Z NAPADI NA FINANČNE USTANOVE IN DENAR

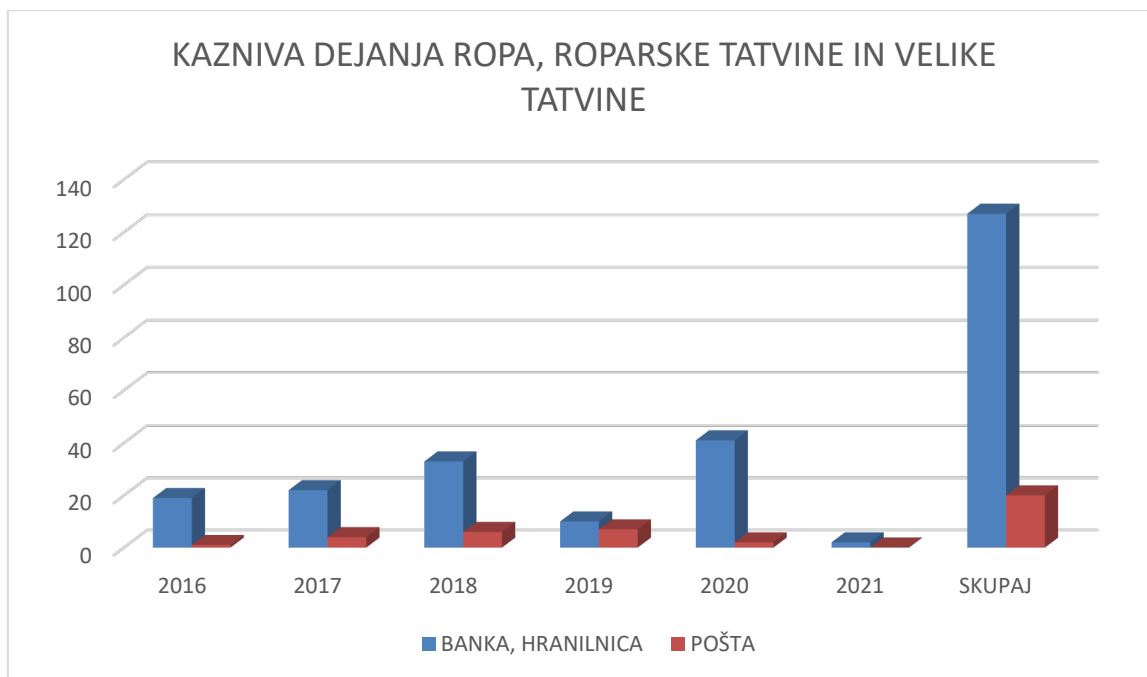
V nadaljevanju bom ob uporabi statističnih podatkov iz javno objavljenih Letnih poročil o delu Policije, za obdobje od leta 2015 do vključno 2020 (statistični podatki za leto 2021 še niso objavljeni), izdelala tabele, v katerih bom prikazala statistične podatke o izvršenih kaznivih dejanjih na finančne institucije, pri čemer bom vključila tudi izvršena kazniva dejanja, katerih predmet napada je bil bankomat (mreža bankomatov zagotavlja dvig gotovine in druge storitve uporabnikom po povezavi z bankami in hranilnicami). Iz istega vira bom pridobila tudi podatke o izvršenih kaznivih dejanjih z izvršitveno obliko, poimenovano spletne goljufije. Na podlagi pridobljenih podatkov bom izračunala delež kaznivih dejanj ter s pridobljenimi podatki potrdila sklepne ugotovitve na osnovi postavljenih hipotez.

Tabela 1: Kazniva dejanja rop, roparske tatvine in velike tatvine na prizoriščih bank (bankomati), hranilnice in pošte

LETO	NAPAD	BANKA, HRANILNICA	POŠTE
2016		19	1
2017		22	4
2018		33	6
2019		10	7
2020		41	2
2021		2	0
SKUPAJ		127	20

Vir: (Kriminaliteta, 2021)

Tabela prikazuje število kaznivih dejanj ropov, roparskih tatvin in velikih tatvin na prizoriščih bank (bankomati), hranilnic in pošt med leti 2016–2021. Iz tabele je razvidno, da je bilo veliko več kaznivih dejanj storjenih na bankah ter hranilnicah. Največ storjenih dejanj se je zgodilo v letu 2020.



Graf 1: Kazniva dejanja roba, roparske tatvine in velike tatvine na prizoriščih bank (bankomati), hranilnice in pošte

Vir: (Kriminaliteta, 2021)

Tabela 2 : Kazniva dejanja uporabe ponarejenega negotovinskega plačilnega sredstva

LETO \ NAPAD	UPORABA PONAREJENEGA NEGOTOVINSKEGA PLAČILNEGA SREDSTVA
2016	276
2017	193
2018	222
2019	251
2020	308
SKUPAJ	1250

Vir: (Kriminaliteta, 2021)

Tabela prikazuje kazniva dejanja uporabe ponarejenega negotovinskega plačilnega sredstva – zloraba bančnih kartic. Zajema petletno obdobje. Največ zlorab bančnih kartic se je zgodilo leta 2020.



Graf 2: Kazniva dejanja uporabe ponarejenega negotovinskega
plačilnega sredstva

Vir: (Kriminaliteta, 2021)

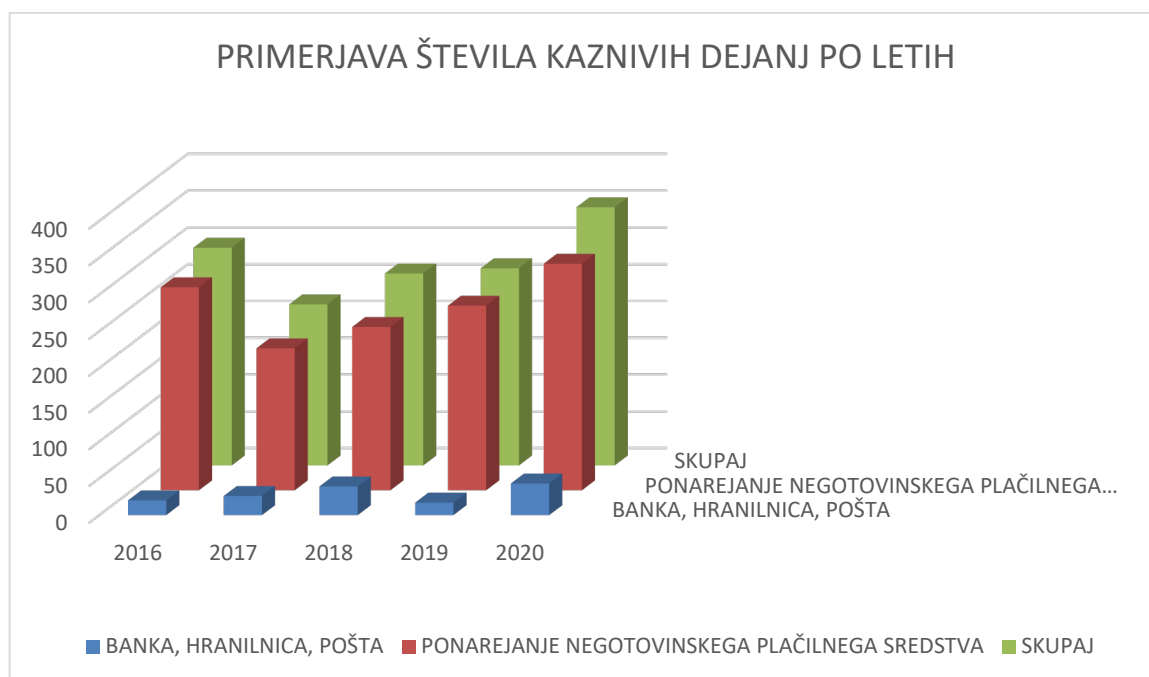
Tabela 3: Primerjava števila kaznivih dejanj, kjer je predmet napada objekt bank ali hranilnic ter pošt, s številom,
kjer je sredstvo storitve kaznivega dejanja spletno bančništvo

NAPAD LETO	BANKA, HRANILNICA, POŠTA	PONAREJANJE NEGOTOVINSKEGA P. SREDSTVA	SKUPAJ
2016	20	276	296
2017	26	193	219
2018	39	222	261
2019	17	251	268
2020	43	308	351

Vir: (Kriminaliteta, 2021)

Tabela 3 prikazuje število kaznivih dejanj, in sicer primerjavo med dejanjem, kjer je bil predmet napada banka, hranilnica ali pošta ter storitev kaznivega dejanja s spletnega bančništva (zloraba bančnih kartic). Tabela zajema obdobje od 2016 do 2020. Razvidno je, da je kaznivih dejanj

ponarejanja negotovinskega plačilnega sredstva občutno več kot kaznivih dejanj fizičnih napadov na finančne institucije. Izstopa leto 2020.



Graf 3: Primerjava števila kaznivih dejanj, kjer je predmet napada objekt bank ali hranilnic ter pošt, s številom, kjer je sredstvo storitve kaznivega dejanja spletno bančništvo

Vir: (Kriminaliteta, 2021)

Tabela 4: Primerjava petletnega obdobja kaznivih dejanj, kjer je predmet napada finančna institucija ali spletno bančništvo

KAZNIVO DEJANJE LETA	BANKA, HRANILNICA, POŠTA	PONAREJANJE NEGOTOVINSKEGA P. SREDSTVA
2016–2020	147	1250

Vir: (Kriminaliteta, 2021)

Tabela 4 prikazuje skupno število kaznivih dejanj v petletnem obdobju, in sicer primerjava med fizičnim napadom na finančne institucije in spletnega bančništva.



Graf 4 : Primerjava petletnega obdobja kaznivih dejanj, kjer je predmet napada finančna institucija ali spletno bančništvo
Vir: (Kriminaliteta, 2021)

9 SKLEP

Sodobne demokratične države, med katere spada tudi RS z zakoni in podzakonskimi akti, del varovanja premoženja vse pogostejše prepuščajo v izvedbo zasebnim varnostnim družbam. Izjeme so posebej določene, in sicer iz razlogov varovanja kritične infrastrukture in nujnosti za delovanje najbolj varnostno pomembnih funkcij države. Varovanje finančnih institucij je eno izmed področij, za katero je država z zakoni in podzakonskimi akti predpisala obveznost izvedbe varovanja po zasebni varnostni družbi. Istočasno je bilo treba zakonsko predpisati tudi ključne pogoje, ki jih mora izpolnjevati zasebna varnostna družba, da bi lahko izvajala varnostne naloge za finančno institucijo. Za izvajanje varovanja življenja in premoženja po zasebni varnostni družbi pa je bilo tudi nujno treba podeliti pooblastila varnostnikom, da bi lahko ob varnostno tveganih dogodkih ustrezno ukrepali. Ukrepi in izvajanje pooblastil, predpisanih po zakonu, pa je nujno povezano z usposabljanjem in pridobivanjem licence. Izpopolnjenost izvedbe tehničnega in fizičnega varovanja v 21. stoletju zagotavlja maksimalno varnost za finančno institucijo po problematiki tehničnega in fizičnega varovanja. Tehnično in fizično varovanje pa je samo del varnostnega sistema, potrebnega za celovito izvedbo varnosti v finančni instituciji. Vse pogostejša uporaba negotovinskih plačilnih sredstev, kot so razne plačilne kartice, aplikacije, nameščene na mobilne telefone, spletno bančništvo in delovanje po vsem svetu, zahteva vzpostavitev varnostnih sistemov, ki morajo 24 ur na dan, vse dni v letu, zagotavljati neprekinjeno spletno bančništvo in hkrati odvrčati nenehna varnostna tveganja. Varnostni sistem, ki skrbi za varnost informacijske tehnologije, je popolnoma ločen od varnostnega sistema fizičnega in tehničnega varovanja, pa vendar skupaj tvorita celovito varnostno mrežo, ki zagotavlja neprekinjeno bančno poslovanje. Zasebne varnostne družbe v RS še nimajo potrebnih specifičnih znanj in resursov, da bi lahko prevzele celovito varovanje v finančni instituciji, zato se finančne institucije za ta del varnostnega sistema poslužujejo najema zunanjih specifičnih izvajalcev in zaposlovanjem strokovnjakov s področja IT, s katerimi zagotavljajo potrebno varnost bančnega poslovanja. Vloga varnostnega managementa v finančni instituciji je ključna za povezovanje vseh varnostnih sistemov v operativno celoto in zagotavljanje vseh potrebnih resursov (tehničnih, kadrovskih in finančnih) po sodelovanju z upravo in lastniki. Vsaka finančna institucija za celovito rešitev varnostnega sistema skrbi sama, za vse pa je skupno to, da so vsi podatki o zgradbi, delovanju in protokolu ravnanj ob varnostnih dogodkih varovani kot tajnost in niso dostopni širši javnosti. Tako sem bila tudi sama opozorjena na to neizpodbitno dejstvo, med drugim tudi pri izvedbi intervjuja s pooblaščen

varnostno osebo v banki. Ne glede na to omejitev sem z vpogledom v dokumentacijo, intervijem in raziskovanjem ter pregledom javno dostopne literature dosegla zastavljen cilj.

Varovanje finančnih institucij na območju RS je z uporabljenimi najnovejšimi tehničnimi rešitvami z vseh področij tehničnega varovanja med delujočimi varnostnimi sistemi najbolj izpopolnjeno in s tem najmanj izpostavljeno varnostnim tveganjem tudi ob upoštevanju t. i. človeškega, saj še zmeraj velja, da je odgovorno ravnanje zaposlenega v varnostnem sistemu ključno za varnost celote. Bistveno za potrditev postavljene trditve je dejstvo, da se osnova varnostnega sistema vzpostavlja že ob načrtovani gradnji in se ob izvedbi faz samo dopolnjuje in nadgrajuje v celovito varnostno rešitev. Prav tako potrditev trditve izhaja iz opravljene analize statističnih podatkov Policije o obravnavanih kaznivih dejanjih, kjer je predmet napada objekt finančne institucije in denar. Pri statističnih podatkih ni bilo mogoče posebej izločiti napadov na bankomate, ki so po svoji specifikaciji objekt bančne institucije, ki pa je večinoma zgolj tehnično varovan.

Z analizo statističnih podatkov Policije o obravnavanih kaznivih dejanjih, povezanih z uporabo ponarejenega negotovinskega bančnega sredstva (bančne kartice), sem z gotovostjo potrdila trditve, da je največ negativnih varnostnih dogodkov povezanih z bančnim poslovanjem po spletu. Pri tej potrditvi velja izpostaviti, da je spletno bančništvo in z njim povezano varnostno tveganje možno uspešno obvladovati zgolj in samo ob doslednem samozaščitnem ravnanju uporabnika. Zavedati se je namreč treba, da se znotraj bančnega poslovanja izvaja več avtomatskih procesov, pri katerih ni možno sproti ocenjevati tveganj, zato mora uporabnik s svojim ravnanjem karseda omejiti možnost zlorabe bančnih podatkov, ki so ključni za postopek prenosa plačil.

Po raziskovanju, pregledu spletnih objav in z opravljenim intervijem sem potrdila trditve, da je varnostni sistem optimalen samo takrat, ko vsi uslužbenci prevzamejo varnostno zavest in se dosledno izvajajo vsa varnostno predpisana ravnanja in pravila delovanja. Varnostni management v finančni instituciji ima pri tem bistveno vlogo, saj je stičišče vse informacij o delovanju celovitega varnostnega sistema in s tem lahko opredeljuje programe usposabljanj za uslužbenca glede na dejstvo, s katerimi varnostnimi sistemi bo zaposleni imel opraviti pri opravljanju svojega dela v instituciji. Tudi pri tem je bistvenega pomena varovanje tajnih podatkov in s tem krepitev varnostne zavesti uslužbencev in s tem varnostih sistemov nasploh.

Ključno za delovanje varnostnih sistemov v finančnih institucijah je profesionalna izvedba vseh operativnih aktivnosti za preprečitev in odpravo varnostnih tveganj, pri čemer je nujno potrebno

zagotoviti tudi zunanje izvajalce, ki v skladu z določili varovanja tajnosti nudijo nujno potrebno, predvsem IT podporo delujočim varnostnim sistemom. Vsaj del varnostnih sistemov se glede na oceno tveganj redno dopolnjuje in posodablja, za kar je potrebno sodelovanje zunanjih in notranjih kadrovskih resursov s specifičnim znanjem. Glede na trenutno lastniško strukturo finančnih institucij v RS je za pričakovati, da se uporabne varnostne rešitve delijo in s tem se krepi celoten varnostni sistem. Zaenkrat zasebne varnostne družbe pri nas še niso sposobne zagotavljati celovitega varnostnega sistema v finančni instituciji. Opaziti pa je, da vsaj dve večji zasebni varnostni družbi trgu ponujata tudi druge storitve, pri čemer pa sem mnenja, da te storitve niso povezane z izpopolnjevanjem varnostnih sistemov in ne izkazujejo potreb po visoko kvalificiranem ozko specializiranem kadru, ki je nujno potreben za obvladovanje varnostnih tveganj predvsem pri spletnem bančništvu.

Varnostni sistem je najranljivejši ob opustitvi predpisanega ravnanja ali malomarnem ravnanju posameznika, kar se v zadnjih nekaj letih izkazuje ob povečanju zlorab pri bančnem poslovanju po spletu. Pridobivanje ključnih bančnih podatkov, s katerimi je v nadaljevanju možno pridobiti korist (dvig denarja, spletni nakup, plačilo tretji osebi in podobno) se ne izvaja samo v okviru IT finančne institucije, temveč tudi pri uporabnikih storitev. Uporabniki storitev smo spletno bančništvo in poslovanje po spletu zelo hitro prevzeli, pri čemer pa se nismo dovolj izobrazili, kako to varno početi. Zato je nujno treba izobraziti ne samo bančne uslužbence, temveč vse uporabnike, za kar se bi morale zavzemati tudi finančne institucije.

10 VIRI IN LITERATURA

Bučar, F. (2012). *Rojstvo države*. Ljubljana: Didakta.

Pravilnik o načinu prevoza in varovanja gotovine ter drugih vrednostnih pošiljk. (30. december 2016). Pridobljeno iz PIS: <http://pisrs.si/Pis.web/pregledPredpisa?id=PRAV12339>

Vačovnik, M. & Stergar, T. (2018). *Delovanje varnostno nadzornih centrov in intervencije*. Ljubljana: Zbornica za razvoj slovenskega zasebnega varovanja.

Savski, S., Rozman, J., Velički, D., Polutnik, B. & Hartman, J. (2017). *Varovanje ljudi in premoženja*. Ljubljana: Zbornica za razvoj slovenskega zasebnega varovanja.

Varovanje v sektorju bančništva. (brez datuma). Pridobljeno iz Aktiva: <https://www.aktiva-varovanje.si/resitve-varovanja/varovanje-v-sektorju-bancnistva/>

Protokolarno varovanje. (brez datuma). Pridobljeno iz Sintal: <https://www.sintal.si/storitve/fizicno-varovanje/varovanje-prireditve/protokolarno-varovanje/>

Letna poročila o delu policije. (brez datuma). Pridobljeno iz Policija: <https://www.policija.si/o-slovenski-policiji/statistika>

Deposit protection: why your money is protected. (19. oktober 2020). Pridobljeno iz N26: <https://n26.com/en-eu/blog/deposit-protection-why-your-money-is-protected>

Banke. (17. februar 2022). Pridobljeno iz Republika Slovenija: <https://www.gov.si/drzavni-organi/drugi-drzavni-organi/banka-slovenije/>

Banka Slovenije. (2022). Pridobljeno iz Moje Delo: <https://www.mojedelo.com/banka-slovenije-110>

Academia. (18. december 2015). *Gostujoče predavanje sodelavcev časopisa Večer*. Pridobljeno iz Academia Novice: <http://academia.si/novice/gostujoce-predavanje-sodelavcev-casopisa-vecer/>

Uredba o obveznem organiziranju varovanja. (26. oktober 2012). Pridobljeno iz PIS: <http://pisrs.si/Pis.web/pregledPredpisa?id=URED6002>

Odredba o določitvi programa strokovnega izpopolnjevanja za prevoz in varovanje gotovine ter drugih vrednostnih pošiljk. (6. julij 2012). Pridobljeno iz PIS: <http://pisrs.si/Pis.web/pregledPredpisa?id=ODRE2180>

Temni splet. (1. avgust 2021). Pridobljeno iz Wikipedia:
https://sl.wikipedia.org/wiki/Temni_splet

Banka Slovenije Evrosistem. (2017). Pridobljeno iz bsi: <https://www.bsi.si/o-nas>

Zakon o Banki Slovenije. (4. julij 2002). Pridobljeno iz PIRS:
<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2988>

Zakon o bančništvu. (8. junij 2021). Pridobljeno iz PIRS:
<http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO8319>

Zakon o gospodarskih družbah. (19. april 2006). Pridobljeno iz PIRS:
<http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4291>

Basel II. (12. marec 2013). Pridobljeno iz wikipedia: https://sl.wikipedia.org/wiki/Basel_II

Uredba o varovanju tajnih podatkov. (5. avgust 2005). Pridobljeno iz PIS:
<http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED3453>

Zakon o varstvu osebnih podatkov. (5. avgust 2004). Pridobljeno iz PIS:
<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906>

Zakon o varstvu pred požarom. (30. december 1993). Pridobljeno iz PIS:
<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO302>

Pravilnik o požarnem varovanju. (23. november 2007). Pridobljeno iz PIS:
<http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV7993>

Pravilnik o študiji požarne varnosti. (2. februar 1998). Pridobljeno iz Uradni list:
<https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1998-01-0527/pravilnik-o-studiji-pozarne-varnosti>

Zakon o zasebnem varovanju. (11. marec 2011). Pridobljeno iz PIS:
<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5760>

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih. (23. marec 2006).
Pridobljeno iz PIS: <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4284>

Zakon o varnosti in zdravju pri delu. (3. junij 2011). Pridobljeno iz PIS:
<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5537>

- Roparja SKB banke v priporu – informacija z novinarske konference.* (19. marec 2012). Pridobljeno iz Policija: <https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/62265-roparja-skb-banke-v-priporu-nk-2012>
- Policija uspešno preiskala deset poštnih in bančnih ropov.* (11. februar 2013). Pridobljeno iz Policija: <https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/66025-policija-uspesno-preiskala-deset-postnih-in-bancnih-ropov-2013>
- Pogumni ljubljanski policist ujel storilca, ki je oropal že več bančnih poslovalnic.* (13. marec 2018). Pridobljeno iz Policija: <https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-pu-ljubljana/91881-pogumni-lj-policist-ujel-storilca-ki-je-oropal-ze-vec-bancnih-poslovalnic-2018>
- Lopova zažgala BMW takoj po oboroženem ropu vozila za prevoz denarja.* (21. oktober 2019). Pridobljeno iz SIOL: <https://siol.net/novice/crna-kronika/neznanca-oropali-vozilo-za-prevoz-denarja-509988>
- Roparjema pošte v Divači in Kresnicah nižja kazen.* (21. november 2012). Pridobljeno iz Delo: <https://old.delo.si/novice/kronika/roparjema-poste-v-divaci-in-kresnicah-nizja-kazen.html>
- Kriminaliteta.* (2021). Pridobljeno iz Policija: <https://www.policija.si/o-slovenski-policiji/statistika/kriminaliteta>
- Vačovnik, M. (22. februar 2022). Interno gradivo.
- Begić, Đ. (6. oktober 2021). Intervju – Đani Begić, vodja službe varnosti Intesa Sanpaolo Bank. (N. Lamut, Izpraševalec)
- Bobovnik, D. (2020). *Analiza vsebin na temnem spletu*. Maribor: Denis Bobovnik.

11 PRILOGE

11.1 *Priloga 1: Intervju – Dani Begić, vodja službe varnosti Intesa Sanpaolo Bank*

1. Kakšne so Vaše kompetence, izobrazba in odgovornosti v finančni instituciji?

Zaposlen sem kot vodja službe varnosti v banki Intesa Sanpaolo. Na tem delovnem mestu sem pet let in vodim področje varnosti, v kar spada tako kot fizična, informacijska in zagotavljanje neprekinjenega poslovanja. Sicer sem po izobrazbi ekonomist, imam pa dvajset let delovnih izkušenj na področju IT (informacijske tehnologije). Moja odgovornost v banki je opredeljena v 34. členu: »Sklepa o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice.«

2. Katere varnostne sisteme imate? Kako se varnostni sistemi delijo glede na to, kdo z njimi upravlja?

Po svoji funkciji in tudi sicer smo zaposleni v banki zavezani k spoštovanju določil o varovanju informacij, opredeljenih kot tajni podatki, med katere vsekakor sodijo podatki o varnostnih sistemih v banki, zato podajam splošne in generične odgovore na zastavljeno vprašanje. V banki imamo v uporabi sisteme zagotavljanja fizičnega varovanja, različne tipe sistemov tehničnega varovanja, pristopnih kontrol in video nadzora, ki so v upravljanju fizične varnosti v banki. Ločeno se zagotavlja informacijska varnost, ki je v upravljanju službe informacijske tehnologije, in zajema:

- požarne pregrade – zunanje in notranje sisteme IPS med različnimi segmenti omrežij;
- protivirusne zaščite na vseh strežnikih in vseh delovnih postajah, ki morajo vključevati EDR povezljivost in upravljanje;
- zaščite pred naprednimi in vztrajnimi tipi napada, ki vključujejo t. i. peskovnike za sprožanje različnih tipov datotek in povezav in sprotno ter naknadno preverjanje vsebine in povezav in
- inskripcija sistemov vseh podatkov in vseh poti prenosa teh podatkov.

Pod varnostne sisteme, ki delujejo v naši banki, bi omenil tudi sistem izobraževanj za zaposlene v banki, ki jih izvaja Služba upravljanja s kadri. Po mojem mnenju je ta sistem ključnega

pomena za varovanje banke. Vsak zaposleni s svojim ravnanjem postavlja temelj varnosti banke, prav tako pa predstavlja tudi njen najšibkejši člen, v kolikor je izpostavljen.

3. Kakšno je Vašo mnenje glede pomena lastnika banke v povezavi z delovanjem varnostnih sistemov?

Lastnik banke najprej zagotavlja vse zakonske predpisane pogoje varnosti, ki so v veljavi na območju RS. Nato lastnik banke postavlja, preverja, nadzira delovanje upravljavskih funkcij banke (Uprava) skozi postavljene nadzore funkcije banke (Nadzorni svet) v dvotirnem sistemu upravljanja. V kolikor gre za enotirni sistem upravljanja banke, sta zgoraj opisani funkciji združeni v eno. V obeh primerih pa je dolžnost funkcije, da v skladu z zakonodajo in dobro prakso upravlja tveganja pri izvrševanju bančnih storitev. V današnjem času je upravljanje tveganj, ki izhajajo iz informacijske varnosti, ključnega pomena in se nenehno dopolnjuje. Zato uprava in nadzorni svet potrjujeta strategijo upravljanja s tveganji, ki izhajajo iz informacijske varnosti in neprekinjenosti poslovanja. S potrditvijo strategije se zagotavljajo vsa potrebna tehnična, finančna in druga sredstva, potrebna za zagotavljanje varnosti poslovanja.

Brez aktivne podpore lastnikov banke ni mogoče izgraditi učinkovitega varnostnega sistema.

4. Kateri varnostni sistemi finančne institucije se oddajajo zunanjim zasebnim izvajalcem?

V praksi se v zunanje izvajanje oddajo varnostni sistemi, ki zahtevajo posebne licence za izvajanje teh nalog; to so licence za izvajanje fizičnega varovanja, projektiranje sistemov tehničnega varovanja, vzdrževanje teh sistemov, projektiranje sistemov požarnega varovanja ipd. Zraven teh se v zunanje izvajanje oddaja penetracijo testiranja in »Security operations center« iz razloga, ker je za tovrstno izvajanje potrebno specifično znanje, ki ga banke s svojimi zaposlenimi ne zagotavljajo. Zunanje izvajalce najemamo za pomoč in svetovanje tudi pri uvajanju in upravljanju sistemov varovanja banke, pri čemer zunanji izvajalci niso nosilci teh dejavnosti, ampak zgolj pomoč pri sprejemanju rešitev.

5. Kakšni so sistemi varovanja delovanja finančne institucije po spletu?

Pojem delovanje banke po spletu je širok in ga zato razmejimo na dve pomembni področji. Področja delovanja plačilnih storitev po spletu in druga področja, kot so bančne spletne strani, druge storitve povezovanja in sodelovanja, oblačne storitve, prenosi in drugo. Obe področji sta za finančne institucije regulirani v Direktivi PSD2 in vseh tehničnih standardih, ki iz tega izhajajo. Omeniti je treba še NIS Direktivo. Zraven tega imamo tudi lokalne direktive, ki to

področje regulirajo. Izpolniti je treba tudi zahteve iz standardov, kot so ISO, NIST, COBID, PCI-DSS ... Vse te zgoraj naštetе zahteve, opisane v direktivah, ki jih banke moramo upoštevati kot osnovo našega sistema varovanja informacij, poleg »skladnostne varnosti«, imamo vpeljane sisteme varovanja informacij, ki vključujejo tehnične rešitve:

- preverjanje prometa (IPS, WAF);
- demilitariziranih con;
- nadzor nad prevarami;
- nadzor nad ranljivostmi s stalnim »skeniranjem« izpostavljenih naslovov;
- inskripcije in varne povezave.

6. Ali so kakšne potrebe po novih tehničnih rešitvah pri delovanju varnostnega sistema? Na kakšno obdobje oziroma na čigav predlog se tehnične sisteme spreminja?

Tehnične rešitve se stalno dopolnjujejo, in sicer na podlagi ocene prepoznanih tveganj in ocene vpeljanih mitigacijskih ukrepov. Spremembe v varovanju so stalnica, ker se tudi tveganja stalno razvijajo. Današnji »heker« ni več hišni računalničar, ampak gre za osebe, ki so s strani države financirani agenti s skoraj neomejenimi resursi. Namen delovanja »hekerja« ni več dokazovanje, da zmore vdreti v sistem, ampak destabilizacija sistema v državah, kar se lahko zelo hitro doseže z destabilizacijo finančnega trga.

Tudi stalno preverjanje odprtosti proti novo zaznamim ranljivostim (CVE) ali tveganjem na področju fizične varnosti je stalnica služb, ki za različna področja varnosti skrbijo. Nenazadnje pa je tu še izobraževanje, ki se mora prilagajati novostim in različnim profilom zaposlenih v banki.

Predloge oziroma potrebe po novih tehničnih rešitvah izhajajo iz vseh služb, ki so vzpostavljena v banki za namen varovanja v širšem pomenu. Predlogi se pošiljajo Upravi, še posebej takrat, če zahtevajo več neplaniranih sredstev v tekočem letu. Sicer se predlogi s planiranimi sredstvi predlagajo v izvedbo za prihodnje leto. Predlogi za tehnične rešitve sistema varovanja, ki zahtevajo kadrovske resurse, se usklajujejo med povezanimi službami banke in službo varnosti tako v fazi razvoja in implementacije. Razvoj tehničnih rešitev pri delovanju varnostnega sistema banke je stalni proces, ki se odvija v banki.

7. Kako poteka usposabljanje in nadziranje uslužbencev v finančnih institucijah v povezavi z delovanjem varnostnih sistemov?

Usposabljanje uslužbencev se izvaja interno skozi sprejete sisteme izobraževanj, ki so predlagani po preučitvi potreb. Izobraževanja se po potrebi izvedejo tudi pri zunanjih izvajalcih, posebej za določene profile uslužbencev, predvsem informatika, varnost in vodstvene funkcije.

Nadzor uslužbencev v banki zajema predpisana pravila in omejitve, ki so zapisane v pravilnikih, navodilih in politiki vodenja banke. Večji del nadzora pa je urejen kot tehnične omejitve na samih orodjih, ki jih uporabljajo uslužbenci pri svojem delu, kot primer so prepovedi uporabe USB ključkov brez uporabe nastavitev na programu za zaščito pred zlonamerno kodo. Prav tako se pri tem vključuje tudi funkcionalnost nadzora nad zunanjimi napravami delovne postaje zaposlenih v banki. Dodatno imamo vpeljan sistem sledenja dogodkov skozi sisteme zbiranja in shranjevanja logov, ki se naknadno vključijo v sisteme SIEM, ter v kontrole SOC-a v primeru sumljivih dogodkov. Pri tem ne gre za nadzor oseb, ampak za nadzor nad dogodki, ki odstopajo od običajnega delovanja in poslovanja; kot primer navajamo prijavo uporabnika z oddaljenim dostopom iz Ukrajine, čeprav drugače živi v Mariboru in do zdaj pri poslovanju še nikoli ni dostopal iz druge lokacije kot iz Maribora. V takšnem primeru se za nadzor uporabnika prosi, da potrdi svoj oddaljen dostop iz Ukrajine. S tem sicer posežemo v zasebnost uporabnika, vendar imamo zato utemeljen sum nevarnosti, ki upraviči izvedbo nadzora.

8. Kakšna je vloga policije pri izvajanju nalog varovanja v finančnih institucijah?

Vloga policije pri izvajanju nalog varovanja je predvsem pri izvedbi funkcije nadzora in obvladovanja tveganj na področjih kriminalitete, ki se lahko izkazuje v obliki fizičnih tveganj, prevar, goljufij in tudi zlorab IT sistemov. Fizično tveganje razumevamo kot nasilje, rop, vlom, grožnje in je delovanje policije izvedeno kot nadgradnja ukrepov zasebne varnostne službe. Tveganja prevar in goljufij na področju kartičnega poslovanja, finančnih transakcij in drugih malverzacij z uporabo spleta varnostne službe v banki težje odkrivajo in je zato vloga policije pri teh tveganjih posledično zelo pomembna (objave v medijih, preventiva, kazenski pregon).

9. Kdo vse sodeluje pri pripravi varnostnega načrta za izvedbo varovanja finančne institucije?

Priprava varnostnega načrta najprej vključuje izpolnitev regulatornih zahtev po specifičnih licencah za pripravo ocen tveganj in načrtov varovanja. V to se vključuje tako lastnik procesa ali produkta ter Služba varnosti finančne institucije. Prav tako pri pripravi varnostnega načrta za izvedbo varovanja banke sodeluje skoraj vsaka služba za svoje interno področje.

10. Kako ocenjujete ranljivost finančne institucije z vidika varnosti? Kateri del oziroma sistem finančne institucije je najranljivejši?

Finančne institucije so varnostno ranljive na vseh področjih, zato mora biti vpeljan sistem stalnega izboljšanja varnosti na vseh področjih. Nobeno področje ni samostojno v zagotavljanju varnosti finančne institucije in tudi ne moremo potrditi, da bi katero koli od teh področij bilo popolnoma varno. Razlog zato je, ker se okolje, v katerem poslujemo, nenehno menjuje in s tem omogoča nastanek novih varnostnih tveganj in nevarnosti za neprekinjeno poslovanje.

Najpomembnejši element sistema varovanja banke je človek, ki predstavlja tudi najranljivejšo točko sistema varovanja.

11. Kakšne so Vaše lastne izkušnje pri obvladovanju in reševanju varnostnih incidentov?

Varnostnih incidentov v smislu vdora v IT naša finančna institucija še ni evidentirala, čeprav smo zabeležili pogoste poskuse vdorov, ki pa so bili zaustavljeni na nivoju delovne postaje sistemov varovanja. V smislu onemogočanja storitev (DoS ali DDoS) smo poskuse uspešno odbili in zagotovili dosegljivost storitev našim uporabnikom. Incidentov na področju fizične varnosti smo se odzivali s postopkovnimi aktivnostmi, kot so obveščanje pristojnih, aktivacija kriznih skupin za predlaganje ukrepov, naknadno zavarovanje dokazov, analiziranje zbranih podatkov, predlogi izboljšav na kratki rok za zmanjšanje tveganja ter akcijski načrti za dodatna zmanjšanja ali za popolno odpravo nastalih tveganj. Za uspešnost obvladovanja in reševanja varnostnih incidentov je potrebno korektno in sprotno poročanje lastnikov banke odstraniti obvladovanja tveganj in stopnji preostalega tveganja (Begić, 2021).