Dragan Trivan Dejan Pavlović Vladimir Jovanović
Aleksandar Jakišić Ljubomir Radović Srđan Srdić

PRIRUČNIK ZA MENADŽERE KORPORATIVNE BEZBEDNOSTI

Beograd 2024.

PRIRUČNIK ZA MENADŽERE KORPORATIVNE BEZBEDNOSTI

Autori:
Dragan Trivan
Ljubomir Radović
Aleksandar Jakišić
Vladimir Jovanović
Dejan Pavlović
Srđan Srdić

Recenzenti:
Prof.dr Milan Milošević
Prof.dr Goran Matić
Prof.dr Denis Čaleta
Mr Alen Ostojić

Lektor:
Prof.dr Olja Arsenijević

Izdavač:
Srpska asocijacija menadžera korporativne bezbednosti SAMKB
Centar za multidisciplinarne studije CEMS

Za izdavača:
Prof. dr Dragan Trivan

Tehnički urednik: Zoran Bojanić

Štampa: Lampas, Beograd

Tiraž: 300

Godina: 2024.

ISBN 978-86-83040-00-1

Srpska asocijacija menadžera korporativne bezbednosti
Centar za multidisciplinarne studije

PRIRUČNIK
ZA MENADŽERE KORPORATIVNE BEZBEDNOSTI

Dragan Trivan
Aleksandar Jakišić
Dejan Pavlović
Ljubomir Radović
Vladimir Jovanović
Srđan Srdić

Beograd, 2024.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

005.934

PRIRUČNIK za menadžere korporativne bezbednosti / Dragan Trivan ... [et al.]. - Beograd : Srpska asocijacija menadžera korporativne bezbednosti SAMKB : Centar za multidisciplinarne studije CEMS, 2024 (Beograd : Lampas). - 244 str. : graf. prikazi, tabele ; 24 cm

Tiraž 300. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 227-244.

ISBN 978-86-83040-00-1

1. Триван, Драган, 1977- [аутор]
а) Корпоративна безбедност -- Менаџмент

COBISS.SR-ID 157255689

SADRŽAJ

SKRAĆENICE

AI (Artificial Intelligence) – veštačka inteligencija

BI (Business Intelligence) - poslovno obaveštajno delovanje

DPO (Data Protection Officer) - lice za zaštitu podataka o ličnosti

EU - Evropska unija

ENISA (European Union Agency for Network and Information Security) - Agencija Evropske unije za sajber bezbednost

IKT sistem - sistem informaciono-komunikacione tehnologije (podjednako se koriste pojmovi IT sistem, kompjuterski, računarski ili sajber sistem)

IoT (Internet of things) - internet stvari

ISO (International Organization for Standardization) – Međunarodna organizacija za standardizaciju

ISS – Institut za standardizaciju Srbije

KZ - Krivični zakonik Republike Srbije

KI - kritična infrastruktura

MUP - Ministarstvo unutrašnjih poslova Republike Srbije

NIST (National Institute of Standards and Technology) – Nacionalni institut za standarde i tehnologiju Ministarstva trgovine Federalne vlade Sjedinjenih Američkih Država

NFPA (National Fire Protection Association) – Međunarodna organizacija za prevenciju požara, električnih i srodnih opasnosti

RATEL - Regulatorno telo za elektronske komunikacije i poštanske usluge Republike Srbije

RS - Republika Srbija

SRB-CERT - Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima RS

CERT/CERT(Computer EmergencyResponse Team) - Centar za prevenciju bezbednosnih rizika u IKT sistemima

CER (Critical Entities Resilience) - otpornost kritičnog entiteta

CCSO (Chief Corporate Security Officer) - menadžer korporativne bezbednosti – označava poziciju najvišeg, izvršnog nivoa rukovođenja zaduženu za razvoj i primenu strateškog bezbednosnog okvira kojim se identifikuje, procenjuje i upravlja svim bezbednosnim rizicima na način koji doprinosi uspehu i otpornosti organizacije; za takvu poziciju se u teoriji i praksi nailazi na sinonime kao što su Director of Corporate Security / Chief Corporate Security Executive/ SeniorSecurity Executive / Chief Security Officer / Responsible Security Executive

CISO (Chief Information Security Officer) - menadžer bezbednosti informacija

PREDGOVOR

Najvažniji cilj i misija svake organizacije jeste efikasno funkcionisanje i ostvarivanje svrhe za koje je osnovana, bez obzira na vrstu delatnosti, osnivača ili vlasničku strukturu. Da bi se postigla dobit (profit), kao ciljna funkcija organizacija prevashodno privatnog sektora, ili realizovala svrhu zbog kojeg je oformljena kada su u pitanju organizacije iz javnog (državnog) sektora, nužno je da pravna lica budu dobro (ruko)vođena (eng. governance)[1], tj. da poslovne odluke koje se u njima donose budu najbolje moguće pri datim okolnostima. Osnovni preduslov za donošenje valjanih poslovnih odluka je dobro ustrojen sistem upravljanja/menadžmenta (eng. Management system). Kada je reč o pojmu korporativnog upravljanja, možemo konstatovati da ne postoji jedinstveno terminološko određenje, a za potrebe ovog Priručnika poslužićemo se definicijom koja je data u srpskom priručniku za korporativno upravljanje, gde se taj termin pojašnjava kroz „strukture i procese za vođenje i kontrolu privrednih društava“[2]. U tom smislu, korporativno upravljanje predstavlja skup mehanizama kroz koje organizacija funkcioniše kada je svojina odvojena od upravljanja, a radi se o skupu najvažnijih pravila po kojima deluje unutrašnja organizacija preduzeća (nadležnosti i procedure skupštine, upravnog odbora, top menadžmenta itd.). Vremenom je pojam korporativnog upravljanja prihvaćen kao zajednički naziv i vid najbolje prakse upravljanja organizacijom, ne samo korporacijom kao pojmom angloameričkog porekla, a koji „podrazumeva najrazvijeniji oblik poslovnih sistema u današnjim tržišnim privredama, a takođe i jedan od pravno regulisanih oblika trgovačkih društava, odnosno društava kapitala, za koji postoji uverenje da ima odgovarajuće prednosti u odnosu na druge pravne oblike tih subjekata“ [3]. Principe korporativnog upravljanja podjednako primenjuju i druge forme

1 Prikaz termina na engleskom jeziku u Priručniku dat je u funkciji preciznijeg određivanja pojmova oko kojih postoji nedoslednost prilikom upotrebe i nejednakost pri prevođenju na srpski jezik.

2 *Korporativno upravljanje – Priručnik*, IFC, Beograd, 2011., str. 6.

3 Trivan Dragan, *Osnovi korporativne bezbednosti*, Fakultet za poslovne studije i pravo Univerziteta «Union – Nikola Tesla», Beograd, 2017., str. 41.

organizacija, bez obzira da li pripadaju privatnom ili javnom sektoru[4], pa se u ovom Priručniku, uz sve specifičnosti, podjednako koriste pojmovi kao što su kompanija, preduzeće, privredno društvo, firma, institucija, poslovni subjekt ili najšire - pravno lice, odnosno jednostavno - organizacija.

Korporativna bezbednost[5] predstavlja opšteprihvaćen naziv za funkciju u čijem su delokrugu poslovi ukupne zaštite i jačanja otpornosti pravnog lica, i odnosi se na upravljanje bezbednošću pre svega, srednjih i velikih preduzeća (uključujući holdinge i koncerne, odnosno poslovna udruženja), dok bi male i mikro organizacije po veličini svakako trebalo da pri poslovanju postupaju u skladu sa principima koji su zastupljeni u poslovima korporativne bezbednosti. Da ne bi zbog svog naziva dovela do zablude, neophodno je naglasiti da menadžment korporativnom bezbednošću podrazumeva upravljanje poslovima ukupne bezbednosti i otpornosti kako privrednih društava (ortačko društvo, komanditno društvo, društvo s ograničenom odgovornošću, akcionarsko društvo) i drugih oblika organizovanja u smislu *Zakona o privrednim društvima*[6], tako i ostalih pravnih lica, odnosno organizacija sa priznatom pravnom sposobnošću, bez obzira na veličinu i delatnost, nezavisno da li pripadaju javnom ili privatnom sektoru, tj. da li su profitnog ili neprofitnog karaktera. S obzirom da su u domaćoj i međunarodnoj bezbednosnoj teoriji i praksi prisutne razlike u pojmovnom određivanju korporativne bezbednosti, možemo reći da ne postoji jedinstvena definicija ove discipline nauke o bezbednosti, ali postoji univerzalni stav da predstavlja neophodnu poslovnu funkciju i sastavna je komponenta najvišeg nivoa menadžmenta organizacije.

Funkcija korporativne bezbednosti ima za zadatak da na efikasan način kompaniju čini što bezbednijom i otpornijom, relaksirajući na taj način top menadžment i ostale zaposlene pritiska od pretnji i opasnosti, koji u takvom okruženju mogu da usmere svoj rad u pravcu ostvarenja primarne misije i ciljeva organizacije. Težnja ka ostvarivanju sveukupne bezbednosti i otpornosti organizacije uz optimizaciju troškova jeste generalni cilj funkcije korporativne bezbednosti, koja mora da razume poslovanje organizacije i da uskladi bezbednosne sa poslovnim procesima. Uspešne kompanije sve više usvajaju stav da se korporativna bezbednost ne razlikuje od bilo

4 Korporativno upravljanje je prepoznato u Strategiji nacionalne bezbednosti Republike Srbije, u delu ekonomskog razvoja i ukupnog prosperiteta Republike Srbije, gde se kao mera unapređenja profitabilnosti preporučuje uvođenje modela korporativnog upravljanja i u javnim preduzećima.

5 Pojedini autori korporativnu bezbednost poistovećuju sa pojmom bezbednost poslovanja (eng. enterprise security).

6 "Službeni glasnik RS", br. 36/2011, 99/2011, 83/2014 - dr. zakon, 5/2015, 44/2018, 95/2018, 91/2019 i 109/2021.

koje druge funkcije - koja prihvata izazove vezane za savremeno poslovanje, vodeći računa o promenljivom poslovnom okruženju.

Imajući u vidu vlasničku strukturu i organizacioni aspekt, korporativna bezbednost predstavlja i segment privatne bezbednosti, time i činilac nacionalne bezbednosti. Delujući na očuvanje i jačanje ukupnog poslovanja svojih organizacija, korporativna bezbednost najviše od svih segmenata privatne bezbednosti, posrednim putem, utiče na ekonomski razvoj društva, a jedan od osnovnih preduslova očuvanja globalne stabilnosti je upravo obezbeđivanje ekonomske stabilnosti. Doprinos korporativne bezbednosti u jačanju nacionalnih interesa koji imaju ekonomski značaj je neupitan, ali ćemo se složiti sa stavovima autora koji ističu da raspoložive korporativne bezbednosne sposobnosti nisu adekvatno iskorišćene, niti su adekvatno zastupljene u sistemu nacionalne bezbednosti naše zemlje[7]. Korporativna bezbednost pripada nedržavnom sektoru bezbednosti koji je „širi pojam od privatnog sektora bezbednosti, jer pored delatnosti privatnih firmi i agencija za pružanje različitih bezbednosnih usluga na komercijalnoj osnovi, obuhvata i specifične poslove korporativne bezbednosti koji se sprovode od strane unutrašnjih organizacionih jedinica i samostalnih izvršilaca u korporacijama, javnim preduzećima i drugim poslovnim subjektima, bez spoljnog angažovanja nadležnih državnih službi i usluga privatnih bezbednosnih kompanija po modelu outsourcing-a“[8].

Živimo u vremenu sve bržih, dramatičnijih i kompleksnijih promena koji diktiraju i utiču na promenu percepcije bezbednosnih rizika, što neizostavno vodi ka promeni shvatanja i primene zaštitnih i kontrolnih mera u smeru predvidljivosti i prilagodljivosti. Iz razloga što nije više dovoljno samo adekvatno zaštiti organizaciju i njeno poslovanje, neophodno je da korporativna bezbednost izgradi sistem koji će imati sposobnost da napade detektuje, da na njih adekvatno odgovori i da se od njih što pre oporavi, omogućavajući nastavak procesa i kontinuitet poslovanja. Dakle, pored upravljanja merama prevencije i zaštite do različitih oblika tradicionalnih i savremenih pretnji, opasnosti i izazova, funkcija korporativne bezbednosti integriše kontrole za stvaranje što veće otpornosti organizacije[9] i omogućavanje kontinuiteta

7 Lečić Boriša, „Place and role of corporate security in the national safety system“, In: Trivan Dragan, *Contemporary Concept of Corporate Security*, Faculty of Business Studies and Law, University „Union-Nikola Tesla“, Belgrade & Austrian Institute for European and Security Policy/AIES Wien & Institute for Corporative Security Studies, ICS, Ljubljana, 2018., pp. 175 - 191.

8 Trivan Dragan, *Osnovi korporativne bezbednosti*, op. cit. str. 32.

9 Kao što se ne može postići apsolutna bezbednost, tako organizacije mogu biti samo manje ili više otporne jer ne postoje apsolutne mere, niti konačni ciljevi. Otpornost organizacije se može definisati kao sposobnost organizacije da apsorbuje i prilagođava se u promenljivom okruženju

poslovanja u slučaju bezbednosnih incidenata, događaja i kriza, posebno u uslovima raznovrsnog i sve agresivnijeg konkurentskog delovanja, kao i uticaja klimatskih promena. Dobar primer ukazivanja na značaj jačanja otpornosti organizacije može se videti u tzv. *CER direktivi EU* kojom se uređuju mere u cilju postizanja visokog nivoa otpornosti kritičnih subjekata (Directive (EU) 2022/2557)[10], a koji treba da budu u poziciji da ojačaju svoju sposobnost da spreče, reaguju, da se odupru, ublaže, apsorbuju, prilagode i oporave od incidenata koji imaju potencijal da poreme-te pružanje osnovnih usluga. Slično je i sa tzv. *DORA uredbom* (Regulation (EU) 2022/2554)[11] kojom se uređuje digitalna otpornost finansijskog sektora, a kojom se zahteva ne samo izgradnja adekvatnog sistema prevencije i zaštite IKT sistema, već i uspostavljanje mera odgovora i oporavka u cilju obezbeđivanja kontinuiranog pru-žanja finansijskih usluga i njihov kvalitet, bez obzira na napade, prekide i poreme-ćaje.

Iako se stav o neophodnosti postojanja adekvatne funkcije korporativne bez-bednosti polako i nezaustavljivo menja i razvija u pravcu sve većeg prihvatanja od strane raznorodnih organizacija, i dalje je prisutno (pogotovo na prostoru našeg re-giona) prevaziđeno poimanje poslova bezbednosti, pre svega svođenjem na poslove fizičko-tehničke zaštite, kao i da se funkcija posmatra isključivo kroz prizmu troška. Ključna stvar u prevazilaženju ovakvog mišljenja jeste ukazivanje i dokazivanje, pre svega vlasnicima i najvišem rukovodstvu, da rezultati i benefiti koje korporativna bezbednost donosi omogućavaju organizaciji ne samo povraćaj investicija koje su uložene, nego i ostvarivanje dodatne vrednosti, uz omogućavanje realizacije misi-je i poslovnih ciljeva, kao i ostvarivanje konkurentske prednosti. Menadžer korpo-rativne bezbednosti (CCSO) adekvatnom kulturom komunikacije i upravljanjem bezbednosnim rizicima na način koji je orijentisan na ostvarivanje rezultata, mora da pokaže i dokaže da je organizacija bezbednija, efikasnija i otpornija, a kako bi vlasnik, odnosno generalni menadžer, kao i drugi članovi top menadžmenta[12] kor-poracije sa liderske pozicije uvažavali potrebu za planiranjem i upravljanjem bez-bednosnim potrebama i inicijativama. Veoma je bitno da CCSO radi na uspostavlja-nju jake korelacije poslova bezbednosti sa misijom, vizijom i strategijom poslovanja,

(više u: *ISO 22316:2017, Security and resilience - Organizational resilience - Principles and attributes*).

10 *OJL 333, 27.12.2022*, pp. 164–198 (The Critical Entities Resilience Directive), Brussels, 27 December 2022.

11 *OJL 333, 27.12.2022*, p. 1 (The Digital Operational Resilience Act), Brussels, 27 December 2022.

12 Grupa ljudi koja usmerava i kontroliše organizaciju na najvišem nivou, i ima moć da delegira ovlašćenja i obezbedi resurse unutar organizacije.

odnosno njenom efikasnošću i poslovnom etikom, robnim markama, uslugama i drugim vrednostima.

Postoji mnogo puteva za izgradnju uspešnog sistema menadžmenta korporativnom bezbednošću. Ne postoji univerzalno rešenje za svaku kompaniju i potrebno je uzeti u obzir granu industrije u kojoj se posluje, tradiciju, organizacionu hijerarhiju, korporativne prioritete i mnoge druge faktore. Kojim god putem da se krene, snažno vođstvo je ključ, i lideri (menadžeri korporativne bezbednosti) moraju biti u stanju da komuniciraju u skladu sa poslovnim ciljevima i da pronalaze rešenja za prevazilaženje izazova na „terenu" i prilikom implementacije potrebnih promena. Integracija i usklađivanje svih poslova bezbednosti, mera i kontrola koje proizilaze iz tih poslova, kao i njihovo usklađivanje sa zakonskim obavezama, zahtevima primenjenih standarda i preporuka, a u kontekstu specifičnosti i potreba organizacije, predstavlja ključni zadatak izgradnje i održavanja adekvatnog sistema menadžmenta korporativnom bezbednošću. Funkcija korporativne bezbednost ne sme postati sama sebi cilj ili, još gore, kočničar razvoja organizacije, a neophodno je da razume kontekst organizacije, njene potrebe i očekivanja zainteresovanih strana. Bitno je imati u vidu dimenziju subjektivnog osećaja koji implementirani sistem bezbednosti ostavlja na najviše upravljačke organe korporacije, kao i na sve zaposlene. Taj osećaj tzv. sigurnosti (spokojstva) odražava poverenje u mere i kontrole koje smo primenili da bismo zaštitili sve vrednosti organizacije i obezbedili dalje poslovanje.

Šta našoj organizaciji može da se desi negativno/štetno sa aspekta bezbednosti i zašto? Koja je verovatnoća da se opasnosti ili pretnje ostvare, iskoriste ranjivosti? Koje će biti negativne posledice po poslovanje u slučaju ostvarenja pretnji, nastupanja opasnosti ili zloupotrebe ranjivosti? Da li je moguće i kako da se spreči ili barem ublaži šteta i gubici i tako doprinese očuvanju kontinuiteta poslovanja i profitabilnosti? Da li smo razvili bezbednosnu svest, uvežbali i testirali sisteme i postupke, i da li smo planirali kontinuitet poslovanja i pripremili se na incidente ili za stanje krize? Ovo su samo neka od pitanja na koje je Priručnik ponudio odgovore ili bar dao smernice za njihovo pronalaženje, ukazujući na neophodnost baziranja primenjenih mera i kontrola na stalnom procesu procene bezbednosnih rizika, kao i izgradnji i unapređenju adekvatnog sistema upravljanja korporativnom bezbednošću.

Priručnik upućuje na osnovne stavove i mišljenja akademskih krugova, kao i na obaveze koje proizilaze iz pozitivnih zakonskih propisa, a ukazuje na standarde, preporuke, druge izvore i značajne primere iz prakse koji su u vezi sa poslovima korporativne bezbednosti, a koji mogu menadžerima korporativne bezbednosti i drugim

zainteresovanim licima da olakšaju donošenje odluka o merama i kontrolama pri izgradnji celovitog sistema bezbednosti. Uzimajući u obzir i svesni činjenice postojanja različitih delatnosti i industrijske prakse, pokušali smo da navedemo najbolje primere koji se odnose na poslove korporativne bezbednosti, ujedno navodeći različite međunarodne, nacionalne, sektorske/granske, kao i smernice i standarde priznatih strukovnih udruženja, koji mogu biti od koristi u izgradnji celovitog sistema bezbednosti, a koji neophodno sadrže mere i kontrole kojima se diže nivo otpornosti organizacije na sve izazove, opasnosti, pretnje i ranjivosti, kao i upravlja rizicima koji su u vezi sa njima. Standardi[13] predstavljaju pretočenu i sistematizovanu najbolju praksu, a njihov sve veći značaj, pa i obavezu implementacije onih koji se odnose na bezbednost i otpornost, možemo videti na primeru domaćih, kao i propisa EU, Sjedinjenih Američkih Država, Kanade i drugih visoko razvijenih država. Primera radi, *Zakon o privatnom obezbeđenju*[14] ukazuje na obavezu sprovođenja procesa procene rizika u zaštiti lica, imovine i poslovanja po zahtevima i na način propisan važećim srpskim standardom u oblasti privatnog obezbeđenja, a ranije pomenuta tzv. CER direktiva EU kojom se uređuje otpornost kritičnih entiteta, navodi da države članice treba da podstiču upotrebu evropskih i međunarodnih standarda i tehničkih specifikacija relevantnih za mere bezbednosti i otpornosti. Podrazumevajući i značaj standardizacije u pogledu interoperabilnosti tehnologija, standardi su od suštinskog značaja za obezbeđivanje ujednačenog kvaliteta u pružanju bezbednosnih usluga, što je Evropska Komisija istakla u *Politici industrije bezbednosti - Akcionom planu za inovativnu i konkurentnu industriju bezbednosti*[15].

Sa idejom da bude koncizan, sistematičan i prikladan za upotrebu u praksi, Priručnik je namenjen, pre svega, menadžerima korporativne bezbednosti pri njihovom svakodnevnom radu, a zbog svoje sadržine može koristiti ostalim izvršnim menadžerima u kompanijama, rukovodiocima drugih nivoa, kao i široj stručnoj javnosti, ali i studentima i drugim licima zainteresovanim za oblast korporativne bezbednosti.

Nadamo se da će ovo izlaganje olakšati rad menadžera korporativne bezbednosti u praksi, ali i pomoći ostalim zainteresovanim licima da u svojim organiza-

13 Institut za standardizaciju Srbije određuje standard kao dokument koji obezbeđuje uslove, specifikacije, smernice ili karakteristike koje se mogu koristiti kako bi se osiguralo da materijali, proizvodi, procesi i usluge odgovaraju svojoj svrsi. Standardi se utvrđuju konsenzusom, a odobravaju ih priznata tela. Koriste se širom sveta, i to ne samo u visokorazvijenim, već i u zemljama u razvoju (https://iss.rs/sr_Cyrl/shta-je-standard_p13.html) 30.1.2024.

14 „Službeni glasnik RS", br. 104/2013, 42/2015 i 87/2018.

15 *EC COM(2012)417 final*, European Commission, Brussels, 26.7.2012.

cijama iniciraju i implementiraju procese, mere i kontrole iz funkcije korporativne bezbednosti, i na taj način u značajnoj meri zaštitite poslovanje njihove kompanije, kao i omoguće njen dalji rast i razvoj, bez obzira na veličinu organizacije, delatnost ili svojinske odnose. Naglašavajući prednost integrisane i na holistički način primene poslova korporativne bezbednosti, prepuštamo sudu vremena ocenu uspešnosti izlaganja, ostajući otvoreni za sve dobronamerne predloge, primedbe i sugestije koji budu dolazili od čitalaca, što će predstavljati veliku pomoć u eventualnoj kasnijoj doradi ovog Priručnika.

Prvo poglavlje

Ugrožavanje bezbednosti i otpornosti korporacije

Sadržaj poglavlja

Ranije navedena nejednakost i nedoslednost pri prevođenju i korišćenju bezbednosnih pojmova u pozitivnim propisima, domaćim bezbednosnim standardima, ali i stručnoj literaturi, može da oteža i shvatanje pojma “ugrožavanje“, a kasnije i njegovu praktičnu upotrebu pri obavljanju poslova korporativne bezbednosti. Kako korporativna bezbednost obuhvata spektar poslova, i kako je potrebno objedinjeno identifikovati sve izvore, nosioce i oblike ugrožavanja, neophodno je sagledati šta se sve pod ugrožavanjem organizacije podrazumeva, odnosno od čega je potrebno da je zaštitimo, kao i da razvijemo mehanizme koji će ojačati otpornost i omogućiti nastavak poslovanja, odnosno ostvarivanje opredeljenih ciljeva i misije organizacije.

Ne ulazeći u različita razmatranja pojma ugrožavanja koji su zastupljena u domaćoj i stranoj stručnoj literaturi, možemo navesti da relevantni srpski standard u zaštiti lica, imovine i poslovanja *SRPS A.L2.001*[1] određuje ugrožavanje kao

> *"stanje potencijalne opasnosti u kojem postoji kapacitet da izazove negativne posledice".*

Upravo izvori koji mogu da proizvedu ove negativne posledice ili štetu po bezbednost i otpornost korporacije mogu biti, pre svega, *društveni*, sa čovekom kao nosiocem ovog izvora ugrožavanja, koji svojim namernim ili ne namernim delovanjem (činjenjem) ili propuštanjem da uradi dužnu radnju (nečinjenjem) može da ugrozi organizaciju. Mogući izvor negativnih posledica jeste i *priroda*, koja svojim negativnim delovanjem može u većoj ili manjoj meri tangirati bezbednost lica, imovine i poslovanja, i na čije uzroke, za razliku od delovanja čoveka, ne možemo da utičemo. Iako projektovani, izgrađeni i održavani od strane ljudi, *tehničko-tehnološki* kapaciteti predstavljaju zaseban izvor ugrožavanja, uz napominjanje mogućnosti postojanja *kombinovanog* učinka tri prethodno navedena izvora ugrožavanja. Dužnost i zadatak funkcije korporativne bezbednosti jeste da sve navedene izvore koji utiču na štićene vrednosti[2] (nominalne/materijalne ili nenominalne/nematerijalne prirode) sveobuhvatno identifikuje i tretira.

Pre nego što ukažemo na oblike ugrožavanja, iz praktičnih razloga je potrebno naglasiti da ljudi, odnosno fizička lica, shodno odnosu koji imaju sa korporacijom, mogu predstavljati unutrašnje (interne), spoljašnje (eksterne) i kombinovane nosioce društvenog izvora ugrožavanja.

Unutrašnje ili interne nosioce društvenog izvora ugrožavanja čine svi zaposleni koji sa korporacijom imaju zaključen ugovor o radu na određeno ili neodređeno vreme, odnosno lica koja su po drugom zakonskom osnovu angažovani na rad van radnog odnosa. Iz razloga poznavanja unutrašnjih prilika, procesa, a naročito zbog pristupa tzv. osetljivim korporacijskim informacijama, zaposleni kao unutrašnja potencijalna opasnost u većini slučajeva su identifikovani i ocenjeni kao visoko rizični sa aspekta bezbednosti. Insajdere, kao posebnu kategoriju unutrašnjih izvršilaca zlonamernih dela, počelo je da prepoznaje i domaće zakonodavstvo, a zloupotreba

1 *SRPS A.L2.001:2008, Društvena bezbednost - Usluge privatnog obezbeđenja – Rečnik,* Institut za standardizaciju Srbije, Beograd, 2008.

2 Srpski standard za procenu rizika u oblasti privatnog obezbeđenja definiše termin „štićene vrednosti (protectedasset)" kao „elemente organizacije od značaja za njeno postojanje i funkcionisanje".

insajderskih informacija je ikažnjivo kao krivično delo *Zakonom o tržištu kapitala*[3], kao i *Zakonom o digitalnoj imovini*[4]. Insajderi su, takođe, prepoznati i u različitim bezbednosnim standardima koji ukazuju na neophodnost sprovođenja procene od insajderske pretnje, gde su primera radi, u standardu koji daje smernice za upravljanje rizicima bezbednosti informacija *ISO/IEC 27005*[5], insajderi određeni kao jedan od pet vrsta izvora koji potiču od ljudi, i na koje je potrebno obratiti posebnu pažnju, a obuhvataju sledeće zaposlene:

- slabo obučene;
- nezadovoljne;
- zlonamerne;
- bivše zaposlene;
- zaposlene koji dela čine iz nehata.

Motivi za insajdersko delovanje mogu biti različiti, od znatiželje i povređenog ega do ideoloških razloga i finansijske ili druge koristi, a posedovanje programa za praćenje i vrednovanje pokazatelja insajderskih pretnji predstavlja jednu od osnovnih mera u zaštiti korporacije od njenog štetnog uticaja.

U spoljašnje ili eksterne nosioce društvenog izvora ugrožavanja ubrajaju se sva fizička lica koja shodno *Zakonu o radu*[6] nisu ni po jednom osnovu angažovana od strane korporacije. Ovim nosiocima pripadaju fizička lica koja, obično namernim delovanjem, žele da u svoju ili korist drugog lica, načine negativne posledice po korporaciju. U vremenu u kome je outsourcing visoko zastupljen pri poslovanju, možemo reći da specifičnu kategoriju eksternih nosioca čine zaposleni kod pravnih lica ili preduzetnika koji pružaju određene usluge korporaciji, pa su samim tim, kao i zaposleni koji čine interne nosioce, uključeni u mnoge procese i imaju određeni uvid i pristup različitim poslovnim informacijama korporacije, uključujući i one poverljive. Sličnu poziciju mogu imati i zaposleni kod pravnih lica ili preduzetnika koji sa korporacijom imaju određeni ugovorni odnos za potrebe pružanja usluga ili isporuke dobara (dobavljači, kupci, serviseri i drugi). U novije vreme posebnu kategoriju eksternih nosioca društvenog izvora ugrožavanja čine lica koja rade za organizacije

3 "Službeni glasnik RS", br. 129/2021.

4 "Službeni glasnik RS", br. 153/2020.

5 *ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management*.

6 "Službeni glasnik RS", br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - US, 113/2017 i 95/2018 - Autentično tumačenje.

angažovane i sponzorisane od strane pojedinih država, naročito angažovane na polju sajber kriminala i industrijske špijunaže.

Kombinovane nosioce društvenog izvora ugrožavanja zajednički čine interni i eksterni nosioci, odnosno zaposleni i lica koja nisu u radnom odnosu, a čije zajedničko delovanje, umišljajna sinergija može da dovode do negativnih posledica, tj. štete po korporaciju, odnosno njene vrednosti.

Svi navedeni nosioci mogu da ugroze korporaciju, odnosno mogu da budu izvor rizika kroz svoje pojavne slučajeve[7] i oblike, koji u osnovnom smislu mogu biti u formi pretnji. Zbog sveukupnog sagledavanja faktora ugrožavanja svakako je potrebno identifikovati i opasnosti i ranjivosti koje su prisutne u korporaciji, a u najširem smislu i izazove, o čemu će kasnije biti više reči. Svaki potencijalni izvor, nosilac i oblik ugrožavanja koji nije u početku prepoznat iz bilo kojeg razloga i zato ne bude obuhvaćen procesom procene rizika (kao osnovnim i početnim korakom u određivanju mera zaštite i izgradnji sistema upravljanja korporativnom bezbednošću) predstavlja konstantni i skriven ugrožavajući element po korporaciju.

Zakonska regulativa i bezbednosni standardi (bilo da se odnose na bezbednost informacija, kontinuitet poslovanja, fizičko-tehničku zaštitu ili na neke druge bezbednosne poslove), a što je potvrdila i najbolja praksa, upućuju na neophodnost sprovođenja procesa procene rizika pre preduzimanja bilo kakvih zaštitnih mera, odnosno kontrola. A jedna od početnih radnji pri sprovođenju procesa procene rizika jeste identifikacija izvora, nosioca i oblika ugrožavanja, tj. identifikacija opasnosti i pretnji, kao i izazova i ranjivosti, čija će se verovatnoća i uticaj, odnosno posledice u slučaju njihove realizacije, kasnije analizirati i vrednovati (ocenjivati).

Pretnje i izazovi po bezbednost i otpornost korporacije

Osnovni oblik ugrožavanja bilo koje organizacije jeste *pretnja* (eng. threat), koju međunarodni dokument za određivanje termina koji se koriste u standardima bezbednosti i otpornosti *ISO 22300*[8] definiše kao

7 Kako je uređeno članom 11 *Pravilnika o programima i načinu obavljanja stručne obuke za vršenje poslova privatnog obezbeđenja i redarske službe* ("Službeni glasnik RS", br. 15/2019) organizator obuke za vršenje poslova privatnog obezbeđenja može da po posebnom zahtevu vrši obuku službenika obezbeđenja u vezi „sa pojavnim slučajevima i oblicima ugrožavanja lica i imovine i poslovanja".

8 *ISO 22300:2021, Security and resilience - Vocabulary.*

Slika 1.1. Pretnje i izazovi po bezbednost i otpornost korporacije

> *"potencijalni uzrok neželjenog incidenta, koji može dovesti do štete pojedincima, imovini, sistemu ili organizaciji, životnoj sredini ili zajednici".*

Prema navedenom standardu upravo *bezbednost* (eng. security) predstavlja

> *"stanje bez opasnosti i pretnji kada se poštuju procedure ili nakon preduzimanja odgovarajućih mera",*

te se značaj funkcije korporativne bezbednosti ogleda, pre svega, u eliminaciji, odnosno smanjenju verovatnoće ostvarenja pretnji, kao i u organizovanju adekvatne reakcije i odgovora u slučaju njene realizacije, a u cilju umanjenja posledica.

I važeći zakonski propisi RS koji se odnose na poslove korporativne bezbednosti prepoznaju i određuju obavezu zaštite od pretnji. Pri uređenju oblasti kritične infrastrukture[9] zakonodavac je odredio da njena zaštita predstavlja skup aktivnosti

i mera koje imaju za cilj zaštitu u slučaju pretnji, da je jedno od pet načela delovanja načelo zaštite od raznih vrsta pretnji, a da je oficir za vezu (koga moraju da imenuju operatori kritične infrastrukture) dužan da obezbeđuje stalnu kontrolu pretnji, kao i da obaveštava MUP o evaluaciji pretnji. Zato je potrebno permanentno analizirati pretnje kao postupka identifikacije, kvalifikacije i kvantifikacije potencijalnih uzroka neželjenih događaja koji mogu proizvesti štetu po korporaciju, posebno vodeći računa o novo pojavnim oblicima i trendovima. U eri sofisticiranih tehnologija i postojanja organizovanih međunarodnih kriminalnih grupa (sve češće iniciranih i podržanih od državnih aparata pojedinih zemalja[10]), neophodno je analizirati i imati odgovor na napredne trajne pretnje i nepoznate *"0-day"*[11] zlonamerne softvere, kao i periodično sprovoditi adekvatna testiranja na pretnje. Svakako da je pravljenje scenarija pretnji jedna od poželjnih i neophodnih radnji kojom bi se razmatrale ne samo pretnje sa ekstremnim i verovatnim posledicama, nego i oni napadi i događaji koji se smatraju malo verovatnim da će da se realizuju, odnosno oni koji se nisu nikada ranije desili u prošlosti.

Lepeza pretnji je veoma široka, a lista pretnji mora da sadrži kako one oblike ugrožavanja koji primarno mogu da nanesu štetnu posledicu licima[12] ili imovini[13], tako i one pretnje koje imaju objedinjeni uticaj na sve vrednosti i celokupno poslovanje, odnosno kontinuitet funkcionisanja korporacije (npr. zemljotres visokog intenziteta, teroristički čin ili ratno stanje). Iz tog razloga, neophodno je da nosioci funkcije korporativne bezbednosti izvrše identifikaciju svih pretnji, zasnovanu na holističkom pristupu kako bi mere zaštite imale optimalan učinak. Kao pomoć

10 Prema izveštaju *The European Union Agency for Cybersecurity (ENISA) „Threat Landscape Report 2018"*, Version 1.0, 2019, o top 15 sajber pretnjama i trendovima, u 2018. godini uočen je rast broja sajber napada na kompanije podržanih, tj. organizovanih od strane pojedinih država (Kina, SAD, Rusija i dr.). Takođe, navode da je potrebno uzimati u obzir i napomenu da pojedine korporacije (zbog značaja i strateške uloge koju imaju za državu, a u cilju dobijanja konkurentske prednosti) koriste gotovo iste tehnike napada kao one koje koriste napadači koji su sponzorisani od strane određenih država.

11 Izveštaj *ENISA Threat Landscape 2022*, November 2022 ukazuje na trend povećanja iskorišćenja „0-day" napada, u kom smislu bi organizacije trebale ulagati stalni napor na smanjenju dostupnosti ranjivosti koje se mogu iskoristiti povećavajućizrelost svojih programa odbrane i sajber bezbednosti, čime bi uticale na povećanje troškova protivnika, otežavajući im namere i terajući ih u pravcu stalnog razvijanja i/ili kupovine „0-day" eksploatacije.

12 Primera radi, napad ili druga radnja koja za posledicu može da ima smrt, povredu ili narušavanje zdravlja službenika obezbeđenja ili drugog zaposlenog, kao i otmica (obično vlasnika, generalnog menadžera ili drugog odgovornog lica, odnosno njihovih članova porodice) su primarno pretnja po fizičku bezbednost zaposlenog ili drugog lica, a sekundarno imaju uticaj na celokupno poslovanje korporacije.

13 Npr. sitna krađa, utaja ili prevara su prvenstveno pretnja po određenu imovinu korporacije, koja se sekundarno u većoj ili manjoj meri odražava i na njeno ukupno poslovanje.

pri sačinjavanju liste pretnji, koja obavezno mora da sadrži one pretnje koje su se ostvarile u prošlosti, kao i specifične oblike ugrožavanja karakteristične za određenu delatnost ili područje, mogu poslužiti primeri pretnji dati u mnogobrojnim standardima, smernicama i preporukama izdatih od strane međunarodnih, nacionalnih i granskih organizacija i udruženja. Jedna od najširih lista pretnji navedena je u katalogu[14] koji je publikovala nemačka kancelarija za bezbednost informacija, u kome je navedena i opisana ukupno 621 pretnja, a koje su grupisane u šest kategorija:

- bazične pretnje;
- viša sila;
- organizacioni nedostaci;
- ljudske greške;
- tehnički nedostaci;
- namerni napadi.

Takođe, različite internacionalne i državne institucije, kao i relevantne strukovne organizacije i udruženja, publikuju izveštaje iz svog domena, prateći zastupljenost i razvoj pretnji, kao i ukazujući na trendove. Iz jednog takvog izveštaja[15] koji je urađen na bazi istraživanja sprovedenog u 1000 američkih kompanija, prikazano je rangiranje po oblastima, a u ukupnom plasmanu najveća pretnja, unazad nekoliko godina, su sajber napadi, odnosno oblici ugrožavanja usmereni na informaciono-komunikacione tehnologije. Prilikom identifikacije pretnji svakako se moraju uzimati u obzir i analize zvaničnih institucija RS, pa se na primeru dokumenta MUP-a o proceni javne bezbednosti[16], pored ostalog, može videti da u

> *"ukupnom kriminalu na teritoriji Srbije preovlađuju krivična dela opšteg kriminala, koja čine skoro 90% krivičnih dela. Krivična dela privrednog kriminala čine oko 8%, dok su krivična dela visokotehnološkog i ekološkog kriminala, pojedinačno, zastupljena s manje od 1%. U okviru svakog od tih, zasebnih vidova kriminala postoje određeni oblici organizovanog kriminala."*

14 *IT-Grundschutz Catalogues*, Federal Office for Information Security (BSI), 13th version, Bonn DE, 2013.

15 *Top Security Threats and Management Issues Facing Corporate America*, Securitas Security Services USA, Parsippany NJ, 2016.

16 *Strateška procena javne bezbednosti*, MUP Republike Srbije - Direkcija policije, Beograd 2017., str. 21.

Za sačinjavanje konačne liste pretnji nezaobilazna je i primena srpskog standarda *SRPSA.L2.003*[17] kojim su trenutno definisani zahtevi i kriterijumi za identifikaciju potencijalnih opasnosti i pretnji za 11 grupa rizika, i to za:

- rizike opštih poslovnih aktivnosti;
- rizike po bezbednost i zdravlje na radu;
- pravne rizike;
- rizike od protivpravnog delovanja;
- rizike od požara;
- rizike od elementarnih nepogoda i drugih nesreća;
- rizike od eksplozija;
- rizike po životnu sredinu;
- rizike u procesu upravljanja ljudskim resursima;
- rizike u oblasti informaciono-komunikaciono-telekomunikacionih sistema;
- rizike od neusaglašenosti sa standardima.

Svakako da ovim nisu obuhvaćene sve pretnje po bezbednost lica, imovinu i poslovanje korporacije, a u planu je izrada zahteva i kriterijuma za identifikaciju potencijalnih opasnosti i pretnji za još osam grupa koji će biti definisani u posebnim delovima ovog standarda:

- vanredne situacije;
- požari i eksplozije;
- životna sredina;
- odbrana;
- planiranje sistema tehničke zaštite;
- oblast životnog i neživotnog osiguranja;
- zdravstvo;
- prosveta.

17 *SRPS A.L2.003:2017, Bezbednost i otpornost društva — Procena rizika*, Institut za standardizaciju Srbije, Beograd, 2017.

Za uspešno poslovanje u savremenim uslovima korporacije moraju anticipirati buduće događaje i pretnje, a top menadžment je dužan da definiše primerene poslovne odgovore svim izazovima. Pored toga, poslovanje današnjih korporacija ne može se posmatrati izolovano, već povezano i zavisno od različitih okolnosti i događaja uslovljenih globalizacijskim procesima. *Izazov* se može definisati kao

> *"ponašanje, odnosno postupak, vezan za određenu prirodnu ili društvenu pojavu koja pokreće akciju ili reakciju. Izazovi su i potencijalni oblici ugrožavanja bezbednosti. Izazovi su najudaljeniji po svom položaju u odnosu na zaštićeni objekat, ali predstavljaju izvorište rizika i pretnji. Zbog toga je neophodno da im se posveti odgovarajuća pažnja jer se mogu pretvoriti u rizike i pretnje čiji je uticaj na objekat bezbednosti neposredniji i štetniji."*[18]

Iz praktičnih razloga potrebno je navesti da identifikacija izazova predstavlja i zakonsku obavezu korporacija, odnosno privrednih društava, drugih pravnih lica i preduzetnika, tj. subjekata od značaja za odbranu. Iako *Zakon o odbrani*[19] bliže ne pojašnjava pojam izazova uvodi kao obavezu subjektima od značaja za odbranu, identifikaciju vojnih (agresije, oružane pobune i drugi oblici upotrebom oružane sile) i nevojnih izazova, rizika i pretnji (terorizam, organizovani kriminal, korupcija, elementarne nepogode, tehničko-tehnološke i druge nesreće i opasnosti) prilikom izrade sopstvenih procena vojnih i nevojnih izazova, rizika i pretnji po bezbednost.

Ukoliko se na startu procesa procene rizika propusti da se identifikuju pretnje i određeni izazovi koji mogu imati negativan uticaj na korporaciju, zaštitne i kontrolne mere predviđene na bazi procene, biće nedovoljne i neefikasne za adekvatnu odbranu organizacije, a sistem bezbednosti ličiće na tzv. "Mažino liniju"[20].

Bez obzira da li potiče od unutrašnjih, spoljašnjih ili kombinovanih nosioca ugrožavanja, da li pripada tzv. kriminalu belog ili plavog okovratnika, ili je u pitanju neki drugi delikt, zbog preduzimanja adekvatnih mera zaštite i kasnijeg potrebnog procesuiranja neophodno je sve pretnje sagledati kroz prizmu protivprav-

18 Trivan Dragan, *Osnovi korporativne bezbednosti*, op. cit. str. 91.

19 „Službeni glasnik RS", br. 116/2007, 88/2009, 88/2009 - dr. zakon, 104/2009 - dr. zakon, 10/2015 i 36/2018.

20 Odbrambena linija sačinjena od povezanih betonskih utvrđenja, tenkovskih prepreka, tunela i ostalih vidova odbrane koje je Francuska konstruisala duž svojih granica sa Nemačkom i Italijom pred Drugi svetski rat. Prilikom napada linija je ostala netaknuta jer su je nemačke snage zaobišle i okupirale Francusku, pa se izraz „Mažino linija" koristi kao metafora za nešto neefikasno, a na šta se neko sa pouzdanjem oslanja.

nosti, odnosno krivično-pravne, građansko-pravne, upravno-pravne ili disciplinske odgovornosti (ne zanemarujući ni moralni aspekt odgovornost kao bitni faktor u očuvanju bezbednog ambijenta). Uzimajući u obzir da se funkcija korporativne bezbednosti fokusira na analizu protivpravnih radnji koja ugrožavaju bezbednost organizacije, jasno je da u tom smislu glavne rizike čine krivična dela. Svakako da se prilikom identifikacije pretnji ne smeju zanemariti ni prekršaji i privredni prestupi koji predstavljaju niži stepen opasnosti, a moraju se uzeti u obzir i disciplinski prestupi u meri srazmernoj njihovoj štetnosti i učestalosti. Građansko-pravni delikti, takođe, moraju biti predmet kontrolnih mera jer prouzrokovane štete koje nastaju kršenjem građansko-pravnih dispozicija mogu imati značajan uticaj na kontinuitet poslovanja korporacije, te moraju biti u adekvatnom sistemu unutrašnje, pre svega, pravne zaštite i brzog pravnog reagovanja. Napominjemo da je i srpskim standardom za procenu rizika u zaštiti lica, imovine i poslovanja određeno da identifikacija krivičnih dela ili drugih oblika nezakonitog delovanja (iz oblasti imovinskog kriminaliteta, privrednog kriminaliteta, privrednih prestupa, težih prekršaja protiv javnog reda i mira, kao i drugih krivičnih dela, privrednih prestupa i prekršaja) predstavlja neophodnu fazu procesa procene rizika.

Zbog različitih načina unutrašnjeg uređenja korporacija neophodno je u startu jasno odrediti opseg i ulogu funkcije korporativne bezbednosti u upravljanju zaštitnim merama i kontrolama, odnosno granice njene odgovornosti u borbi protiv protivpravnih delikta. Posebno je osetljiva njena uloga u identifikaciji delikta koja spadaju u grupu tzv. *kriminalitet korporacije*, koji se čine od strane odgovornih lica[21] koja imaju diskreciona ovlašćenja i poziciju moći, obično članova top menadžmenta korporacije. Odgovorno lice može u okviru svojih poslova, odnosno ovlašćenja da učini krivično delo u nameri da za pravno lice ostvari korist, u kom slučaju korporacija odgovara, a izrečene krivične sankcije znatno mogu da utiču na njeno ukupno poslovanje. Pored novčane kazne, uslovne osude i mera bezbednosti (zabrana obavljanja određenih registrovanih delatnosti ili poslova; oduzimanje predmeta; javno objavljivanje presude), kao glavna kazna korporaciji se može izreći i najteža kazna - prestanak pravnog lica. Ukoliko se izuzme faktor nerazumevanja značaja i uloge funkcije bezbednosti od strane top menadžmenta, nepostojanje ovih poslova u okviru organizacije, odnosno njeno marginalizovanje može ukazivati da se pravno lice prividno bavi legalnim poslovima, a u suštini obavlja protivzakonite poslovne ak-

21 Članom 5 *Zakona o odgovornosti pravnih lica za krivična dela* („Službeni glasnik RS", br. 97/2008) određeno je da je odgovorno lice fizičko lice kome je pravno ili faktički poveren određeni krug poslova u pravnom licu, kao i lice koje je ovlašćeno, odnosno za koje se može smatrati da je ovlašćeno da postupa u ime pravnog lica.

tivnosti. Ova grupa delikta (kao što su utaja poreza, pranje novca, mito, zagađivanje hrane i vode, proizvodnja nebezbednih proizvoda itd.) može da proizvede izuzetno teške posledice u vidu velikog broja ljudskih žrtava, ugrožavanja zdravlja ljudi ili ogromnih materijalnih gubitaka, posebno kada se ispoljava u ekološkoj oblasti. Slična je situacija kod tzv. kriminaliteta belog okovratnika, s tim da se u ovom slučaju delikti vrše iz privatnog interesa za ličnu korist. Treba biti svestan postojanja visoke tamne brojke ove vrste kriminaliteta iz razloga što je broj otkrivenih ili prijavljenih slučajeva znatno manji od stvarnog.

Pošto nijedan od oblika ugrožavanja koji potiče od ljudi nema značaj niti težinu kao kriminalno delovanje, u nastavku će biti navedena pojedina krivična dela koja bi morala biti u fokusu funkcije korporativne bezbednosti i koje su pretnja gotovo svim organizacijama, bez obzira na delatnost, veličinu i oblik svojine. Svesni činjenice da pojedina krivična dela mogu biti učinjena samo od strane unutrašnjeg nosioca, a druga izvršena isključivo od strane spoljašnjeg nosioca (ne zaboravljajući postojanje kombinovane nosioce ugrožavanja), neophodno je da svako krivično delo mora biti zakonom predviđeno kao krivično delo, da mora biti protivpravno i skrivljeno. Potrebno je naglasiti da je preduzimanje mera radi vršenja radnji usmerenih na sprečavanje krivičnih dela zakonski osnov, a Zakon o privatnom obezbeđenju propisuje i vođenje evidencije izveštaja o krivičnim delima koja se gone po službenoj dužnosti od strane pravnih lica i preduzetnika za privatno obezbeđenje. Iz Posebnog dela *Krivičnog zakonika*[22] možemo navesti pojedina krivična dela koja bi, pored drugih, trebala da se nalaze na listama za identifikaciju pretnji, raspoređenih u sledeće grupe:

- krivična dela protiv sloboda i prava čoveka i građanina – otmica (član 134.);
- krivična dela protiv prava po osnovu rada - nepreduzimanje mera zaštite na radu (član 169.);
- krivična dela protiv intelektualne svojine - povreda pronalazačkog prava (član 201.);
- krivična dela protiv imovine - krađa (član 203.), teška krađa (član 204.), razbojnička krađa (član 205.), razbojništvo (član 206.), utaja (član 207.), prevara (član 208.), sitna krađa, utaja i prevara (član 210.),ucena (član 215.);

22 „Službeni glasnik RS“, br. 85/2005, 88/2005 - ispravka, 107/2005 - ispravka, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

- krivična dela protiv privrede - pronevera u obavljanju privredne delatnosti (član 224.), odavanje poslovne tajne (član 240.);
- krivična dela protiv opšte sigurnosti ljudi i imovine - izazivanje opšte opasnosti (član 278.),
- izazivanja opasnosti neobezbeđivanjem mera zaštite na radu (član 280.);
- krivična dela protiv bezbednosti računarskih podataka - oštećenja računarskih podataka (član 298.), računarske sabotaže (član 299.), pravljenja i unošenja računarskih virusa (član 300.), računarske prevare (član 301.), neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302.);
- krivična dela protiv javnog reda i mira - nasilničko ponašanje (član 344.).

Adekvatna zaštita korporacije od prethodno navedenih krivičnih dela i drugih pretnji može se ostvariti samo sveobuhvatnom primenom integrisanih bezbednosnih mera i kontrola sadržanih u poslovima korporativne bezbednosti, koji će detaljnije biti navedeni u narednom poglavlju. Zarad sagledavanja obima i delikatnosti izazova u zaštiti zaposlenih i drugih lica, celokupne materijalne i nematerijalne imovine i ukupnog poslovanja, kao i zbog kompleksnosti problematike i potrebe za holističkim pristupom u rešavanju bezbednosnih pitanja i ostvarivanju otpornosti, nadalje u tekstu biće navedeni pojedini oblici ugrožavanja (pretnje) čijim negativnim uticajima su podložne većine organizacija, bez obzira na veličinu, svojinski oblik, lokaciju ili vrstu delatnosti.

Prevara i korupcija

Ranije naveden holistički pristup u analizi pretnji neophodan je i prilikom sagledavanja *prevare*, gde je ona kao krivično delo protiv imovine, pre svega, određena članom 208. KZ koji predviđa kaznu zatvora i novčanu kaznu za onog ko

> *"u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist dovede koga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini ili ne učini …".*

Takođe, KZ sankcioniše i sitnu prevaru, prevaru u obavljanju privredne delatnosti, ali i računarsku prevaru iz grupe krivičnih dela protiv bezbednosti računarskih podataka, kao i prevare u službi. Već na osnovu navedenog može se naslutiti

spektar opasnosti od prevare po korporaciju, ali se zbog izgradnje adekvatnog sistema odbrane ne sme ispusti iz vida činjenica dase pod prevarom (eng. fraud) u praksi podrazumeva širi spektar aktivnosti i krivičnopravnih dela, internog i eksternog karaktera, kao što su krađa, korupcija, socijalni inženjering, pronevera, pranje novca, podmićivanje, iznuda i drugo. Vodeća međunarodna organizacija iz domena interne revizije (*The Institute of International Auditors - IIA*) u svom publikovanom standardu[23] vezanom za sprovođenje interne revizije, određuju prevaru kao

> *"svaki nezakonit čin koga karakteriše obmana, prikrivanje ili kršenje poverenja",*

a najveća internacionalna asocijacija za borbu protiv prevare - *Association of Certified Fraud Examiners (ACFE)* određuje da prevara u najširem smislu

> *"obuhvati bilo koji delikt iz koristoljublja koji koristi obmanu kao svoj glavni modus operandi"*[24].

Konkretnije navodeći definiciju prevare iz istaknutog pravničkog rečnika *Black's Law*[25] prevara je

> *"svesno pogrešno predstavljanje istine ili prikrivanje stvarne činjenice kako bi se izazvalo nečije delovanje na sopstvenu štetu",*

ACFE u izveštaju[26] vezanom za prevare u poslovanju, ističe da generalno gledano gubitak svakog pravnog lica zbog prevara iznosi 5% svojih godišnjih prihoda, kao i da je srednja godišnja vrednost prijavljenog gubitka za region istočne Evrope (uključujući i Republiku Srbiju) 150 000 USD po organizaciji.

Na ovako šire prihvaćen pojam prevare nije imuna ni jedna vrsta organizacije[27], a najviše su zastupljene u bankarskom poslovanju i drugim organizacijama koje

23 *Global Internal Audit Standards, IIA, Lake Mary, 2024*

24 https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud, 04.11.2024.

25 Garner A. Bryan (ed.), Black's Law Dictionary, 8th Ed., West, Eagan MN, 2004. p. 1950

26 *Occupational Fraud 2024: A Report to the Nations, ACFE, Austin TX, 2024.*

27 Ni verske institucije koje važe za visoko moralne i etičke organizacije nisu otporne na razne oblike prevara, a za primer možemo navesti proneveru oko 1,1 miliona evra učinjenu od strane blagajnika Srpske pravoslavne crkve S. Ž. koga je Apelacioni sud u Beogradu pravosnažno osudio na višegodišnju zatvorsku kaznu (http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:510000-Beograd-Blagajniku-SPC-devet-godina-i-tri-meseca-zatvora-za-proneveru, 14.09.2014.). Takođe, prevara može biti posebno destabilišuća za male organizacije koje obično imaju manje sredstava za sprečavanje i oporavak od prevare, a često imaju povećan

pružaju finansijske usluge. Banke, društva za upravljanje investicionim fondovima, društva za osiguranje i druge finansijske organizacije posebno su osetljive na protivpravne radnje pranje novca i finansiranje terorizma, te su shodno *Zakonu o sprečavanju pranja novca i finansiranja terorizma*[28], podzakonskim propisima, kao i preporukama, odnosno smernica donetih na osnovu ovog zakona, dužne da preduzimaju niz radnji i mere za njihovo sprečavanje i otkrivanje. Izgradnja adekvatnog sistema sprečavanja pranja novca i finansiranja terorizma mora da se zasniva na analizi i upravljanju rizicima od pranja novca i finansiranja terorizma, a funkcija korporativne bezbednosti treba da bude uključena i u radnje obaveznih bezbednosnih provera zaposlenih koji su angažovani na određenim radnim mestima. Takođe, potrebno je da funkcija korporativne bezbednosti sprovodi redovnu unutrašnju kontrolu obavljanja poslova sprečavanja i otkrivanja pranja novca i finansiranja terorizma, kao i da učestvuje u izradi i sprovođenju programa obaveznog stručnog obrazovanja, osposobljavanja i usavršavanja zaposlenih koji obavljaju te poslove.

U odnosu na nosioce ugrožavanja preovlađuju prevare internog karaktera koje se manifestuju kroz više vrsta i oblika obrazujući čitavo stablo prevara u poslovanju, koje možemo grupisati u tri glavne kategorije:

- korupcija (podmićivanje, sukob interesa, nelegalno čašćavanje, finansijsko ucenjivanje i dr.);
- prevara finansijskih izveštaja (fiktivni prihodi i rashodi, nepravilno unošenje vrednosti sredstava i sl.);
- zloupotreba sredstava (utaja, posluga, krađa, oštećenje i druge nedozvoljene radnje i zloupotrebe novca, inventara i drugih vrednosti).

U odnosu na ovakvu kategorizaciju najveći broj slučajeva prevare odnosi se na zloupotrebu sredstava, ali nominalno posmatrano ona nosi najmanju vrednost, dok je najmanje prevara finansijskog izveštavanja koja nosi višestruko veću nominalnu vrednost[29].

Korupcija predstavlja veliku pretnju po poslovanje svakog pravnog lica, a zbog izuzetne društvene opasnosti država je donela niz zakonskih propisa i odredila je

nivo poverenja u zaposlene zbog niže sposobnosti da sprovedu kompleksne kontrole protiv prevare.

28 "Službeni glasnik RS", br. 113/2017, 91/2019, 153/2020 i 92/2023.

29 Propast u to vreme najveće američke energetske kompanije Enron krajem 2001. godine predstavlja primer jedne od najkompleksnijih knjigovodstvenih prevara u istoriji. Ta kompanija je bankrotirala iako je u godini koja je prethodila imala prihod od blizu 100 milijardi američkih dolara. Krah Enrona je doveo do propasti brojnih povezanih korporacija i penzijskih fondova.

organizaciju i nadležnosti državnih organa u suzbijanju korupcije. U praksi je prisutan čitav spektar pojavnih oblika u izvršenju koruptivnih krivičnih dela, a MUP u publikovanoj proceni[30] iznosi da ona u privrednim subjektima podrazumevaju

> *"različite vidove zloupotrebe u raspolaganju imovinom preduzeća, od kojih je najčešća stavljanje pod hipoteku bez saglasnosti akcionara; zloupotrebe u postupcima javnih nabavki; različite vidove zloupotreba izvršenih korišćenjem više funkcija koje lice ima (najčešće istovremeno odgovorno lice u privatnom i društvenom preduzeću); plaćanje fiktivnih usluga drugim privrednim subjektima (kako bi se pribavila korist tim subjektima); nenamensko trošenje sredstava dobijenih iz budžeta i dr.".*

Jedna od glavnih mera pravne i praktične prirode kojim se sprečavaju i otklanjaju mogućnosti za nastanak i razvoj korupcije[31] jeste donošenje plana integriteta, kako od strane državnih organa i organizacija, tako i od strane organa teritorijalne autonomije i lokalne samouprave, javnih službi i preduzeća koji imaju više od 30 zaposlenih, a na dobrovoljnoj osnovi, i od strane svih drugih pravnih lica i organizacija koja nisu obveznici donošenja plana integriteta. Plan integriteta, kao sastavni deo ukupnog programa prevencije prevara, pored ostalog, sadrži procenu intenziteta rizika od korupcije, utvrđivanje procesa koji su naročito rizični za nastanak korupcije, kao i preventivne mere kojima se otklanjaju rizici od korupcije, a njegova izrada je određena *Uputstvom za izradu i sprovođenje plana integriteta*[32]. Poželjno je da lice odgovorno za plan integriteta bude u okviru funkcije korporativne bezbednosti, a jedna od ključnih mera je izrada adekvatnih komunikacijskih kanala za prijavu korupcije i drugih radnji prevare u širem smislu, uzimajući u obzir i izgradnju sistema zaštite lica koja takve radnje prijavljuju, uključujući i uzbunjivače shodno *Zakonu o zaštiti uzbunjivača*[33]. Izgradnja sistema borbe protiv mita može da upotpuni radnje prevencije korupcije, i u tom smislu poželjna mera je implementacija standarda *SRPS ISO 37001*[34], koji predstavlja prvi međunarodni standard iz oblasti sistema me-

30 *Strateška procena javne bezbednosti*, op. cit., str. 59.

31 *Zakon o sprečavanju korupcije* („Službeni glasnik RS", br. 35/2019, 88/2019, 11/2021 - Autentično tumačenje, 94/2021 i 14/2022) određuje korupciju kao „odnos koji nastaje korišćenjem službenog ili društvenog položaja ili uticaja radi sticanja nedozvoljene koristi za sebe ili drugoga".

32 "Službeni glasnik RS", br. 119/2022.

33 "Službeni glasnikRS", br. 128/2014.

34 *SRPSISO 37001:2017, Sistemi menadžmenta protiv mita – Zahtevi sa uputstvom za korišćenje*, Institut za standardizaciju Srbije, Beograd, 2017.

nadžmenta namenjen za borbu protiv mita i korupcije. Primenljiv je na sve organizacije (ili delove organizacije), nezavisno od tipa, veličine ili prirode aktivnosti, bez obzira na to da li su u javnom, privatnom ili neprofitnom sektoru, a koncipiran je tako da pomogne organizacijama u borbi sa rizikom od mogućeg podmićivanja u sopstvenim radnim procesima. Ovaj standard poseduje potencijal za umanjenje korporativnog rizika i troškova u vezi sa pojavom podmićivanja, težeći da obezbedi fleksibilan poslovni okvir kojim se sprečava, otkriva i rešava podmićivanje.

Zbog problematike povraćaja i nadoknade svega što je prevarom izgubljeno najisplativiji način ograničavanja gubitaka je da se spreči da do prevare dođe. Procena rizika od prevara, kao neophodna mera u procesu borbe protiv prevara mora da uzme u obzir faktore koje utiču na prevare, poznate pod nazivom "trougao prevare":

1. postojanje podsticaja, pritiska kao motiva za vršenje prevare (potreba za novcem, dugovi, bolest, poroci i dr.);

2. postojanje mogućnosti, prilike da se prevara realizuje (nepostojanje ili loša kontrola, spajanje funkcija u jednu i slično);

3. stav lica koja vrše prevare, ali i stav menadžera i drugih zaposlenih(opravdanje za izvršenje protivpravnih radnji).

Pojedini autori ovim faktorima dodaju još jedan element - sposobnost da se prevara izvrši, čime se dobija tzv. "dijamant prevare", a proaktivne i reaktivne mere u okviru sistema borbe protiv prevara moraju da obuhvataju programe prevencije, odvraćanja, detekcije, sanacije i edukacije. Upravo nedostatak ovih programa predstavlja najveći rizik od prevarnih radnji, a motivisanost i svest zaposlenih su od presudnog značaja za njihovo uspešno sprovođenje, dok mere zaštite moraju da budu inkorporirane u sve poslovne procese. Zato u borbi protiv prevara moraju biti uključeni kako spoljni subjekti (eksterna revizija, inspekcijski organi i dr.), tako i sve interne organizacione celine (funkcija korporativne bezbednosti, interna revizija, kontrola kvaliteta, računovodstvo, nabavke i dr.), a top menadžment mora da insistira na izradi i primeni kontrola koja naročito uređuju:

- kodeks ponašanja;
- postojanje adekvatne linije prijavljivanja;
- reviziju finansijskog izveštavanja;
- program podrške zaposlenima i nagrade za prijavljivanje;

- trening za borbu protiv prevare, naročito članova izvršnog rukovodstva;
- iznenadne i nenajavljene popise;
- rotacije na poslu;
- obavezno korišćenje odmora i drugo.

Prevaru nije lako uočiti i zato detekcija predstavlja jednu od najosetljivijih faza u borbi protiv prevara, a kako navodi *ACFE* u svojoj studiji[35] o prevarama u vezi poslovanja, najveći broj prevara detektovano je na osnovu dojave, i to pre svega od strane zaposlenih. Iz tog razloga funkcija korporativne bezbednosti mora da adekvatno upravlja procesima dojave prevara, kao i da obezbedi zaštitu zaposlenih i drugih lica od nepotrebnog identifikovanja i proganjanja, kao i da izgradi različite vidove linija komunikacije i dojave kako bi prijavljivanje bilo moguće i od strane kupaca, odnosno korisnika usluga, dobavljača, ali i anonimnih lica. Pored toga, neophodno je odrediti indikatore, odnosno obeležiti procese, radna mesta i zaposlene tzv. "crvenim zastavicama", koje ukazuju na okolnosti i moguće postojanje prevare kao što su život iznad mogućnosti, finansijske teškoće, neobično bliska povezanost sa dobavljačima i kupcima, nespremnost za deljenje obaveza itd. Po saznanju o prevari neophodno je odmah preduzeti istragu, a brzina i stručnost u realizaciji istrage omogućavaju pravovremenu sanaciju, smanjenje novčanih gubitaka i očuvanje reputacije korporacije. Spoznaja šema prevare je od posebne važnosti za tok istrage, a u slučajevima kada se sprovodi istraga specifičnih prevarnih radnji neophodno je poznavanje posebnih znanja, veština i tehnika kao što je finansijska forenzika, kompjuterska forenzika, tehnike forenzičkih intervjua i slično, za šta se u nedostatku sopstvenih kadrova sa tim znanjima mogu uslužno angažovati i specijalizovane kompanije.

U procesu borbe protiv prevara korporativna bezbednost mora da bude nosilac poslova bezbednosne provere kandidata prilikom zapošljavanja, kao i zaposlenih tokom radnog odnosa, a sprovođenje osnovnih, periodičnih i posebnih obuka zaposlenih vodi ka povećanju njihovog nivoa razumevanja rizika prevara u poslovanju koja su pod njihovom kontrolom. Od velike prednosti je da zaposleni angažovani na poslovima borbe protiv prevara budu obučeni za te poslove i osposobljeni za sprovođenje prevencije, istrage i drugih program, kao i da poseduju adekvatan sertifikat (npr. *Certified Fraud Examiner*). Pored toga što postoje preporuke i standardi čijom implementacijom se povećava otpornost na posebne vrste i specifične prevare, karakteristične za određene delatnosti ili poslove (sajber prevare, bankarske prevare,

35 *Report to the Nations - Global study on occupational fraud and abuse*, Eastern Europe and a Western/Central Asia edition, ACFE, Austin TX, 2018.

prevare u nabavci i dr.), za svaku organizaciju je poželjno da uspostavi sveobuhvatan pristup prevenciji prevara putem implementacije univerzalnih principa i smernica.[36]

Odavanje poslovne tajne ("industrijska špijunaža") i nelojalna konkurencija

Informacije predstavljaju jednu od najvećih vrednosti svake organizacije i zato je neophodno svim podacima i informacijama koje nastaju u poslovanju pristupati sa oprezom, a moraju biti i u određenom režimu korišćenja i čuvanja. Ovo se posebno odnosi na one podatke i informacije koje su poverljive, tajne i kao takve na odgovarajući način klasifikovane i pod adekvatnim merama zaštite, a kojima pripada i *poslovna tajna* koju, kako je određeno članom 240. KZ, čine

> *"podaci i dokumenti koji su zakonom, drugim propisom ili odlukom nadležnog organa donesenom na osnovu zakona proglašeni poslovnom tajnom čije bi odavanje prouzrokovalo ili bi moglo da prouzrokuje štetne posledice za subjekt privrednog poslovanja".*

Poslovna tajna bliže je određena *Zakonom o privrednim društvima*[37] i predstavlja

> *"podatak čije bi saopštavanje trećem licu moglo naneti štetu društvu, kao i podatak koji ima ili može imati ekonomsku vrednost zato što nije opšte poznat, niti je lako dostupan trećim licima koja bi njegovim korišćenjem ili saopštavanjem mogla ostvariti ekonomsku korist i koji je od strane društva zaštićen odgovarajućim merama u cilju čuvanja njegove tajnosti".*

Sa naučno-tehnološkim razvojem i usložnjavanjem tržišnih uslova poslovna tajna dobija sve više na značaju, ali je i njeno odavanje sve prisutnije[38] uz postoja-

36 Niz preporuka, smernica, strategija i standarda publikovanih od strane međunarodnih, regionalnih, nacionalnih i granskih organizacija pomažu izgradnju sistema borbe protiv prevara, od kojih možemo izdvojiti *Fraud Risk Management Guide*, COSO, Morristown NJ, 2016.; *BSI - BS 10501:2014*, *Guide to implementing procurement fraud controls* BSI, London 2014*; Reducing the risk of wholesale payments fraud related to endpoint security*, BIS, London 2018 i dr.

37 "Službeni glasnik RS", br. 36/2011, 99/2011, 83/2014 - dr. zakon, 5/2015, 44/2018 i 95/2018.

38 Jedan od najvećih obelodanjenih slučajeva odavanja poslovne tajne, vredan nekoliko stotina miliona evra, dogodio se vodećoj svetskoj korporaciji za izradu čipova i drugih poluprovodnika ASML iz Holandije, koja je pretrpela štetu učinjenu od strane bivših zaposlenih koji su imali

nje velike tamne brojke koja je prisutna, pre svega, zbog želje za očuvanjem ugleda korporacija koje su pretrpele štetu i koje smatraju da bi iznošenje takvih podataka moglo oslabiti njihovu reputaciju, odnosno dovesti do pada vrednosti njenih akcija, raskida određenih ugovorenih poslova, razotkriti slabosti i slično.

Osnovna svrha uspostavljanja instituta poslovne tajne je obezbeđenje njene pravne zaštite od različitih aktivnosti nelojalne konkurencije, odnosno zaštita konkurentske prednosti na tržištu koju držaoc poslovne tajne ima ako poseduje takvu informaciju. Korporacije moraju biti svesne i uticaja *konkurencije*, kao i pretnji koje dolaze od nelojalne konkurencije, odnosno od konkurencije koja je na sve spremna u cilju zauzimanja dominantnijeg položaja na tržištu. Zaštita od radnji nelojalne konkurencije koja želi neovlašćeno i suprotno dobrim poslovnim običajima da nezakonito pribavi informacije koje predstavljaju poslovnu tajnu (uključujući i znanje i iskustvo, poslovne informacije i tehnološke informacije) uređena je *Zakonom o zaštiti poslovne tajne*[39]. Inače, domaće zakonodavstvo ne prepoznaje pojam *industrijske špijunaže*[40], koji se kao takav navodi u određenoj inostranoj zakonskoj regulativi i literaturi, a koji je još poznat pod terminima ekonomska, komercijalna, korporativna, odnosno poslovna špijunaža. Predmet industrijske špijunaže jesu, pre svega, informacije koje predstavljaju poslovnu tajnu, odnosno oni podaci i informacije koje su zakonom ili drugim propisom proglašene poslovnom tajnom[41], kao i one koje se smatraju poslovnom tajnom po odluci nadležnog organa, odnosno predstavljaju tajnu jer nisu u celini ili u pogledu strukture i skupa njihovih sastavnih delova opšte

pristup izvornim kodovima i drugim podacima koji su predstavljali poslovnu tajnu. Kršeći ugovorne obaveze bivši zaposleni su saopštavali podatke konkurentskoj kompaniji XTAL koja je na osnovu njih ostvarila korist i, pored ostalog, preuzela velike kupce kao što je elektrogigant Samsung. Konačni epilog parnice, koja je vođena pred američkim sudom tokom 2019. godine, jeste presuda u korist korporacije ASML, vredne 845 miliona američkih dolara, ali koja neće moći biti naplaćena zbog odlaska XTALu stečaj. Pored toga, XTAL je dobio i zabranu obavljanja delatnosti, a ASML postaje vlasnik intelektualne svojine XTAL u delu koja je bila predmet parnice, kao i dozvolu da može da dopre do stvarnih ili potencijalnih klijenata XTAL i informiše ih o rezultatima presude (https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=329062638, 10.06.2019.).

39 "Službeni glasnik RS", br. 53/2021.

40 Bez bližeg pojašnjenja, pojam industrijske ili komercijalne špijunaže bio je naveden u do skoro važećem *Zakonu o zaštiti poslovne tajne* („Službeni glasnik RS", br. 72/11) kao jedan od načina nezakonitog pribavljanja, korišćenja i otkrivanja informacije koja predstavlja poslovnu tajnu.

41 Primera radi, *Zakon o platnim uslugama* ("Službeni glasnik RS", br. 139/2014 i 44/2018) određuje da se poslovnom tajnom „smatraju podaci do kojih je u toku poslovanja došao pružalac platnih usluga", a *Pravilnik o načinu vršenja poslova tehničke zaštite i korišćenja tehničkih sredstava* ("Službeni glasnik RS", br. 91/2019) predviđa da su to dokumenta sačinjena u toku izvođenja i upotrebe tehničke zaštite (akt o proceni rizika u zaštiti lica, imovine i poslovanja, plan sistema tehničke zaštite i dr.).

poznate ili lako dostupne licima koja u okviru svojih aktivnosti uobičajeno dolaze u kontakt sa takvom vrstom informacija i kao takve imaju komercijalnu vrednost. Pored poslovne tajne, industrijska špijunaža ima zadatak da dođe i do ostalih osetljivih informacija, ali i do onih koje to nisu, odnosno "običnih" podataka koje nisu zaštićene od neovlašćenog korišćenja poput informacija o radnim navikama zaposlenih, o njihovoj stručnosti, produktivnosti, interpersonalnim odnosima, vrlinama i slabostima menadžera i drugo. Ne sme se ispustiti iz vida da nelojalna konkurencija u cilju dolaženja do informacija u velikoj meri koristi javne, otvorene izvore (statističke podatke, medijska izveštavanja, ekspertske ocene i analize, posete sajmovima i dr.) koji predstavljaju izvore tzv. legalne špijunaže, ali prilikom prikupljanja podataka upotrebljava i nedozvoljene mere koje su u isključivoj nadležnosti određenih državnih institucija, odnosno koriste posebne mere tajnog prikupljanja informacija. Iz ovih razloga menadžment pravnog lica treba dobro da poznaje konkurenciju i istovremeno da zaštiti sopstvene podatke i informacije od konkurencije[42].

Tretiranje konkurencije je neophodno i prilikom uspostavljanja eksternog konteksta shodno zahtevu nacionalnog standarda za procenu rizika u oblasti bezbednosti i otpornosti *SRPS A.L2.003*, kojim je potrebno sagledati sve faktore izvan organizacije koji mogu da imaju uticaj na njene ciljeve. Pitanje zaštite svih poslovnih informacija aktuelno je u istoj meri kao i njihovo prikupljanje i kao takvo predstavlja jedan od najvećih izazova modernog poslovanja, a korporacije su dužne da razviju sopstvene programe poslovno-obaveštajnog delovanja (eng. business intelligence) i kontra delovanja (eng. business counterintelligence) koji su u stanju da blagovremeno detektuju pretnje od industrijske špijunaže, kao i da prikupe i pripreme top menadžmentu pravovremene informacije neophodne za kontinuitet rada i dalji razvoj na tržištu.

Zaštita poslovne tajne predstavlja jedan od nerazvijenih segmenta poslovanja domaćih organizacija, gde ne postoje jasno definisani kriterijumi i pravila za njegovu realizaciju, pa i u slučaju otkrivanja nezakonitog pribavljanja poslovne tajne način procesiranja je veoma težak, uz nepostojanje razvijene sudske prakse. S obzirom da nepridržavanje obaveze čuvanja poslovne tajne može proizvesti radnopravnu, materijalnu i kazneno-pravnu, odnosno krivičnu i prekršajnu odgovornost, neophodno je primeniti mere u cilju efikasne zaštite poslovne tajne, koje isključivo moraju biti u sklopu celovitog sistema korporativne bezbednosti. Uloga korporativne bezbednosti u zaštiti poslovne tajne ogleda se pre svega u sprečavanju neovlašćenih lica da dođu

42 Mandić J. Goran, *Osnovi sistema obezbeđenja pravnih lica*, Fakultet bezbednosti Univerziteta u Beogradu, Beograd, 2012., str. 65 - 70.

u posed takvih informacija, odnosno implementaciji odgovarajućeg preventivnog i proaktivnog sistema, koji je daleko efikasniji od najboljih mera represije i reaktivnog delovanja. Drugim rečima, bolje je sprečiti nastajanje štete zbog odavanja poslovne tajne nego i najefikasnijim metodama sanirati štetne posledice, koje u nekim slučajevima mogu biti i neotklonjive, odnosno dovesti do prestanka rada organizacije.

Prvi korak u preduzimanju razumnih mera za očuvanje tajnosti informacija je normativni, i ogleda se u donošenju internog akta o rukovanju poslovnom tajnom i određivanju kruga lica sa njihovim pravima i obavezama prilikom rukovanja poslovnom tajnom, a kriterijume poslovne tajne određuje svaka korporacija za svoje potrebe u skladu sa propisima i internim aktom, uz uvažavanje činjenice da poslovna tajna predstavlja dinamičku kategoriju, odnosno da ono što je danas tajna ne mora nužno biti i sutra. Klasifikacija, kao opšta mera zaštite svih informacija, mora se realizovati i nad podacima koje predstavljaju poslovnu tajnu, bez obzira da li nalaze u pismenom/štampanom ili elektronskom obliku. U praksi se nalazi i podela poslovne tajne po nivoima, koja može da olakša praktičnu primenu i koja je proistekla po ugledu na stepenovanje iz propisa kojim je uređena zaštita tajnosti podataka. Provera postojanja potpunog i adekvatnog normativnog okvira kojom se štite podaci i dokumenta poslovne tajne je i deo zahteva za procenu pravnih rizika shodno SRPS A.L2.003, a svakako je potrebno da se unutrašnjim aktima kojim se uređuje ponašanje zaposlenih, reguliše i zabrana odavanja poverljivih informacija, uključuju poslovnu tajnu. Jedna od normativnih mera sastoji se u utvrđivanju poslova koje zaposleni ne može da radi u svoje ime i za svoj račun, kao i u ime i za račun drugog pravnog ili fizičkog lica, bez saglasnosti poslodavca kod koga je u radnom odnosu (zabrana konkurencije). Zabrana konkurencije može da se utvrdi samo ako postoje uslovi da zaposleni radom u organizaciji stekne nova, posebno važna tehnološka znanja, širok krug poslovnih partnera ili da dođe do saznanja poslovnih tajni, a ugovorom o radu shodno Zakonu o radu utvrđuje se i teritorijalno važenje zabrane konkurencije. Samo pod tim uslovima, a u slučaju da zaposleni prekrši zabranu konkurencije, poslodavac ima pravo da od zaposlenog zahteva naknadu štete.

Kao i prilikom zaštite bilo koje druge vrednosti korporacije, pre određivanja mera zaštite neophodno je sprovesti procenu rizika, u ovom slučaju od nezakonitog pribavljanja, korišćenja i otkrivanja informacija koje predstavljaju poslovnu tajnu. Bezbednosna provera koju preduzimaju zaposleni iz sektora korporativne bezbednosti prema licima koja konkurišu za rad u korporaciji, kao i tokom radnog angažovanja, je jedna od stalnih proaktivnih mera zaštite poslovne tajne, dok je brza inter-

na istraga u slučaju saznanja da je došlo do njenog odavanja neophodna reaktivna mera.

Zbog sve veće upotrebe IKT sistema u poslovanju, potrebno je obezbediti njihovu adekvatnu zaštitu, posebno onih sistema koji pripadaju organizacijama od posebnog značaja, u koje se pored organa javne vlasti ubrajaju kompanije koje se bave delatnošću od opšteg interesa i to u oblastima proizvodnje i prenosa električne energije, prometa nafte i naftnih derivata, elektronske komunikacije, finansijske institucije i druge. Pored fizičke zaštite objekata i prostorija, odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema koji se koriste za obradu i čuvanje poslovne tajne, neophodno je uspostaviti strogu kontrolu pristupa i dodele dozvola, odnosno pristupnih prava za svaki dokument. Pored ostalog, mere zaštite od bezbednosnih rizika IKT sistema moraju da omoguće i postizanje bezbednog rada na daljinu i upotrebu mobilnih uređaja, zaštitu nosača podataka, kriptozaštitu, a potrebno je da otkriju i otklone pretnje od zlonamernog softvera, kao i da zaštite sistem od "curenja informacija" i svih drugih pretnji i slabosti i to na način predviđen zakonskim propisima, primenom bezbednosnih standarda (pre svih primenom serije standarda ISO 27000) i najbolje prakse.

Iniciranje i realizacija programa edukacije je nezaobilazan zadatak funkcije korporativne bezbednosti koja, kada je u pitanju zaštita poslovne tajne, za krajnji cilj ima podizanje svesti o značaju i načinju njenog čuvanja, ali i da ukaže na štetne posledice po korporaciju i zaposlene, odnosno da naglasi njihovu odgovornost u slučaju odavanja.

Visokotehnološki kriminal ("sajberkriminal")

Jedan od savremenih oblika ugrožavanja, koji sa razvojem tehnike i interneta svakoga dana postaje sve izraženiji i kompleksniji, jeste visokotehnološki kriminal, popularniji pod nazivom kompjuterski/računarski kriminal, a u novije vreme sve prisutniji pod terminom "sajber kriminal" (eng. cybercrime).Visokotehnološki kriminal obuhvata skup krivičnih dela i u smislu *Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*[43] predstavlja

> *"vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku".*

43 „Službeni glasnik RS", br. 61/2005, 104/2009, 10/2023 i 10/2023 – dr. zakon.

Podaci iz Strateške procene javne bezbednosti koji govore da je visokotehnološki kriminal zastupljen s manje od 1% u ukupnom kriminalu na teritoriji Republike Srbije, ne smeju da nas navedu na pogrešne zaključke o postojanju minimalnih rizika od ovog oblika pretnje po korporacije, jer su, kako je dalje u tekstu procene navedeno, porast broja i posledice ispoljavanja različitih vidova visokotehnološkog kriminala trenutno nesagledive, a moramo navesti i pitanje postojanja veličine tamne brojke.

Jedna od glavnih karakteristika sajber kriminala, koja otežava poslove internih istraga, je ta da učinioci ovih dela ne moraju da budu, i po pravilu ne ostvaruju neposredni fizički kontakt sa vrednostima organizacije koje su im meta napada, odnosno ova dela mogu da se vrše na različitim geografskim lokacijama u realnom vremenu. Prilikom istraga moramo biti svesni i poznavati moguće nosioce sajber incidenata koji, prema smernicama[44] za izbor dobavljača koji pružaju usluge odgovora na sajber incidente, mogu uslovno biti podeljeni na nosioce "tradicionalnih" IT bezbednosnih incidenata (učinjeni od strane:

- sitnih kriminalaca;
- individualaca ili grupa koji dela čine iz zabave;
- lokalnih ili u određenim grupama ujedinjenih učinilaca - haktivista;
- insajdera) i
- nosioce sajber bezbednosnih napada koji mogu biti učinjeni od strane organizovanih kriminalnih grupa, napadača podržanih od strane određenih država, kao i delovanjem ekstremnih grupa.

Samo na osnovu prethodno navedenih nosioca sajber napada može se uočiti sva kompleksnost i sofisticiranost ovih dela, koji u znatnoj meri mogu da otežaju interne istrage i druge reaktivne aktivnosti, te ukazuje da akcenat delovanja poslova sajber bezbednosti mora biti usmeren na prevenciju, edukaciju i druge preventivne i proaktivne mere borbe protiv sajber kriminala. U prilog ovoj konstataciji ide i činjenica, a koju mnogi zanemaruju, da ostvarivanje sajber bezbednosti nije samo tehničko-tehnološko pitanje, već su sajber napadi, pre svega, omogućeni ljudskim delovanjem (činjenjem ili nečinjenjem). Kako ističe i visoki predstavnik EU za spoljne poslove i

44 *Cyber Security Incident Response Supplier Selection Guide*,Version 1. 2013., CREST, Slough UK, 2013.

bezbednosnu politiku, u dokumentu o izgradnji sajber bezbednosti EU[45], oko 95% sajber incidenata omogućeno je

> *"nekom vrstom ljudske greške - namerne ili nenamerne, odnosno da je u pitanju bio izražen ljudski faktor".*

Rezultat uspešnih sajber napada je ostvarivanje negativanog uticaja na bezbednost mrežnih i informacionih sistema, čime se postiže neovlašćeno pristupanje IKT sistemima, odnosno narušavanje integriteta, raspoloživosti, autentičnosti i neporecivosti podataka koji su u njima, i onemogućavanje tih sistema da funkcionišu kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica. Postoje različite vrste sajber napada, ali se oni generalno mogu klasifikovati u četiri osnovne kategorije[46]:

1. presecanje, prekidanje (engl. interruption) - je napad na raspoloživost;
2. hvatanje (engl. interception) - je napad na poverljivost;
3. izmena (engl. modification) - je napad na integritet;
4. proizvodnja tj. fabrikovanje (engl. fabrication) - je napad na autentičnost.

Na pretnje od sajber kriminala posebnu pažnju moraju da obrate organizacije koje pripadaju kritičnoj infrastrukturi, jer od otpornosti i bezbednosti njihovog poslovanja zavise i ukupni ekonomski, zdravstveni i drugi sistemi na kojima počiva funkcionisanje celokupne države. Kako bi bezbedno i u kontinuitetu isporučivale svoje usluge i proizvode, kritične infrastrukture, ali i druge organizacije moraju da preduzimaju set mera, odnosno neophodno je da sprovode određene funkcije, koje prema okviru[47] za sajber bezbednost sačinjenog od strane američkog nacionalnog instituta za standarde i tehnologiju NIST, pružaju najviši nivo strukture za organizovanje osnovnih aktivnosti sajber bezbednosti. Te funkcije su:

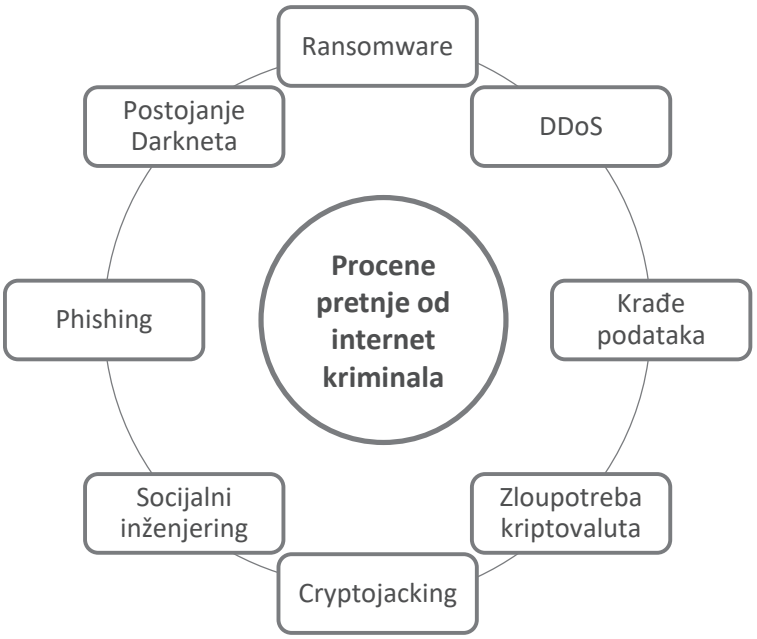
- identifikacija,
- zaštita,

45 *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN (2017) 450 final, European Commisssion, Brussels, 13.9. 2017.

46 Pleskonjić Dragan, Maček Nemanja, Đorđević Borislav, Carić Marko, *Sigurnost računarskih mreža*, Viša elektrotehnička škola, Beograd, 2006., str. 2 – 4.

47 *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018., NIST, Gaithersburg MD, 2018.

- detekcija,
- odgovor i
- oporavak.



Slika 1.2. Procene pretnje od internet kriminala

U cilju uspostavljanja adekvatnog sistema odbrane i primene integrisanih mera zaštite od sajber pretnji, mogu nam biti od koristi i podaci iz procene[48] pretnje od internet organizovanog kriminala iz 2018. godine izrađene od strane Europola, u kojoj su navedeni sledeći ključni nalazi:

- Ransomware je zadržao dominaciju, motivisan finansijskom zaradom, ali i za dolaženje do različitih podataka koji će služiti za dalju zloupotrebu (ličnih i poslovnih podataka za pristup bankovnim računima i sl.);
- DDoS nastavlja da bude istaknuta pretnja privatnom i javnom sektoru;
- Krađe podataka (i dalja preprodaja na Darknetu) i prevare platnim karticama i dalje su visoko zastupljene, bez obzira na blagi opadajući trend;

48 *Internet organised crime threat assessment (IOCTA) 2018*, Europol, The Hague NL, 2019.

- Sa porastom zloupotreba kriptovaluta njihovi korisnici postaju sve više mete napada;
- Cryptojacking postaje novi trend sajberkriminala (odnosi se na zloupotrebu eksploatacije propusnog opsega Internet korisnika i procesorske snage pri "rudarenju" kriptovaluta);
- Socijalni inženjering je i dalje pokretač mnogih sajber kriminalnih dela;
- Socijalni inženjering je i dalje visoko prisutan (phishing ostaje najčešći oblik socijalnog inženjeringa, dok ga prate vishing i smishing).

Socijalni inženjering se koristi za postizanje niza ciljeva:

- o za dobijanje ličnih podataka,
- o zloupotrebu bankovnih računa,
- o krađu identiteta,
- o iniciranje nelegitimnog plaćanja, ili
- o za ubeđivanje žrtve da nastavi sa bilo kojom drugom aktivnošću protiv njihovog ličnog interesa, kao što su transfer novca ili deljenje ličnih podataka);

- Postojanje Darknet za potrebe nelegalnog tržišta (i pored gašenja nekoliko najvećih Darknet tržišta 2017. godine, kao što su AlphaBay, Hansa i RAMP, brzo dolazi do migracije korisnika prema postojećim ili novoformiranim tržištima, ili potpuni prelazak na druge platforme, kao što su enkriptovane aplikacije za komunikaciju).

Na teritoriji Republike Srbije sve su češće i prevare na štetu pravnih lica poznate kao "kompromitovani poslovni imejl" (business compromised email) i "rensomver" (ransomware), tj. "softver za ucenu". Pojavile su se i "CEO" prevare, u kojima se izvršioci preko elektronskih poruka lažno predstavljaju kao nadređeni (šefovi, rukovodioci ili direktori) i od žrtava, zaposlenih u privrednim subjektima, traže da uplate novac na njihov račun. Koristeći autoritet nadređenog lica i socijalni inženjering, oni sastavljaju poruke koje deluju sasvim autentično i stilom podražavaju stvarnu situaciju, tako da zaposleni nimalo ne sumnjaju da je potrebno izvršiti traženu uplatu. Elektronske adrese često podražavaju stvarne adrese nadređenih. U manjem broju slučajeva kompromituju se i elektronske adrese nadređenih. Tada su prevarne poruke još opasnije jer je teško uočiti razliku između adresa. Izvršioci su u takvim slu-

jevima detaljno upoznati s načinom na koji nadređeni komunicira sa zaposlenima, što koriste za prilagođavanje stila komunikacije.[49]

Uprkos sve većoj digitalizaciji poslovanja i povećanja problematike sajber pretnji i rizika, načelno možemo reći da korporacije, ali i druga pravna lica nisu u potpunosti spremni za adekvatnu odbranu od njih. U prilog tome govore i podaci iz istraživanja[50] globalno prisutne revizorske organizacije Pricewaterhouse Coopers, u kojem je utvrđeno da više od polovine ispitanih kompanija nije usvojilo i ne primenjuje ključne procese (procenu ranjivosti, penetraciono testiranje i dr.) za identifikaciju i upravljanje sajber rizicima u poslovanju.

Za koordiniranje radnji prevencije i borbe protiv sajber kriminala u okviru funkcije korporativne bezbednosti zaduženi su, pre svega, poslovi sveukupne bezbednosti informacija, koji po pravilu uključuju i poslove bezbednosti IKT sistema (eng. IT security/ICT security/computer security/cybersecurity) – o čemu će biti reči u delu Bezbednost informacija, Bezbednost IKT sistema (cybersecurity).

Imovinski delikti

Najzastupljeniji oblik opšteg kriminala jesu imovinski delikti, a u strukturi imovinskog kriminaliteta *krađa*[51] zauzima vodeće mesto po broju izvršenih, ali i otkrivenih krivičnih dela. U tom smislu nosioci funkcije korporativne bezbednosti moraju biti upoznati sa krivično pravnim normama, bićem krivičnih dela protiv imovine i načinom izvršenja, kako bi na adekvatan način implementirali zaštitne mere i kontrole, kao i predvideli blagovremene reaktivne postupke za potrebe odgovora i otkrivanja dela, čime bi ublažili posledice i učestvovali u daljem internom ili eksternom procesiranju. Pored krađe kao osnovnog krivičnog dela, ili kako se još naziva prosta ili obična krađa, korporativna bezbednost mora da uzme u obzir, odnosno svoje mere mora usmeriti na sprečavanje i/ili ublažavanje vršenja i krivičnih dela *sitne krađe* (član 210.KZ) i *teške krađe* (član 204.KZ).

Krivično delo sitne krađe, koje se odnosi i na delo sitne utaje i prevare, je veoma interesantno jer predstavlja lakši ili privilegovani oblik krađe s obzirom da je, izme-

49 *Strateška procena javne bezbednosti*, op. cit., str. 61.

50 *Strengthening digital society against cyber shocks, Key findings from The Global State of Information Security Survey 2018*, PwC, 2019, p. 11.

51 Delo inkriminisano članom 203. KZ „Ko tuđu pokretnu stvar oduzme drugom u nameri da njenim prisvajanjem sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se …".

đu ostalog, vezan za vrednost ukradene ili utajene stvari (trenutno ako ne prelazi iznos od 5000 RSD). Ako se doda i inertnost organa gonjenja prema ovom delu, kao i činjenica da ako je izvršeno na štetu privatne imovine gonjenje se preduzima po privatnoj tužbi, korporacije su prepuštene sebi pri rešavanju ovog problema (krađa, utaja ili prevara vezana za sitni inventar, rezervne delove, energente i dr.). Iz razloga što učestalo vršenje ovog dela u dužem vremenskom intervalu može da poremeti funkcionisanje i utiče na ugled i imidž korporacije neophodno je preduzimanje mera i kontrola na eliminaciji uzroka i ublažavanju posledica od ovog dela, bez obzira što se njime pribavlja mala imovinska korist, odnosno prouzrokuje mala šteta.

Za potrebe izgradnje optimalnog sistema korporativne bezbednosti bitno je istaći da ukoliko je obična krađa izvršena pod otežavajućim okolnostima (obijanjem ili provaljivanjem zatvorenih zgrada, stanova, soba, kasa, ormana ili drugih zatvorenih prostora ili savlađivanjem mehaničkih, elektronskih ili drugih većih prepreka; od strane grupe; na naročito opasan ili drzak način; od strane lica koje je pri sebi imalo kakvo oružje ili opasno oruđe radi napada ili odbrane; za vreme požara, poplave, zemljotresa ili drugog udesa; iskorišćavanjem bespomoćnosti ili drugog teškog stanja nekog lica), kao i kada vrednost ukradenih stvari prelazi 450.000 RSD, odnosno 1.500.000 RSD, tada takva krađa postaje teška krađa. Uzimajući u obzir i činjenicu da je ovo delo učinjeno bez obzira na vrednost ukradene stvari ako ukradena stvar predstavlja kulturno dobro, odnosno dobro koje uživa prethodnu zaštitu ili prirodno dobro ili ukradena stvar predstavlja javni uređaj za vodu, kanalizaciju, toplotu, gas, električnu ili drugu energiju ili uređaje sistema javnog saobraćaja i veza, odnosno delove tih uređaja, nadležni za poslove korporativne bezbednosti u zavisnosti od delatnosti organizacije, dužni su da nakon sprovedenog postupka procene rizika usklade mere i kontrole sa veličinom verovatnoće i posledicama, odnosno sa nivoom rizika od nastupanja ovog oblika ugrožavanja.

Najteža krivična dela protiv imovine s elementom nasilja su *razbojništvo* (član 206. KZ), *razbojnička krađa* (član 205. KZ) i *iznuda* (član 214. KZ). Za potrebe izgradnje optimalnog bezbednosnog sistema bitno je naglasiti da su izvršioci razbojništva, kao najzastupljenijeg krivičnog dela protiv imovine s elementom nasilja, većinom nezaposlena lica životne dobi od 16 do 30 godina, dok su na drugom mestu lica od 31 do 40 godina života, a među kojima je zastupljen i veći broj narkomana. Takođe, potrebno je istaći da su prema podacima iz ranije pomenute *Strateške procene javne bezbednosti*

> *"naročito oružana razbojništva izvršena u objektima koji posluju s većom količinom gotovog novca, kao i razbojništva nad radnicima koji transportuju novac. U periodu 2011–2015. godine izvršena su 1.924 razbojništva u objektima koji posluju s gotovim novcem – u najvećem broju u menjačnicama (26%), na benzinskim pumpama (26%) i u kladionicama (19%), a zatim u poštama, kockarnicama i bankama. Nad transportima novca izvršeno je 35, a nad transportima robe 15 razbojništava. Kada je reč o materijalnim oštećenjima, značajne su serije razbojništava čije su mete uglavnom manji trgovinski objekti."*.

Pored mnogobrojnih i raznovrsnih proaktivnih i reaktivnih mera u cilju sprečavanja ili ublažavanja posledica izvršenja ovog krivičnog dela možemo izdvojiti to da na

> *"vršenje razbojništava u velikoj meri utiču izostanak adekvatnih mera fizičko-tehničke zaštite rizičnih objekata i nizak nivo bezbednosne kulture"*[52],

kao i saradnju sa policijskim snagama, odnosno jačanje i produbljivanje javno-privatnog i privatno-privatnog partnerstva[53].

Iako ne spada u grupu imovinskih delikata, sa razbojništvom može da bude povezano krivično delo otmica (član 134. KZ), koje je bilo zastupljeno i u bližoj prošlosti nad vlasnicima ili članovima porodice vlasnika određenih pravnih lica koja posluju na teritoriji RS. Na međunarodnom planu, kao primer direktne korelacije krivičnog dela otmice i razbojništva možemo navesti primer jednog od najvećih slučajeva razbojništva u Engleskoj izvršenog 2006. godine u depou firme Securitas Cash Management Ltd, gde je pored ostalog čuvan novac i Centralne banke Engleske, a kojom prilikom je odneto oko 53 miliona britanskih funti. Razbojništvu je prethodila otmica menadžera depoa, kao i njegove supruge i deteta, od strane izvršilaca prerušenih u policajce, koji su na taj način primorali menadžera da otkrije bezbednosne procedure i šifre.

Sličan ishod kao kod otmice može biti ostvaren i u slučaju krivičnog dela *ucene* gde učinilac

> *"u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist zapreti drugom da će protiv njega ili njemu bliskog lica otkriti nešto što bi njihovoj časti ili*

52 *Procena pretnje od teškog i organizovanog kriminala*, MUP Republike Srbije, Beograd 2015., str. 5.

53 *Bank Robberies – Executive Summary*, The European Banking Federation, Brussels, 2011.

> *ugledu škodilo i time ga prinudi da nešto učini ili ne učini na štetu svoje ili tuđe imovine"*[54].

Sve su češće ucene koje se ostvaruju posredstvom IKT sistema, napadima na privatnost razgovora, poruka, naloga na društvenim mrežama itd. Iz tog razloga neophodno je vlasnika, članove top menadžmenta i druga lica koja imaju određene odlučujuće odgovornosti u vezi sa vitalnim elementima organizacije, upozoriti i adekvatno obučiti, pre svega da ne dozvole da dođu u takvu situaciju, a potom i da efikasno odreaguju u slučaju ostvarenja pretnje. Takođe, funkcija korporativne bezbednosti prilikom procene rizika mora objektivno analizirati pretnje od otmice i ucene, a mere za postupanje sa rizicima potrebno je da idu u više pravaca po dubini, među kojima možemo izdvojiti razmatranje preraspodele dužnosti i ovlašćenja (prava potpisa i pristupa i dr.), kako ostvarenje pretnji ne bi imalo značajan negativan uticaj na lica, imovinu ili poslovanja organizacije.

Opasnosti i ranjivosti kao ugrožavajući elementi

Opasnost

Jedan od mogućih ugrožavajućih elemenata korporacije jeste i *opasnost* (eng. hazard), koja prema ISO 22300 predstavlja izvor potencijalne štete, a može predstavljati i izvor rizika. Prilikom prevođenja na srpski jezik za hazard se ne koristi uvek identičan pojam, a često se prevodi kao potencijalna opasnost.

Takođe, zbog čestog poistovećivanja pojma opasnost sa pretnjom, smatramo da je potrebno ukazati na određene međusobne razlike, iako i jedan i drugi oblik ugrožavanja može štetno da utiče na lica, imovinu i poslovanje organizacije, a neophodno ih je sinhronizovano i sveobuhvatno analizirati i tretirati. Kao što je napomenuto u rečniku izdatom od strane britanskog *Instituta za kontinuitet poslovanja*[55] pojmovi pretnja i opasnost su često međusobno zamenljivi, s tim da se ugrožavanja koja potiču od katastrofa, odnosno od elementarnih nepogoda ili tehničko-tehnoloških nesreća, obično nazivaju opasnosti (hazards). Zato je prevencija i od opasnosti i od pretnji jedna od osnovnih zadataka funkcije korporativne bezbednosti, kako bi se sprovođenjem adekvatnih mera, kontrola, procesa i tehnika, kao i optimalnom upo-

54 Član 215. KZ.

55 *Dictionary of Business Continuity Management Terms*, The Business Continuity Institute, Reading UK, 2011.

trebom proizvoda, usluga ili resursa, izbegle, smanjile ili kontrolisale te opasnosti i pretnje, kao i rizici povezani sa njima, i kako bio se smanjila njihova potencijalna verovatnoća pojavljivanja ili posledice ostvarenja.

U okviru poslova korporativne bezbednosti identifikacija opasnosti je uslovljena *Zakonom o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama*[56], koji opasnost definiše kao

> *"potencijalno štetan fizički događaj, fenomen ili ljudska aktivnost koja može prouzrokovati ugrožavanje života i zdravlja ljudi, oštećenje materijalnih i kulturnih dobara i životne sredine ili društvene i ekonomske poremećaje".*

Podzakonskim aktom[57] kojim se propisuje metodologija izrade i sadržaj procene rizika od katastrofa i planova zaštite i spasavanja, utvrđena su jedinstvena merila za izradu procene rizika od katastrofa, koja, pored ostalog određuju načina izrade i određivanja opasnosti za koje će se raditi procena. Za opis izabrane opasnosti (od zemljotresa, poplava i ekstremnih vremenskih pojava, preko epidemije i pandemije, do tehničko-tehnoloških nesreća i terorističkih napada) potrebno je koristiti parametre predviđene metodologijom u obimu kojim se stiče jasna slika o verovatnoći pojavljivanja i posledicama. Navedena procena prethodi izradi plana zaštite i spašavanja (od nacionalnog i planova državnih organa i posebnih organizacija do planova subjekata od posebnog značaja za zaštitu i spasavanje i privrednih društava i drugih pravnih lica koji predstavljaju kritičnu infrastrukturu), kojim se planiraju mere i aktivnosti za sprečavanje i umanjenje posledica katastrofa, i koji mora, između ostalog, da sadrži mere zaštite i spasavanja po vrstama opasnosti. Takođe, potrebno je naglasiti da je identifikaciju opasnosti neophodno da sprovode organizacije koje obavljaju aktivnosti u kojima je prisutna ili može biti prisutna jedna ili više opasnih supstanci u propisanim količinama. Shodno *Pravilniku o načinu izrade i sadržaju Plana zaštite od udesa*[58] opasnost od udesa predstavlja

> *"svojstvo opasnih supstanci ili skup određenih okolnosti u vezi sa opasnim supstancama, koje mogu prouzrokovati štetu po zdravlje ljudi i životnu sredinu",*

56 „Službeni glasnik RS", br. 87/2018.

57 *Uputstvo o Metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja* („Službeni glasnik RS", br. 80/2019).

58 „Službeni glasnik RS", br. 41/2019.

a plan mora da sadrži procenu opasnosti koja započinje identifikacijom opasnosti, odnosno identifikacijom kritičnih tačaka, tj. mesta u procesu ili na postrojenju koja predstavljaju najslabije tačke ili moguće izvore opasnosti sa aspekta nastajanja udesa, a sa posebnim osvrtom na analizu ljudskog faktora kao mogućeg uzroka udesa.

Identifikacija opasnosti, odnosno okolnosti ili stanja koja mogu ugroziti zdravlje ili izazvati povredu zaposlenog, sprovodi se shodno *Zakonu o bezbednosti i zdravlju na radu*[59]. Korporacija kao poslodavac je dužna da utvrdi moguće vrste opasnosti, ali i i štetnosti na radnom mestu u radnoj sredini, na osnovu kojih se vrši procena rizika od nastanka povreda i oštećenja zdravlja zaposlenog. Na navedonoj identifikaciji zasniva se akt o proceni rizika koji je poslodavac dužan da donese za sva radna mesta u radnoj sredini, kao i da utvrdi način, mere i rokove za otklanjanje ili smanjenje rizika.

U skladu sa *Zakonom o privatnom obezbeđenju* potencijalnu opasnost je potrebno identifikovati i prilikom procene rizika u zaštiti lica, imovine i poslovanja, i to po zahtevima i na način propisan važećim srpskim standardom u oblasti privatnog obezbeđenja. U tom smislu, a shodno ciljevima procesa procene rizika, potrebno je sprovesti identifikaciju potencijalnih opasnosti, izvora opasnosti, događaj ail i niza okolnosti i njihovih potencijalnih posledica, a moraju biti uključene sve opasnosti, bez obzira na to da li su pod kontrolom organizacije ili nisu i bez obzira na to da li su u datom momentu aktuelne ili ne. Potrebno je naglasiti da opasnosti koje u početnoj fazi procene nisu identifikovane, neće biti obuhvaćene daljom analizom, odnosno neće se razmatrati uzrok i izvor tih potencijalnih opasnosti, pozitivne i negativne posledice, kao i verovatnoća pojavljivanja.

U okviru funkcije korporativne bezbednosti zadatak identifikacije i tretmana opasnosti nalazi se u okviru poslova "*safety*", što je još jedan od pojmova preuzetih sa engleskog govornog područja za koji ne postoji jedinstven i adekvatan termin u srpskom jeziku, a često se poistovećuje i prevodi kao "bezbednost" (eng. security), iako ima drugačije značenje. Takođe, pojam safety se često upotrebljava i prevodi kao "sigurnost". Pojedini autori safety objašnjavaju kao stanje koje je zaštićeno od prirodnih i veštačkih pojava, radnji, procesa i sredstava koja po svom prirodnom, unutrašnjem svojstvu mogu da prouzrokuju povredu, smrt, materijalnu štetu ili drugi neželjeni ishod. Za razliku od safety, bezbednost (security) je stanje zaštićeno od pretnji, odnosno dela učinjenih (ili propuštanjem da se nešto uradi) sa name-

59 „Službeni glasnik RS", br. 35/2023.

rom prouzrokovanja povrede, smrti, materijalne štete ili drugog neželjenog ishoda. Upravo različitost između opasnosti i pretnje pravi distinkciju između poslova safety i security, odnosno delokrug safety poslova je zaštita od opasnosti (hazards), a u opisu poslova security je zaštita od pretnji (threats). Još jednom napominjemo da iz razloga što su moguće negativne posledice po lica, imovinu i poslovanje organizacije, i u jednom i u drugom slučaju iste (šteta po lica, imovinu i poslovanje), i što se zaštitne mere i kontrole međusobno nadopunjuju i prepliću, preporučljivo je, i u praksi je čest slučaj, da funkcija korporativne bezbednosti upravlja i poslovima safety i security. U suprotnom, ukoliko se poslovi safety (zbog vrste delatnosti korporacije, internih organizacionih potreba ili drugih razloga) nalaze van sektora korporativne bezbednosti njihova saradnja mora biti veoma bliska, a međusobni odnosi unapred, jasno i formalno uređeni.

Ranjivost

Ako ranjivost (eng. *vulnerability*) posmatramo kao

> *"unutrašnje svojstvo podložno izvoru rizika što može da dovede do događaja sa posledicom"*

- kako je navedeno u rečniku datim međunarodnim smernicama za upravljanje rizicima[60], odnosno kao

> *"slabost sredstva ili kontrole koja može biti iskorišćena od strane jedne ili više pretnji"*[61],

možemo zaključiti da ona svakako predstavlja značajan ugrožavajući element i suprotna je karakteristika otpornosti korporacije. Takođe, potrebno je imati u vidu da sve što je čovek osmislio i stvorio, u materijalnom ili nematerijalnom obliku, nikad nije stoprocentno neranjivo i nosi sa sobom određene slabosti.

Sledeća svojstva unutar korporacije mogu biti podložna izvoru rizika i iskorišćena od strane pretnji:

60 *ISO/Guide 73:2009, Risk management — Vocabulary.*

61 *ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary.*

- rukovođenje (način na koji se organizuje i upravlja bezbednosnom i svakom drugom funkcijom u kompaniji),
- ljudski faktor (njihovo realno znanje, veštine, motivisanost, zla namera, nemar itd.),
- procesi (posebno njihova adekvatna mapiranost i međuzavisnost) i
- tehničko-tehnološka ranjivost (zavisnost poslovanja od tehnologija, njihova obimnost i sveprisutnost, održavanje, daljinska dostupnost itd.).

Svojstvo čija ranjivost ima najviše uticaja na ostala i može da dovede do događaja sa neotklonivim posledicama, jeste rukovođenje (eng. governance), pa je zato potrebno posebno obraćati pažnju prilikom planiranja unutrašnje organizacije i upravljačkih procesa, kao i pri sprovođenju procene rizika koja uključuje proces identifikacije svih ranjivosti. Odgovorno za ukupnu unutrašnju organizaciju, kao i za nivo bezbednosne svesti i kulture svih zaposlenih, odnosno za celokupnu radnu atmosferu, neadekvatno rukovođenje od strane top menadžmenta (pre svega neshvatanje i nedavanje podrške funkciji korporativne bezbednosti, nerazdvajanje određenih dužnost, nerazvijanje adekvatnih programa prevencije i dr.) može da stvori uslove da i druga svojstva mogu biti iskorišćena od strane jedne ili više pretnji. Naravno, i neadekvatno rukovođenje funkcijom korporativne bezbednosti povlači sa sobom značajnu ranjivost celokupne organizacije. U tom smislu, pomoć u sagledavanju i proceni složenosti sistema organizacije možemo potražiti i u važećim smernicama *ISO/TS 22375*[62], predviđenih za primenu principa i procesa koji omogućavaju organizaciji da identifikuje potencijalne skrivene ranjivosti svog sistema i da obezbedi ranu indikaciju rizika usled složenosti, čime sveobuhvatno može da se utiče i poboljša njena ukupna otpornost i bezbednost. Od značaja je i primena standarda *SRPS EN ISO/IEC 29147*[63] koji pruža zahteve i preporuke organizacijama u otkrivanju ranjivosti proizvoda i usluga, omogućavajući korisnicima da upravljaju tehničkom ranjivošću.

Ugroženost organizacije od strane ranjivosti uočena je i od strane zakonodavca koji je *Zakonom o kritičnoj infrastrukturi* propisao operatorima kritične infrastrukture obavezu da moraju odrediti *oficira za vezu* koji je, pored ostalog, u obavezi da obaveštava MUP o evaluaciji ranjivosti. Dok naši nadležni organi određuju početne korake u identifikaciji kritične infrastrukture, mnoge evropske države, uključujući i

62 *ISO/TS 22375, Security and resilience — Guidelines for complexity assessment process.*

63 *SRPSENISO/IEC 29147:2020, Informacione tehnologije – Tehnike bezbednosti – Otkrivanje ranjivosti.*

zemlje iz okruženja, poseduju niz podzakonskih akata kojim se, pored ostalog, uređuje način analize rizika poslovanja kritičnih infrastruktura, u okviru čega se propisuje i analiza ranjivosti, odnosno merila i kriterijumi za identifikaciju ranjivosti.

Dobar osnov za početak procene ranjivosti može poslužiti analiza rizika u zaštiti lica, imovine i poslovanja, odnosno određivanje verovatnoće shodno važećem standardu *SRPS A.L2.003*, gde su u *Prilogu N* određeni kriterijumi za određivanje ranjivosti.

Jedna od stalnih kontrolnih mera mora da bude i provera ranjivosti podataka i informacija iz razloga što predstavljaju jedne od najvažnijih, a ujedno i najranjivijih vrednosti svake organizacije. Inače, skeniranje ranjivosti je naročito razrađeno u oblasti informacione bezbednosti, gde oblici ranjivosti mogu biti različiti, uključujući nepravilno podešen ili instaliran hardver ili softver, neadekvatnu fizičku bezbednost, neodgovarajuću obuku zaposlenih, neadekvatno upravljanje incidentima, kašnjenje u primeni i testiranju softvera i zakrpa itd. Prema tehničkom smernicama[64] za testiranje i procenu informacione bezbednosti američkog nacionalnog instituta za standarde i tehnologiju NIST, za potrebe provere ranjivosti mogu se koristiti sledeće tehnike:

- socijalni inženjering,
- penetraciono testiranje,
- razbijanje lozinki (eng. password cracking) i
- testiranje bezbednosti aplikacija.

Svaka korporacija može interno testirati ranjivost, ali za objektivnu identifikaciju pojedinih ranjivih tačaka praksa je pokazala da je efikasnije angažovanje eksternih izvršioca. Pored mnogobrojnih prednosti korišćenja usluga eksternih pružalaca za potrebe skeniranja ranjivosti (usko stručna znanja, veća objektivnost itd.), treba imati u vidu postojanje određenih problema u smislu otkrivanja sopstvenih slabosti drugim licima koji takva saznanja mogu zloupotrebiti. Visoko razvijene zemlje, kao i asocijacije određenih industrijski grana taj problem rešavaju na način javnog objavljivanja spiska pravnih lica koja imaju odobrenje za pružanje usluga testiranja ranjivosti, odnosno da pored zadovoljenja stručnih i etičkih uslova, prolaze i bezbednosnu proveru.

64 *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, Gaithersburg MD, 2008.

Testiranje ranjivosti celokupnog sistema bezbednosti korporacije ili samo pojedinih delova, mora da bude redovna radnja koju je, u zavisnosti od delatnosti i specifičnosti organizacije, potrebno izvoditi u unapred određenim vremenskim periodima (nedeljno, mesečno, kvartalno itd.) ili se sprovodi nakon nastanka određenih promena, odnosno ad hoc shodno određenim dešavanjima i procenama. Svaka provera ranjivosti mora biti dokumentovana, a dalji proces analiza i procene neophodno je da inicira mere i kontrole za ublažavanje i/ili eliminaciju rizika od ranjivosti.

Bezbednosni rizici

Nezavisno od vrste i veličine sve organizacije se suočavaju sa različitim rizicima koji mogu da utiču na ostvarivanje kako njihovih vizija i misija, tako i na realizaciju operativnih i drugih ciljeva. Vlasnike i rukovodstvo korporacije interesuju svi oni interni i eksterni rizici koji mogu da ugroze poslovanje, odnosno da dovedu do smanjenja, kao i propadanja ili prekida u pružanju usluga ili proizvodnji dobara. Pored postojanja mnogobrojnih raznovrsnih rizika pri poslovanju (finansijskih, tržišnih, strateških, reputacionih itd.) fokus funkcije korporativne bezbednosti usmeren je na kompleksnu paletu rizika iz njenog predefinisanog delokruga – na bezbednosne rizike (eng. security risks).

Uz napomenu da za bezbednosni rizik ne postoji univerzalna definicija, možemo konstatovati da je rizik, pre svega, određen u rečniku termina koji se odnose na upravljanje rizikom datim međunarodnim smernicama *ISO/Guide 73*, i predstavlja

> *"efekat neizvesnosti na ciljeve"*.

Pojam bezbednosnog rizika je sporadično pojašnjen u pojedinim domaćim i stranim propisima, pa ga tako *Zakon o tajnosti podataka*[65] određuje kao

> *"stvarnu mogućnost narušavanja bezbednosti tajnih podataka",*

a smernice[66] EU o merama bezbednosti usluga platnog prometa kao

> *"rizik koji je rezultat neadekvatnih ili neuspešnih internih procesa ili eksternih događaja koji imaju ili mogu imati negativan uticaj na dostupnost, integritet i*

65 „Službeni glasnik RS", br. 104/2009.

66 *Guidelines on the security measures for operational and security risks ofpayment services under Directive (EU) 2015/2366 (PSD2),* European Banking Authority - EBA, Paris, 2018.

> *poverljivost informaciono-komunikacionih sistema i/ili informacija koje se koriste za pružanje usluga platnog prometa. Uključuje rizik od sajber-napada ili neadekvatne fizičke bezbednosti.“*

Takođe, uzimajući u obzir da *Zakon o privatnom obezbeđenju* upućuje na identifikaciju rizika u zaštiti lica, imovine i poslovanja, *Zakon o odbrani* na vojne i nevojne rizike, a *Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama* na rizike od katastrofa, možemo zaključiti da bezbednosni rizici podrazumevaju spektar rizika koji ostvaruju “efekat neizvesnosti na ciljeve“ koji se odnose na kontinuitet poslovanja organizacije, spremnost na katastrofe, fizičko-tehničku zaštitu vrednosti, odbrambene pripreme, bezbednost podataka i informacija, ekonomsku bezbednost poslovanja i druge ciljeve kojima se ostvaruje bezbednost i otpornost celokupne korporacije. A težnja ka ostvarivanju sveukupne bezbednosti i otpornosti organizacije jeste generalni cilj funkcije korporativne bezbednosti, kao rezultat koji treba postići i održavati i koji se zasniva na bezbednosnoj politici organizacije. Pored funkcije korporativne bezbednosti i svih poslova iz njenog delokruga, bezbednosni ciljevi moraju da budu predviđeni i za druge relevantne funkcije i nivoe u korporaciji.

Pošto podaci i informacije predstavljaju jednu od vitalnih vrednosti svake organizacije, neophodno je da funkcija korporativne bezbednosti posebno obratiti pažnju na identifikaciju rizika vezanih za zaštitu podataka i informacija, bez obzira u kojem se obliku nalaze. Rizik po bezbednost informacija (eng. information security risk) predstavlja

> *“rizik po poslovne operacije (uključujući misiju, funkcije, reputaciju, ugled), organizaciona sredstva, pojedince, druge organizacije, kao i naciju zbog postojanja potencijala od neovlašćenog pristupa, korišćenja, otkrivanja, prekida, modifikacije ili uništavanja informacija i/ili informacionih sistema“*[67].

Pored navedenog, identifikacija bezbednosnih rizika zahtevana je i *Uredbom o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja*[68], koja propisuje operatorima IKT

67 Pojam predviđen rečnikom termina i definicija datim u smernicama *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, Gaithersburg MD, 2011.

68 „Službeni glasnik RS”, br. 94/2016.

sistema od posebnog značaja, da preispituju akt o bezbednosti u skladu sa promenama u okruženju i u samom IKT sistemu. Prema navedenoj Uredbi povećana izloženost IKT sistema bezbednosnim rizicima proističe iz tih promena

> *"usled nastupanja tehničko-tehnoloških, kadrovskih, organizacionih promena u IKT sistemu i događaja na globalnom i nacionalnom nivou koji mogu narušiti informacionu bezbednost".*

U zavisnosti od veličine, unutrašnje organizacije i drugih internih potreba i faktora, odnosno shodno unapred određenom delokrugu, funkcija korporativne bezbednosti može da, pored upravljanja bezbednosnim rizicima, bude zadužena i za druge srodne rizike koji mogu imati štetan finansijski, poslovni ili reputacioni uticaj, a koji proističu od neadekvatnih ili pogrešnih internih upravljačkih i poslovnih procesa, propusta (nenamernih i namernih) u radu zaposlenih, dobavljača i drugih lica, sistema, ili potiču od eksternih događaja (krađe, prevare, požari, pandemije, neredi, odavanje poslovne tajne i drugo). Dakle, funkciji korporativne bezbednosti, posebno kod kreditnih institucija i investicionih kompanija, kao i organizacija kojima je delatnost osiguranje i reosiguranje, može biti pridodato u nadležnost, kao jedan od poslova prevencije gubitaka, i upravljanje tzv. operativnim rizicima, a koji prema propisima EU (*Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms)*[69] i *Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)* [70]) obuhvataju

> *"rizike od gubitka po osnovu neadekvatnih ili neuspelih internih procesa, kadrova ili sistema ili usled eksternih događaja".*

Mogući operativni propusti uključuju greške ili kašnjenja u obradi, ispadi tehnoloških sistema, nedovoljni kapaciteti, prevare, gubitak podataka i oticanje informacija. Pošto svi ovi rizici mogu da stvore značajne finansijske gubitke, ali i da naruše ugled i spreče organizaciju u dostizanju zacrtanih ciljeva, neophodno je da se identifikuju verovatni izvori operativnog rizika, kako unutrašnji, tako i spoljašnji, i ublaži njihov uticaj kroz korišćenje odgovarajućih sistema, politika, procedura i kontrola.

69 OJ L 176, 27.6.2013, p. 1.

70 OJ L 335, 17.12.2009, p. 1.

Pored navedenog, neophodno je identifikovati bezbednosne rizike koji su specifični za određenu delatnost, a koji su obično predefinisani od strane granskih organizacija ili samih korporacija, putem unapred predviđenih lista faktora rizika. Praksa je ukazala na potrebu stalnog preispitivanja faktora rizika, kao i periodičnog ažuriranja listi, koje su obično date u formi spiskova zahteva - ček listi.

Identifikacija, odnosno utvrđivanje bezbednosnih rizika predstavlja proces pronalaženja, prepoznavanja i opisivanja rizika, a uključuje identifikaciju izvora rizika, događaja, njihove uzroke i njihove potencijalne posledice. Dakle, identifikovanjem ranije pomenutih pretnji, opasnosti i ranjivosti, a uzimajući u obzir kritične procese i vrednosti korporacije, kao i izazove, događaje i različita scenarija, mi utvrđujemo bezbednosne rizike koje ćemo u kasnijoj fazi analizirati i ocenjivati, potom i tretirati, odnosno upravljati njima, što u osnovi predstavlja upravljanje neizvesnostima.

Nakon identifikacije bezbednosnih rizika potrebno je sačiniti registar rizika, koji predstavlja kompilaciju zapisanih informacija o svim identifikovanim rizicima, i koji posle sprovedene analize i ocene rizika uključuje i podatke o verovatnoći, posledicama, tretmanu i vlasnicima rizika.

Neophodno je istaći da je potrebno sveobuhvatno vršiti identifikaciju bezbednosnih rizika, a kasnije i integrisano upravljati njima (o čemu će biti više reči u poglavlju *Holistički princip menadžmenta korporativnom bezbednošću - Menadžment bezbednosnim rizicima*). Holistički pristup potrebno je da bude naročito zastupljen u procesu primene mera za tretman rizika, a menadžment bezbednosnim rizicima mora biti u kontekstu i sastavni deo sistema upravljanja ukupnim rizicima korporacije.

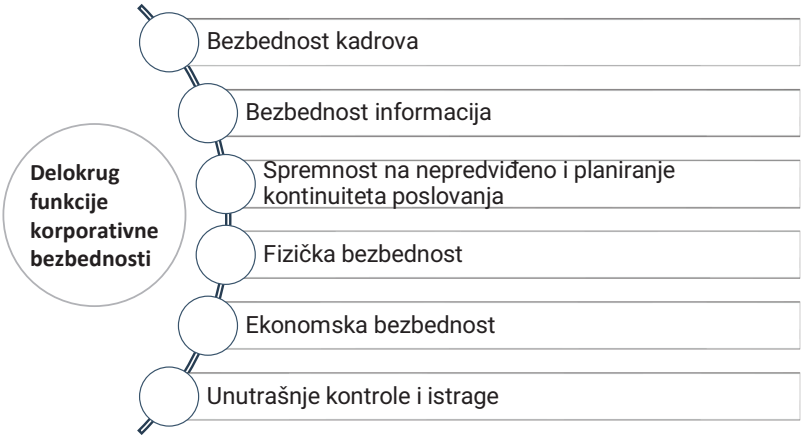
Drugo poglavlje

Delokrug funkcije korporativne bezbednosti

Sadržaj poglavlja

Unutrašnje kontrole i istrage
Unutrašnje kontrole
Unutrašnje istrage

Spektar pretnji, izazova, opasnosti i ranjivosti, kao i sa njima povezani rizici koji su navedeni u prethodnom poglavlju, ukazuju na raznovrsnost izvora, nosioca i oblika ugrožavanja korporacije, a koji pak nagoveštavaju delikatnost i odgovornost poslova i funkcije korporativne bezbednosti na izgradnji sistema koji će omogućiti optimalan nivo bezbednosti i podići stepen otpornosti organizacije na željeni nivo, uz obezbeđenje njenog nesmetanog funkcionisanja i kontinuitet poslovanja.



Slika 2.1. Delokrug funkcije korporativne bezbednosti

Zaštita bilo koje vrednosti korporacije, kao i ostvarivanje njene ukupne bezbednosti i otpornosti, ne može se postići primenom samo jednog od poslova iz delokruga funkcije korporativne bezbednosti, ma koliko on bio značajan. Ključna stvar je u ostvarivanju integrisane bezbednosne arhitekture, gde će svi poslovi biti zastupljeni na holističkom principu. Takođe, ni jedna vrednost ne može biti zaštićena, odnosno ni jedan od poslova korporativne bezbednosti ne može da se optimalno realizuje primenom samo jedne mere ili kontrole iz njenog opsega, već isključivo sveobuhvatnim, integrisanim setom radnji, procesa, sredstava i drugih elemenata primenjenim „po dubini". Uspostavljanje i sprovođenje pristupa „odbrane po dubini" (eng. defence-in-depth) podrazumeva višeslojne mere i kontrole koje uključuju ljudsko delova-

nje, organizacione i druge procese, kao i tehničko-tehnološki aspekt. Takvu zaštitu treba shvatiti kao definisanje više od jedne mere ili kontrole koje pokrivaju isti rizik[1].

Mere i kontrole koje su zastupljene u svim poslovima korporativne bezbednosti, a koje mogu biti preventivnog, proaktivnog ili reaktivnog karaktera, imaju za cilj preduzimanje radnji kako bi se smanjila verovatnoća da će se scenarija pretji, opasnosti i ranjivosti ostvariti, ili da se smanje verovatne posledice, kao i da u što kraćem vremenu organizacija nastavi poslovanje i oporavi se od remetilačkog, štetnog događaja. Sve mere i kontrole možemo generalno podeliti na organizacione, normativne, kadrovske (fizičke) i tehničke.

Teorija i praksa nam ukazuju da potpunu, apsolutnu bezbednost i otpornost ne možemo postići, ali možemo, preduzimanjem svih potrebnih mera i kontrola u okviru poslova korporativne bezbednosti, izgraditi sistem menadžmenta korporativnom bezbednošću koji će u velikoj meri moći kontrolisati rizike i stanje, što preciznije predviđati i adekvatno odgovoriti u slučaju neplanskog narušavanja bezbednosti organizacije, odnosno povratiti i oporaviti stanje na unapred definisan željeni nivo. Pored primene zaštitnih mera, odnosno izbora čitavog spektra odgovarajućih kontrolana osnovu sprovedene procene rizika, korporacija može, i preporučljivo je da osigura[2] određene vrednosti, za šta će moći koristiti i zahteve i kriterijume koji će, kako je najavljeno važećim standardom *SRPS A.L2.003*, biti definisani u posebnom delu – *Deo 6: Oblast životnog i neživotnog osiguranja*.

Raznovrsna domaća i strana stručna literatura je ukazala na širok spektar poslova korporativne bezbednosti, različito grupisanih, čak i različito pojmovno određenih, ali praksa (zasnovana na domaćem i međunarodnom iskustvu) ukazuje da

1 Primera radi, rizik od odavanja poslovne tajne ne može se umanjiti ili eliminisati samo donošenjem internog opšteg akta o zaštiti poslovne tajne ili primenom mera fizičko-tehničke zaštite. Takođe, ni gotov novac u sefu/trezoru nije bezbedan ukoliko je samo određen adekvatan prostor za smeštaj, a nije predviđeno ko, kako i kada može da mu pristupi, niti je sprovedena obuka zaposlenih koji učestvuju u svim procesima toka gotovog novca, ako nisu predviđene procedure protiv različitih zloupotreba i dr. Slično je i sa npr. sajber pretnjama gde primena jedne ili više mera koje podrazumevaju isključivo tehnološki aspekt ne mogu da pruže potpunu zaštitu podataka i informacija u IKT sistemima. Isto važi za bilo koji drugi oblik ugrožavanja, bez obzira da li potiče od strane ljudskog ponašanja, prirodnog delovanja ili tehničko-tehnoloških nesreća. Posebno neće biti od pomoći primena samo jedne mere ili kontrole u slučaju da dođe do ostvarenja neke od pretnje (npr. odata je poslovna tajna, nastao je manjak gotovog novca ili je ukraden, nastupio je sajber napad, požar itd.) i nastanka štete, kada se mora adekvatno odgovoriti, istražiti i ostvariti nastavak realizacije radnih procesa i kontinuitet poslovanja.

2 Pod osiguranjem podrazumevaju se poslovi osiguranja uređeni *Zakonom o osiguranju* ("Službeni glasnik RS", br. 139/2014).

su u delokrugu funkcije korporativne bezbednosti generalno zastupljeni poslovi koji će biti navedeni u nastavku izlaganja. Svakako, to ne isključuje mogućnost da, usled različitih internih i eksternih uticaja i potreba, pojedini predmetni poslovi ne budu sastavni deo ove funkcije, kao i da određeni drugi „nebezbednosni" poslovi budu pridodati delokrugu organizacione celine nadležne za upravljanje sistemom ukupne bezbednosti i otpornosti. Ali moramo istaći da samo principom integracije svih bezbednosnih poslova i holističkom implementacijom mera i kontrola možemo očekivati izgradnju optimalnog i održivog sistema koji će moći na adekvatan način da upravlja lepezom bezbednosnih rizika i omogućiti organizaciji dalje poslovanje i razvoj, uz poštovanje principa ekonomičnosti[3].

Delokrug funkcije korporativne bezbednosti koji je izložen u Priručniku proističe iz praktične potrebe za konvergencijom poslova bezbednosti i otpornosti u smislu obuhvatanja svih elemenata bezbednosti i poslovnih ciklusa, stvarajući jedinstven bezbednosni okvir. Istraživanja su pokazala, a praksa je potvrdila, da efikasan okvir za objedinjenje poslova bezbednosti i otpornosti mora uvrstiti sve zaposlene, procese i strategije koji organizaciji omogućavaju prevenciju, detekciju, odgovor i oporavak od svih bezbednosnih incidenata i događaja. Ukazano je na potrebu korporacija za premeštanjem fokusa sa nepovezanih pojedinačnih funkcija i elemenata bezbednosnog životnog ciklusa (prevencija, detekcija, odgovori, oporavak) na fokus celovitog, jedinstvenog poslovnog ciklusa kao sistema upravljanja.[4] Bez obzira na dostignuti stepen konvergencije, koja je određena organizacionom strukturom i linijama izveštavanja, neophodno je da organizacija ima jedinstven, integrisan sistem menadžmenta bezbednosnim rizicima u svrhu usklađivanja bezbednosne odgovornosti, kao i doslednog i holističkog pristupa u tretiranju raznovrsnih bezbednosnih rizika.[5] Uloga funkcije korporativne bezbednosti u okviru principa integrisanog upravljanja ogleda se u definisanju osnovnih bezbednosnih zahteva i pružanju podrške ostalim organizacionim poslovnim celinama pri kreiranju i optimizaciji bezbednosnih koncepta za zaštitu značajnih i kritičnih resursa, procesa i identifikovanih rizika koji su u njihovom vlasništvu. Koordinirajući i kontrolišući primenu bezbednosnih zahteva u različitim poslovnim celinama kompanije obezbeđuje se

3 O značaju i načinu sveobuhvatnog pristupa u zaštiti poslovanja organizacije pogledati detaljnije: *Standard 2000-1, Wirtschaftsgrundschutz*, Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik i ASW Bundesverband, Berlin DE, 2016.

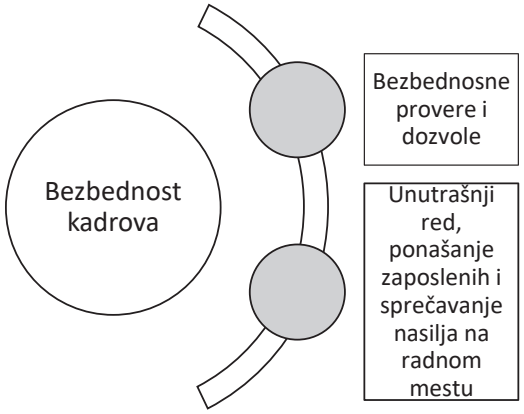
4 O konvergenciji poslova bezbednosti pogledati više: *Convergence of Enterprise Security Organizations*, Alliance for Enterprise Security Risk Management, Booz Allen Hamilton, McLean VA, 2005.

5 *Enterprise Security Risk Management: A holistic approach to security*, ASIS International, Alexandria VA, 2015.

jedinstvenost i holistički princip zaštite svih vrednosti čime se postiže željeni uniformni nivo bezbednosti.

Bezbednost kadrova

Kao što smo do sada više puta napomenuli, svi poslovi korporativne bezbednosti moraju se sprovoditi integrisano i sinhronizovano kako bi rezultati dali optimalan efekat. Ne postoje „važniji" i „manje važniji" poslovi i zato redosled izlaganja koji je prikazan u ovom Priručniku, ne ukazuje na značaj ili redosled sprovođenja predmetnih poslova. Uslovno možemo reći da bezbednost kadrova (eng. personnel security) pripada poslovima od kojeg umnogome zavisi ukupno poslovanje korporacije, iz prostog razloga što se odnosi na najvažniji potencijal svake organizacije – ljudski resurs.



Slika 2.2. Bezbednost kadrova

Pored toga što se u krajnjoj liniji ovim poslom štite i zaposleni, uvidom u delokrug bezbednosti kadrova spoznajemo da se njegovim merama i radnjama organizacija prevashodno štiti od potencijalnog (zlo)namernog ili nenamernog, štetnog delovanja zaposlenih, uključujući i zaštitu od kadrova izvođača radova, dobavljača i drugih pravnih lica sa kojima korporacija ima uspostavljenu određenu saradnju, odnosno određeni ugovorni odnos. Pretnje dolaze od sadašnjih, ali i bivših zaposlenih, pružaoca usluga ili poslovnih partnera, koji mogu zloupotrebiti svoja saznanja kako bi naštetili kadrovima, kupcima/korisnicima, imovini ili ugledu organizacije. Zato je, pored obezbeđenja adekvatne kadrovske politike i strukture zaposlenih neop-

hodno obratiti pažnju na njihove bezbednosne atribute, i u tom smislu kontinuirano izgrađivati i poboljšavati sposobnost upravljanja rizicima koji potiču od zaposlenih, bivših kadrova i drugih lica sa kojima imamo ugovorni odnos, osiguravajući na taj način integritet i pouzdanost radne snage.

Da li zbog nepotpunog regulatornog uređenja, nedovoljno razvijene prakse ili iz drugih društveno-istorijskih razloga, pojam *personnel security* celovito preveden na srpski jezik nije zaživeo kao takav u domaćem zakonodavstvu ni literaturi, odnosno uređeni i obrađeni su samo pojedini delovi. Poslovi bezbednosti kadrova generalno obuhvataju bezbednosnu proveru (eng. security vetting), tj. proveru prošlosti (eng. background checks) i skrining pre zaposlenja (eng. pre-employment screening), kao i davanje dozvola po nivoima za pristup poverljivim informacijama (eng. granting security clearances) i drugih privilegija pristupa informacijama i prostorijama. Takođe, ovi poslovi obično podrazumevaju mere i kontrole koje se odnose na uređenje unutrašnjeg reda i ponašanja zaposlenih, kao i sprečavanja nasilja na radnom mestu.

Bezbednosne provere i dozvole

Ne ulazeći dublje u postojeću problematiku zakonske (ne)uređenosti i procedure sprovođenja bezbednosne provere u RS, smatramo da sve organizacije imaju potrebu da prilikom angažovanja ili u toku rada izvrše bezbednosnu proveru zaposlenih, dobavljača, pružaoca usluga i ostalih lica sa kojim ostvaruju određeni oblik poslovne saradnje, a u cilju zaštite od insajderskih[6] i drugih pretnji koje mogu da nanesu štetu imovini, kupcima i korisnicima, ugledu i ukupnom poslovanju. Napominjemo da društveno-ekonomski visoko razvijene države ohrabruju, kako svoj javni, tako i privatni sektor, u pravcu sprovođenja permanentne provere zaposlenih i drugih lica, olakšavajući im posao putem pune zakonske uređenosti i izrade jasnih smernica za postupanje. Formalne instrukcije koje možemo videti na primeru smernica[7] za bezbednost zaposlenih na Novom Zelandu, predstavljaju primer najbolje prakse za očuvanje i jačanje socijalnih, ekonomskih i bezbednosnih interesa svake zemlje.

Provera prošlosti (prethodna, kao i tokom radnog angažovanja) i adekvatan skrining prilikom zaposlenja značajno utiču na povećanje lojalnosti i pouzdanosti

6 O insajderskoj pretnji više: Matić Goran, *Umanjivanje insajderske pretnje - skripta*, 2024. (https://nsa.gov.rs/extfile/sr/1485/Umanjivanje_insajderske_pretnje-skripta_.pdf), 26.4.2024.

7 *Protective Security Requirements, Guide to personnel security for your organisation*, Department of the Prime Minister and Cabinet, Wellington NZ, 2019.

kadrova, a dobar primer zakonske obaveze vršenja provere zaposlenih dat je *Zakonom o sprečavanju pranja novca i finansiranja terorizma* kojim su banke, društva za upravljanje investicionim i penzijskim fondovima, brokersko-dilerska društva i drugi zakonski obveznici, dužni da prilikom zasnivanja radnog odnosa kandidata za sva radna mesta na kome se primenjuju odredbe ovog zakona, sprovedu postupak provere u smislu da li je lice osuđivano za krivična dela kojima se pribavlja protivpravna imovinska korist ili krivična dela povezana sa terorizmom. Možemo istaći i da pravna lica, odnosno privredna društva koja obavljaju delatnost privatnog obezbeđenja, takođe, imaju određenu zakonsku „olakšicu" u smislu provere prošlosti zaposlenih, jer svi službenici obezbeđenja moraju proći bezbednosnu proveru, odnosno ne sme postojati bezbednosna smetnja za potrebe izdavanje licence fizičkom licu za vršenje poslova privatnog obezbeđenja ili za vršenje poslova redarske službe.

Pored navedenog, sve organizacije, bez obzira da li su iz javnog ili privatnog sektora, a koje u svom radu koriste tajne podatke u smislu *Zakona o tajnosti podataka*, dužne su da poseduju sertifikat, tj. Dozvolu (za pravna i fizička lica) za pristup tajnim podacima izdat od strane nadležnog organa, a koji podrazumeva bezbednosnu proveru (osnovnu, potpunu, posebnu) u cilju prikupljanja podataka o mogućim bezbednosnim rizicima i smetnjama u pogledu pouzdanosti za pristup tajnim podacima (jedan od uslova za fizičko lice je i neosuđivanost na bezuslovnu kaznu zatvora za krivično delo za koje se goni po službenoj dužnosti, odnosno za prekršaj predviđen ovim zakonom, dok je za pravno lice nepostojanje kazne merom zabrane vršenja delatnosti, odnosno neizrečenost kazne prestanka pravnog lica ili mera bezbednosti zabrane obavljanja određenih registrovanih delatnosti ili poslova).

Kao što je nejasno i neprecizno određena kontrola prilikom zasnivanja radnog odnosa predviđena *Uredbom o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima*,[8] slično je predviđeno bezbednosnim standardima koji su, za razliku od zakonskih propisa, pravno neobavezujući, ali čija je implementacija poželjna i korisna za sve organizacije. Primera radi, standardom *ISO/IEC 27002*,[9] u delu koji se odnosi na kontrole vezane za ljudskih resursa, zahtevane su radnje koje prethode zapošljavanju, kao i provera kandidata sa ciljem osiguranja da zaposleni i ugovarači razumeju svoje odgovornosti i da su pogodni za uloge koje su im predviđene. Naravno, kao i svi (inter)nacionalni standardi, i ovaj standard zahteva da sve radnje koje se odnose na bezbednosne provere budu u skladu sa od-

8 „Službeni glasnik RS", br. 53/2011.

9 *ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security controls.*

govarajućim nacionalnim zakonima, propisima i etičkim pravilima, srazmerno poslovnim zahtevima i sagledanim rizicima.

Dobar primer opsega podataka i informacija koje je potrebno da se prikupljaju i proveravaju sadržan je u britanskom standardu za skrining pojedinaca koji rade u bezbednosnom okruženju *BS 7858*,[10] gde je pored osnovnih ličnih podataka, kvalifikacija, određenih znanja i veština, potrebno proveravati i osetljive podatke kao što su finansijski[11] (imovinsko stanje, kreditni status, docnje i dr.) i evidencije o kriminalnoj prošlosti (krivične presude, kažnjiva dela, mere bezbednosti i postupci u toku). Takođe, lepeza podataka bi trebala da obuhvata i reference, vojnu prošlost, medicinsku proveru (uključujući testiranja na alkohol i psihoaktivne supstance), karakterne provere, a iz razloga utvrđivanja tačnosti, praznina i protivurečnosti u odgovorima i podacima dobijenih od kandidata neophodno je da sektor korporativne bezbednosti, u saradnji sa ljudskim resursima kao nosiocima procesa zapošljavanja, sačini adekvatnu proceduru prijema i upitnih formulara. Za određene radne pozicije u praksi su poznati i slučajevi provere kandidata i zaposlenih putem poligrafskog testiranja, kao i provere članova domaćinstva, roditelja, prijatelja, seksualne orijentacije, sklonosti i navika.

Pošto su u pitanju kadrovi neophodno je prilikom razmatranja bezbednosti uzeti u obzir i zahteve vezane za upravljanje ljudskim resursima koji su dati nacionalnim standardom za procenu rizika *SRPS A.L2.003*, prema kome je potrebno analizirati i oceniti postojanje politika upravljanja ljudskim resursima, kriterijuma i procedura za regrutaciju, selekciju i klasifikaciju zaposlenih, planova za obuke i razvoj zaposlenih, kao i druga pitanja koja utiču na adekvatnost i podobnost ljudskog potencijala.

S obzirom da su provere vezane za radni odnos, kao i da se odnose na osetljive podatke, tj. podatke o ličnosti neophodno ih je sprovoditi u skladu sa zakonom, pre svih *Zakonom o radu* i *Zakonom o zaštiti podataka o ličnosti*.[12] U tom smislu, pravni osnov obrade podataka o ličnosti može biti zakon ili pristanak lica o čijim podacima se radi, a različitim propisima može biti regulisana obrada podataka o ličnosti prilikom zasnivanja radnog odnosa, uključujući podatak o osuđivanosti lica i vođe-

10 *BS 7858:2019, Screening of individuals working in a secure environment: Code of practice.*

11 Najbolja praksa kompanija koje posluju u društveno-ekonomski visoko razvijenijim državama, uređena zakonskim propisima i potpomognuta adekvatnim standardima, ukazuje na značaj postojanja instituta savetnika za zaposlene koji zapadnu u ozbiljne finansijske teškoće ili oskudice, sa ciljem umanjenja pritiska i delovanja na faktore koji mogu da utiču na objektivan, savestan i pouzdan rad zaposlenih.

12 "Službeni glasnik RS", br. 87/2018.

nju krivičnog postupka, kao što je to, na primer, slučaj prilikom zasnivanja radnog odnosa u državnim organima, obrazovnim ustanovama i slično. Za ostale slučajeve Zakon o radu

> *„ne propisuje obavezu kandidata za zaposlenje da poslodavcu dostavi dokaz da li se protiv njega vodi krivični postupak, a ukoliko je za poslodavca taj podatak potreban u svrhu zasnivanja radnog odnosa, pravni osnov za ovakvu obradu bio bi pristanak"*[13].

Zbog svega navedenog, kao i zbog činjenice postojanja inicijativa za donošenje posebnog zakona o bezbednosnim proverama, smatramo da problematika provere podobnosti kadrova ostaje otvorena, a na organizacijama je da u skladu sa zakonom što adekvatnije organizuju procedure prijema i provere, imajući u vidu i odredbe o zabrani diskriminacije u oblasti rada propisane *Zakonom o zabrani diskriminacije*.[14]

U svakom slučaju, za potrebe sprovođenja bezbednosnih provera organizacije mogu koristiti usluge pravnih lica i preduzetnika za detektivsku delatnost, odnosno detektiva koji shodno *Zakonu o detektivskoj delatnosti*,[15] a na osnovu zaključenog ugovora mogu obrađivati i podatke o kandidatima za zapošljavanje – i to one podatke za čije prikupljanje je ovlašćen poslodavac, uz pisani pristanak kandidata, kao i o krivičnim delima koja se gone po privatnoj tužbi i o učiniocima ovih krivičnih dela, odnosno o povredama radnih obaveza ili radne discipline.

Na osnovu pozitivnog rezultata sprovedene provere funkcija korporativne bezbednosti izdaje bezbednosnu dozvolu koja ukazuje na nepostojanje prigovora da određeno lice sa bezbednosnog aspekta može zasnovati radni odnos, obavljati određene dužnosti, odnosno pristupiti podacima i informacijama određenog stepena i vrste tajnosti ili prostorijama i imovini organizacije.

Unutrašnji red, ponašanje zaposlenih i sprečavanje nasilja na radnom mestu

Postojanje jasnih i formalnih pravila ponašanja zaposlenih i ostalih aktera u poslovanju korporacije neophodan je faktor ostvarenja bezbednog okruženja koji pred-

13 Opširnije: *Zaštita podataka o ličnosti u oblasti radnih odnosa*, Publikacija br. 3, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Beograd, 2018.

14 „Službeni glasnik RS",br. 22/2009 i 52/2021.

15 „Službeni glasnik RS", br. 104/2013 i 87/2018.

stavlja preduslov uspešnog poslovanja. U tom smislu, možemo navesti da državna regulativa nije jedini normativni fenomen, već korporacija ima prava i dužnosti da stvara interno obavezujuće pravne propise kojima uređuje brojna pitanja. Svi interni pravni akti, koji pripadaju domenu tzv. nedržavnog ili autonomnog prava, predstavljaju efikasno sredstvo u oblasti upravljanja rizikom koji se odnose na unutrašnji red i ponašanje zaposlenih, a koji nisu regulisani državnim pravnim aktima, odnosno u funkciji su primene zakonske norme, prilagođavajući ih specifičnim potrebama sopstvene organizacije.

Na ovo je ukazano i važećim standardom *SRPS A.L2.003* koji u okviru zahteva za procenu pravnih rizika navodi da organizacija mora da utvrdi da li postoji mogućnost nastupanja negativnih posledica na osnovu postojanja, potpunosti i adekvatnosti ravnopravnih i organizacionih mehanizama zaštite bezbednosti poslovanja od zaposlenih i/ili trećih lica, odnosno postojanja, potpunosti i adekvatnosti interne regulative kojom se predviđa nadležnost u oblasti nadzora i kontrole poštovanja internih procedura od strane zaposlenih i odgovornih lica. Takođe, ovaj standard posebno navodi potrebu postojanja, potpunosti i adekvatnosti interne regulative kojom se konstituiše adekvatan sistem unutrašnje kontrole nad radom zaposlenih i angažovanih lica/organizacija zaduženih za fizičku i tehničku zaštitu lica, imovine i kontinuiteta poslovanja.

Pored navedenog, neophodno je da korporacija poseduje formalne procedure disciplinskog postupka kako bi mogle da se preduzimaju mere protiv zaposlenih koji su postupili (ili propustili da učine dužnu radnju) suprotno propisanim i jasno predočenim pravilima. Na postojanje disciplinskih mera direktno ukazuju i bezbednosni standardi, pa tako oni iz serije *ISO/IEC 27000* koji se odnose na upravljanje sistemom bezbednosti informacija navode da je disciplinski postupak jedna od kontrola koja se odnosi na zaposlene tokom radnog angažovanja, odnosno da u okviru segmenta bezbednosti ljudskih resursa mora da postoji zvanični disciplinski postupak sa kojim su zaposleni upoznati, a da bi se mogle preduzimati mere protiv onih zaposlenih koji su narušili bezbednosna pravila. Zato pravila moraju biti normativno određena i jasno predočena svim zaposlenima putem unutrašnjih pravnih akata, a korporacija kao poslodavac može shodno Zakonu o radu da otkaže ugovor o radu zaposlenom koji ne poštuje radnu disciplinu propisanu aktom poslodavca, odnosno ako je njegovo ponašanje takvo da ne može da nastavi rad.

Poštovanje pravila unutrašnjeg reda (kojima se uređuje ulazak zaposlenih i drugih lica u objekte korporacije, korišćenje prostorija, vozila i imovine, odevanje

zaposlenih itd.) i ponašanja (obavljanje aktivnosti van radnog vremena, interpersonalni odnosi, postupanje sa klasifikovanim informacijama i imovinom, primanje poklona i drugih pogodnosti itd.) moraju se odnositi na sve zaposlene, a posebno moraju biti poštovana od strane članova odbora, odnosno top menadžmenta koji su dužni da postupaju na način kojim se ne nanosi šteta ugledu korporacije i poverenju korisnika i javnosti u njen rad, već da ispunjavaju visoke poslovne, bezbednosne i moralne standarde u postupanju pri obavljanju poslova. Primera radi, kao što je *Pravilnikom o poklonima javnih funkcionera*[16] uređen način prijema poklona u organu javne vlasti, bitno je i da pravna lica koja to nisu, na adekvatan način urede proceduru prijema i evidencije poklona različite vrednosti i namene, kao jednu od mera za sprečavanje interne korupcije.

U tom smislu, funkcija korporativne bezbednosti mora da značajno doprinese promociji bezbednog i etičkog okruženja putem kontrole pravila i zaštite zaposlenih i korporacije od neetičkog ponašanja, čime će ujedno da obezbedi i poverenje javnosti da organizacija vrši svoju delatnost na društveno odgovoran način, bez postojanja sukoba interesa. Od velikog je značaja da organizacije koje pripadaju organima javne vlasti urede pravila o sprečavanju sukoba interesa, koji u skladu sa *Zakonom o sprečavanju korupcije*[17] predstavlja situaciju u kojoj

> *„javni funkcioner ima privatni interes koji utiče, može da utiče ili izgleda kao da utiče na obavljanje javne funkcije*".

Isto se odnosi i na državne službenike koji su shodno *Zakonu o državnim službenicima*[18] dužni da preduzmu sve što je u njihovoj mogućnosti kako bi izbegli bilo kakvu situaciju sukoba interesa. S druge strane, iako nisu obavezujući, principi i preporuke sadržani u *Kodeksu korporativnog upravljanja*,[19] donetog od strane Skupštine Privredne komore Srbije kao najbolja praksa korporativnog upravljanja u društvima kapitala, ukazuju na potrebu internog definisanja pravila i procedure za rešavanje eventualnih sukoba interesa između članova i privrednog društva. Takođe, određena privredna društva imaju zakonsku obavezu uređenja i pridržavanja mera sprečavanja sukoba interesa, kao što je slučaj sa bankama čiji su članovi upravnog i

16 „Službeni glasnik RS", broj 118/2020.

17 „Službeni glasnik RS", br. 35/2019, 88/2019, 11/2021 - Autentično tumačenje, 94/2021 i 14/2022.

18 „Službeni glasnik RS", br. 79/2005, 81/2005 - ispravka, 83/2005 - ispravka, 64/2007, 67/2007 - ispravka, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018 i 157/2020.

19 „Službeni glasnik RS", broj 99/2012.

izvršnog odbora dužni da u skladu sa *Zakonom o bankama*[20] dostavljaju podatke o imovinskim pravima čija tržišna vrednost prelazi određenu vrednost, odnosno ukoliko učestvuju u organima upravljanja ili rukovođenja pravnog lica s kojim je banka uspostavila ili planira da uspostavi određeni poslovni odnos, uključujući i podatke o članovima njihovih porodica.

Na ukupnu radnu atmosferu i unutrašnji red u značajnoj meri utiče i način na koji je uređeno sprečavanje nasilja na radu, uključujući i pojave zlostavljanja na radu i u vezi sa radom i zaposlenima shodno *Zakonu o sprečavanju zlostavljanja na radu*.[21] Navedeni zakon nameće poslodavcu i obavezu obezbeđenja uslova rada u kojima zaposleni neće biti izloženi zlostavljanju od strane poslodavca, odnosno odgovornog lica ili zaposlenih kod poslodavca. Odredbe ovog propisa odnose se i na slučajeve seksualnog uznemiravanja, a pravila ponašanja poslodavaca i zaposlenih u vezi sa prevencijom i zaštitom od zlostavljanja, odnosno od seksualnog uznemiravanja uređena su i *Pravilnikom o pravilima ponašanja poslodavaca i zaposlenih u vezi sa prevencijom i zaštitom od zlostavljanja na radu*[22].

Kako se pod nasiljem na radu[23] podrazumeva i nasilje prema drugim licima koja dolaze u kontakt sa korporacijom, potrebno je da organizacija sistemski radi na prepoznavanju i prevenciji svakog nasilja, a kako bi se na adekvatan način sprovelo sprečavanje nasilja neophodno je da se zadovolji niz preduslova, kao što je razvijanje i sprovođenje plana i programa prevencije, postojanje i razvijanje adekvatnih kanala komunikacije i drugo[24].

Bezbednost informacija

Značajna vrednost bilo koje organizacije leži u njenim informacijama zbog čega je njihova bezbednost od ključnog značaja za poslovanje i razvoj, kao i za zadržava-

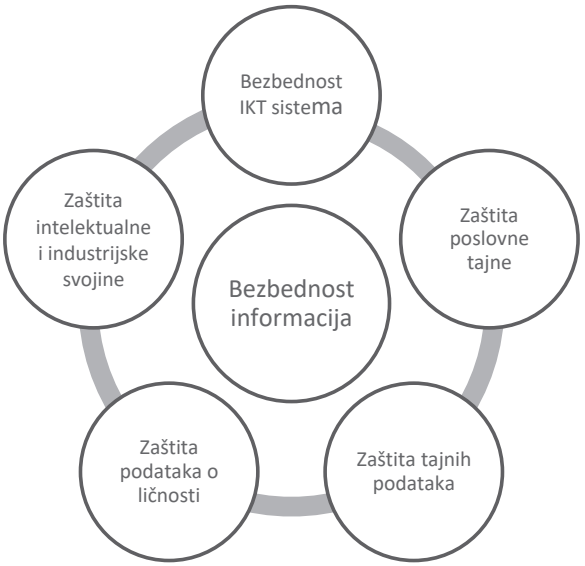
20 „Službeni glasnik RS“, br. 107/2005, 91/2010 i 14/2015.

21 „Službeni glasnik RS“, br. 36/2010.

22 „Službeni glasnik RS“, br. 62/2010.

23 Iako ne postoji univerzalna definicija, možemo se poslužiti pojašnjenjem datim od strane Uprave za bezbednost i zdravlje na radu Ministarstva rada Sjedinjenih Američkih Država, koja pojam nasilja na radu definiše kao svaki akt ili pretnju fizičkim nasiljem, uznemiravanje, zastrašivanje ili drugo preteće ometajuće ponašanje koji se javlja na radnom mestu (http://www.osha.gov/workplace-violence, 31.03.2022.).

24 Mandić J. Goran, *Sistemi obezbeđenja i zaštite*, Fakultet civilne odbrane Univerziteta u Beogradu, Beograd, 2004., str. 223 - 233.



Slika 2.3. Bezbednost informacija

nje kredibiliteta i sticanja poverenja klijenata. „Informacije se mogu čuvati u mnogim oblicima, uključujući:

- digitalnu formu (npr. podatak pohranjen na elektronskim ili optičkim medijima),
- materijalni oblik (npr. na papiru), kao i
- drugačije informacije u vidu znanja zaposlenih.

Informacije se mogu preneti na različite načine, uključujući:

- kurirski,
- elektronski ili
- verbalno.

Bez obzira na oblik informacije, ili način na koji se prenosi, uvek je potrebna odgovarajuća zaštita.[25]“

Prema navodima publikacija[26] američkih zvaničnih institucija pojam bezbednosti informacija (eng. Information security) obuhvata zaštitu informacija i infor-

25 Pogledati poglavlje *4.2.2 Information u ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary.*

26 *An Introduction to Information Security,* NIST Special Publication 800-12, Rev. 1, Gaithersburg

macionih sistema od neovlašćenog pristupa, korišćenja, otkrivanja, prekida, modifikacije ili uništenja kako bi se obezbedila poverljivost, integritet i dostupnost. Pored toga, pojedini autori navode neophodnost očuvanja i autentičnosti, odgovornosti, neporecivosti i pouzdanosti informacija. Naročito je bitna zaštita informacija ukoliko organizacija pripada kritičnoj infrastrukturi, jer, kao što je navedeno u članu 9 *Council Directive 2008/114/EC*[27] kojom se uređuje identifikacija i zaštita kritične infrastrukture EU, neophodno je zaštititi osetljive informacije kritične infrastrukture, uključujući i one nepisane informacije koje se razmenjuju tokom sastanaka na kojima se raspravlja o osetljivim temama.

> *„U početku (pre 20-25 godina), bezbednost informacija bila je integrisana u IT funkciju, i posmatrana je isključivo kao tehnička uloga. Vremena su se menjala i danas postoji mnogo mogućih uloga u okviru poslova bezbednosti informacija."*[28]

Zbog toga i danas u praksi ima primera unutrašnje organizacije gde su zaposleni sa opisom poslova iz oblasti bezbednosti informacija angažovani u okviru IT sektora. Usled potrebe za holističkim pristupom u zaštiti informacija sve je zastupljeniji princip konvergencije bezbednosnih poslova zarad objedinjenog upravljanja bezbednosnim rizicima, kao i u svrhu usklađivanja bezbednosne odgovornosti. U okviru funkcije korporativne bezbednosti lice odgovorno za ukupnu bezbednost svih informacija je menadžer bezbednosti informacija (u teoriji i praksi poznat i pod nazivom *Chief Information Security Officer - CISO*), koji je zadužen za nezavisno, objektivno i integrisano upravljanje bezbednošću svih informacija, bilo da su pisane/štampane, usmene ili u elektronskom/digitalnom obliku, odnosno bez obzira da li su lične, poverljive, tajne ili javne prirode. Takođe, obavlja poslove ili koordiniše i vrši nadzor nad radom lica za zaštitu podataka o ličnosti (DPO), rukovaoca tajnim podacima, kao i menadžera bezbednosti IT sistema (eng. IT security manager) koji je neophodno da poseduje i adekvatna tehnička znanja.

Kao i kod ostalih poslova korporativne bezbednosti, neophodno je da se i zaštita informacija bazira na proceni rizika, odnosno da su primenjene mere i kontrole u srazmeri sa rizikom. Stalno prisutni koncept „odbrane po dubini" potrebno je da bude potpuno izražen, a kao što je, primera radi, navedeno u odluci *Council Deci-*

MD, *2017.; Minimum Security Requirements for Federal Information and Information Systems,* FIPS PUB 200, NIST, Gaithersburg MD, 2006. i dr.

27 *OJ L 345*, 23.12.2008, p. 75.

28 Gelbstein Eduardo, *Information security for non-technical managers*, 1st edition, Bookboon.com, London UK 2013., p. 39.

sion 2013/488/EU[29] kojom se uređuju bezbednosna pravila za zaštitu klasifikovanih informacija EU, za smanjenje rizika neophodno je primeniti niz organizacionih, administrativnih, tehničkih i netehničkih bezbednosnih mera, organizovanih kao više slojeva odbrane (klasifikacija, bezbednost kadrova, fizička bezbednost itd.). Te mere podrazumevaju skup strategija za upravljanje procesima, politikama, tehnikama i svim drugim merama i kontrolama potrebnih za sprečavanje, prevenciju, detekciju, otpornost i oporavak digitalnih i nedigitalnih informacija od bilo kakvog oblika ugrožavanja. Svakako da je time obuhvaćena i bezbednost podataka kao užeg pojma u odnosu na informaciju, odnosno informaciju bez značenja.

Zbog značajnog negativnog uticaja po bezbednost informacija, ističemo socijalni inženjering (eng. *social engineering*) kao vid pretnje koji se opisuje kao proces, metod, tehnika, pa i umetnost obmane, prevare, ubeđivanja, uveravanja, manipulacije. Socijalni inženjering, kao primarno netehnički metod napada zarad dobijanja određenih informacija, u osnovi koristi vezu i odnose među ljudima za postizanje cilja putem različitih metoda ubeđivanja.[30]

Takođe, socijalni inženjering možemo posmatrati i u pozitivnom smislu, kao jednu od tehnika utvrđivanja ciljane ranjivosti, što je navedeno u *Tehničkim smernicama za testiranje i procenu bezbednosti informacija*[31]. U tom slučaju se koristi za testiranje ljudskog elementa i svesti korisnika o bezbednosti, a može otkriti slabosti u ponašanju korisnika.

Kao pretnja za sve delatnosti, koja može da se izvrši kontaktom, beskontaktno ili kombinovano, socijalni inženjering je posebno zastupljen u finansijskom sektoru, u kojem je ostvareno više od polovine svih fišing napada.[32] U tom smislu je Evropska organizacija za plaćanje (*European Payments Council*) u izveštaju[33] o pretnjama i prevarama u vezi sa plaćanjem, ukazala da variraju tipovi informacija koje napadači traže, ali se teži ciljanim pojedincima, od kojih se obično pokušava dobiti akreditiv

29 *OJ L 274*, 15.10.2013, p. 1.

30 O načinima izvršenja socijalnog inženjering, procesu napada, tehnikama i uzrocima podložnosti više: Mandić J. Goran, Stanojević Petar, *Korporativna bezbednost*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2019., str. 305 - 369.

31 *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, Gaithersburg MD, 2008.

32 Prema izveštaju *Spam and phishing in Q1 2017* kompanije Kaspersky od ukupnog broja svih fišing napada 55,9% je ostvareno u finansijskom sektoru, od čega je 25,82% ostvareno nad bankama, u platnom sistemu 13,6%, a u online trgovini 10,89% (http://www.securelist.com/spam-and-phishing-in-q1-2017/78221/, 15.12.2020.).

33 *Payment threats and fraud*, EPC 214-17v1.0, European Payments Council, Brussels, 2017.

ili druge osetljive informacije ili pristup njihovim uređajima u cilju neprimetnog instaliranja zlonamernog softvera, a kojim bi se pristupilo lozinkama i bankarskim informacijama, kao i uspostavila kontrola nad uređajem. U pomenutom izveštaju se, pored ostalog, navodi da uobičajeni napadi socijalnim inženjeringom uključuju metode kao što su imejl od prijatelja (eng. email from a friend), prevara izvršnog direktora (eng. CEO fraud), prevara sa agentom za oporavak (eng.recovery agent fraud) i pokušaj fišinga (eng. phishing attempts) putem imejla ili druge poruke koju prati određeni scenario ili priča. Teorija navodi, a praksa potvrđuje da je ključna mera za umanjenje rizika od socijalnog inženjeringa i očuvanja bezbednosti informacija kontinuirano planiranje i sprovođenje edukacije zaposlenih kojom se podiže svest i bezbednosna kultura.

Izgradnja efikasnog sistema menadžmenta bezbednošću informacija potvrđena je putem primene zahteva sadržanih u istaknutim (inter)nacionalnim smernicama i standardima, kakav je i *ISO/IEC 27001*.[34] Možda i zato jer je primenljivi na sve organizacije, bez obzira na vrstu, veličinu ili delatnost, jedan je od, u praksi, najzastupljenijih međunarodnih bezbednosnih standarda koji upravo specificira zahteve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sistema upravljanja bezbednošću informacija. Pored njega predviđena je i primena standarda *ISO/IEC 27002* jer uključuje zahteve za procenu i tretman rizika bezbednosti informacija prilagođene potrebama organizacije, te služi kao vodič i referenca za određivanje i implementaciju kontrola za tretman tih rizika. Takođe, u okviru familije standarda ISO/IEC 27000 postoje sektorska specifična uputstva koja imaju dodatne kontrole za određene oblasti (npr. *ISO/IEC 27019*[35] za energetsku industriju, *ISO/IEC 27011*[36] za telekomunikacijske organizacije itd.). Na značaj izgradnje sistema upravljanja bezbednošću informacija u okviru celovitog sistema menadžmenta bezbednošću ukazuju i pojedini nacionalni standardi društveno-ekonomski razvijenih zemalja, kao što je to slučaj sa austrijskim standardom *ÖNORM S 2414-1* kojim su date smernice za ugrađivanje bezbednosti informacija u okviru sistema menadžmenta bezbednošću[37].

34 *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

35 *ISO/IEC 27019:2017, Information technology — Security techniques — Information security controls for the energy utility industry.*

36 *ISO/IEC 27011:2016, Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.*

37 ÖNORM S 2414-1:2018, Security management system - Part 1: Guidance for *embeddinginformation security in the security management system.*

Zarad jasnijeg praćenja sadržaja Priručnika, ističemo da pojmovi bezbednost informacija (eng. *Information security*) i informaciona bezbednost (eng. *IT security/ cybersecurity*) nisu sinonimi. Kao što smo ranije naveli, bezbednost informacija podrazumeva spektar mera i radnji zaštite svih informacija i podataka, bez obzira u kom se obliku nalaze, dok informaciona bezbednost

> *„predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica"*[38].

Akcenat daljeg izlaganja odnosi se na zaštitu osetljivih i poverljivih podataka i informacija koje produkuje, obrađuje i čuva većina organizacija, bez obzira da li je iz javnog, privatnog ili neprofitnog sektora, uključujući i bezbednosni aspekt korišćenja takvih podataka i informacija putem IKT sistema, odnosno sajber prostora.

Bezbednost IKT sistema (cybersecurity)

Kao što smo u prethodnom izlaganju naveli da je potrebno razlikovati značenje pojmova bezbednost informacija i informaciona bezbednost, tako postoji i distinkcija među terminima zastupljenim u engleskom govornom područja kao što su *IT security, ICT security, computer security, cybersecurity*, a koji generalno potpadaju pod domaći pojam informacione bezbednosti. Uvažavajući činjenicu sve češće i veće upotrebe pojma *sajber bezbednost* (eng. cybersecurity) kako na domaćem, a posebno na međunarodnom planu, ovaj pojam ćemo koristiti nadalje za objedinjeno označavanje skupa mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni. Ovome u prilog dodajemo činjenicu da je EU uvrstila ovaj termin u naziv svoje krovne organizacije posvećene postizanju zajedničkog visokog nivoa sajber bezbednosti - *The European Union Agency for Cybersecurity (ENISA)*, kao i da ga je Uredbom *Regulation (EU) 2019/881*[39] kojom se uređuje sajber bezbednost i otpornost definisala kao

> *„aktivnosti neophodne za zaštitu mreže i informacionih sistema, korisnika takvih sistema i drugih osoba pogođenih sajber pretnjama".*

38 Član 2. stav 1. tačka 3) Zakona o informacionoj bezbednosti.

39 OJ L 151, 7.6.2019, p. 15.

Uticaj pomenutih sajber pretnji (eng. cyberthreats) dobija na sve većem značaju s obzirom da se poslovanje mnogih organizacija sve više oslanja i zavisi od IKT sistema, a sa pomeranjem aplikacija u oblak, širenjem IoT i korisničkih uređaja, rastom mrežnog saobraćaja, vektori napada se povećavaju i otvaraju organizacije za nova ugrožavanja. Funkcija korporativne bezbednosti mora da izgradi i upravlja različitim programima zaštite od sajber pretnji, koje prema prethodno pomenutoj uredbi EU predstavljaju

> *„svaku potencijalnu okolnost, događaj ili radnju koja može oštetiti, poremetiti ili na drugi način negativno uticati na mrežu i informacione sisteme, korisnike takvih sistema i druge osobe".*

Neophodno je da mere zaštite sprovode kako organizacije iz javnog, odnosno državnog aparata, tako i iz privatnog sektora, jer kako je navedeno u *Strategiji razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine*,[40] rizici informacione bezbednosti postoje kako na strani države odnosno IKT sistema od posebnog značaja, tako i na strani privrede koji su prvi na udaru visokotehnološkog kriminala. Kada je u pitanju informaciona bezbednost privrede, potrebno je naglasiti da u ovoj grupi postoje oni koji su tzv. IKT sistemi od posebnog značaja i koji u skladu sa *Zakonom o informacionoj bezbednosti*[41] imaju obavezu primene mera zaštite kako bi informacionu bezbednost svojih sistema održali na adekvatnom nivou i smanjili rizik od incidenata, ali i oni koji nisu obveznici tog zakona, te je samim tim pitanje informacione bezbednosti za njih pitanje njihovog znanja o značaju i važnosti informacione bezbednosti, posebno u smislu posledica koje mogu usled toga nastati. Na ranjivost privrednog sektora ukazuju i podaci iz istraživanja koje je sproveo Republički zavod za statistiku, prema kojima se uočava da samo oko 20% ispitanika primenjuje IKT bezbednosne mere procene rizika i sprovođenja penetracionih i drugih testova, a samo 26,7% poseduje dokumenta o merama, praksama ili postupcima u vezi sa bezbednošću IKT[42].

Za postizanje sajber bezbednosti i otpornosti neophodna je primena holističkog pristupa pod kojim se podrazumevaju dubinske zaštitne mere i kontrole koje se odnose kako na ljude, tako i na procese i na tehnologije. Čovek je i kod uspostavljanja

40 "Službeni glasnik RS", br. 86/2021.

41 "Službeni glasnik RS", br. 6/2016, 94/2017 i 77/2019.

42 Istraživanje je obuhvatilo ukupno 1597 malih, srednjih i velikih preduzeća iz svih regiona Republike Srbije. Videti više: *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji*, Republički zavod za statistiku, Beograd, 2019.

i održavanja sajber bezbednosti uvek „najslabija karika u lancu", što potvrđuju i navodi iz preambule ranije pomenute Uredbe EU kojom se uređuje sajber bezbednost i otpornost, da

> *„sajber bezbednost nije samo pitanje vezano za tehnologiju, već je i ljudsko ponašanje jednako važno. Zbog toga bi trebalo snažno promovisati „sajber-higijenu", naime, jednostavne, rutinske mere koje, tamo gde ih građani, organizacije i preduzeća sprovode redovno, umanjuju izloženost rizicima od sajber pretnji".*[43]

Iako se trendovi menjaju, možemo reći da je sektor usluga finansija i osiguranja jedan od najčešće napadanih grana industrije, što potvrđuju i podaci iz izveštaja kompanije IBM[44] o sajber pretnjama za 2020. godinu, koji ukazuju da je ovaj sektor unazad pet godina bio izložen najvećem broju sajber napada i sa učešćem od 23%u poslednjoj godini (najmanji broj napada je ostvaren na sektore transporta i edukacije). Zato za primer mogućeg način izgradnje sistema sajber bezbednosti i otpornosti korporacije možemo uzeti smernice[45] koje su publikovane od strane međunarodno relevantnih organizacija u oblasti monetarne i finansijske stabilnosti, odnosno za uređenje finansijskog tržišta - *The Bank for International Settlements (BIS)* i *The International Organization of Securities Commissions (IOSCO)*, a čije principe naravno mogu koristiti i druge organizacije bez obzira na vrstu, veličinu ili delatnost. Uostalom, kao što navode mnogobrojna uputstva iz oblasti sajber bezbednosti, i prethodno pomenute smernice ističu da je prilikom dizajniranja okvira za uspostavljanje sajber otpornosti neophodno implementirati pet primarnih kategorija upravljanja rizikom:

- rukovođenje (eng. *governance*) – jasno definisanje uloga i odgovornosti uz realnu podršku top menadžmenta na stvaranju kulture koja prepoznaje da zaposleni na svim nivoima imaju važne odgovornosti u izgradnji, održavanju i razvoju sajber bezbednosti i otpornosti;
- identifikacija (eng. *identification*) - identifikacija i klasifikacija poslovnih procesa i informacionih sredstva, kao i spoljnih zavisnosti;

43 http://www.ibm.com/reports/threat-intelligence

44 "X-Force Threat Intelligence Index", IBM Corporation, 2021. (http://www.ibm.com/reports/threat-intelligence, 23.04.2024).

45 *Guidance on cyber resilience for financial market infrastructures*, BIS and IOSCO, Basel CH, 2016.

- zaštita (eng. *protection*) - primena adekvatnih mera u cilju eliminacije, odnosno smanjenja verovatnoće ostvarenja pretnji;
- detekcija (eng. *detection*) - što ranije otkrivanje bezbednosnih događaja i incidenata, imajući u vidu prikrivenu i sofisticiranu prirodu sajber napada i postojanje višestrukih ulaznih tačaka kroz koje može doći do kompromitacije;
- odgovor i oporavak (eng. *response and recovery*) - upravljanje incidentima i planiranje kontinuiteta poslovanja sa kriznom komunikacijom, čime se omogućuje što brži, sigurniji i neometani povratak u rad kritičnih procesa i operacija.

Pored navedenih kategorija, za dizajniranje sistema sajber otpornosti, pomenutim smernicama je predviđena neophodnost postojanja i tri sveobuhvatne komponente:

- testiranje – svih elemenata i procesa sajber bezbednosti i otpornosti kako pre implementacije, tako i tokom primene, a u cilju iznalaženja „rupa" u radu i analize o načinima prevazilaženja slabosti; podrazumeva primenu različitih metoda i tehnika uključujući procenu ranjivosti, testiranje zasnovano na scenariju, penetraciono testiranje i testove koji koriste „crvene timove";
- postojanje svesti – na način realnog poznavanja spektra internih i eksternih pretnji i izazova u cilju adekvatnog postupanja sa rizicima i predupređivanja štetnih događaja, kao i omogućavanja brzog i efikasnog odgovora; ključni element u ostvarivanju visokog nivoa svesti je razmena informacija i saradnja unutar organizacije, odnosno sa pouzdanim zainteresovanim stranama unutar i izvan delatnosti;
- učenje i razvoj – brza evolucija sajber pretnji i učenje iz bezbednosnih događaja i incidenata uslovljava permanentno učenje i sticanje novih znanja i veština kako bi mogli uspešno da predviđamo i implementiramo proaktivne mere zaštite; razvoj je uslovljen sprovođenjem redovnih analiza na bazi izgrađenih metrika i modela za utvrđivanje zrelosti, kao i korelacijom nalaza revizija, pregleda od strane najvišeg rukovodstva, analizom bezbednosnih događaja i incidenata, kao i rezultatima sa testova i vežbi.

Primer izgradnje programa sajber bezbednosti i otpornosti za mala i srednja preduzeća dat je i u publikaciji *SRB-CERT Prevencija i zaštita malih i srednjih preduzeća od sajber napada, 2019*[46] .Nezavisno da li organizacija pripada javnom ili

46 http://www.cert.rs/publikacije.html?kategorija=sve-publikacije&page=3,12.01.2023.

privatnom sektoru neophodno je da unapređuje i jača sajber bezbednost i otpornost na napade, a EU u tom smislu podstiče sve organizacije naprimenu najbolje prakse putem usvajanja skupa preporuka koje su *ENISA* i *CERT-EU* publikovali u dokumentu *Povećanje sajber otpornosti vaše organizacije*[47], ukazujući na neophodnost prilagođavanja sopstvenim specifičnim poslovnim potrebama. Bez obzira na veličinu i vrstu pravnog lica, podršku za izgradnju adekvatnog okvira sajber bezbednosti, odnosno koncepta za organizovanje i komuniciranje aktivnostima koji se odnose na sajber bezbednost, možemo potražiti u smernicama za razvoj takvog okvira *ISO/IEC TS 27110*[48].

Za pomoć organizacijama u izgradnji celovitog sistema bezbednosti IKT, naročito ukoliko pripadaju operatorima IKT sistema od posebnog značaja, *Regulatorno telo za elektronske komunikacije i poštanske usluge (RATEL)* je izdalo publikaciju[49] u kojoj je predstavilo model Akta o bezbednosti IKT sistema, kao primer na koji način se mogu obuhvatiti sve mere zaštite predviđene Zakonom o informacionoj bezbednosti, *Uredbom o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja* i *Uredbom o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja*.[50] Prikazani model je potrebno prilagoditi shodno specifičnostima operatora IKT sistema, a ukoliko neke mere zaštite nisu primenjive za određenu organizaciju, potrebno je u istom aktu obrazložiti izuzimanje ili smanjenje obima primene svake mere pojedinačno. Bitno je istaći da navedeni akt predstavlja dokument koji je podložan promenama, te je njegove odredbe potrebno redovno preispitivati i izlagati proverama, a sve u cilju stvaranja što naprednijeg nivoa bezbednosti i izgradnji svesti svih zaposlenih o značaju bezbednosti IKT sistema.

I pored primene svih mera i kontrola baziranih na rezultatima adekvatne procene rizika, ne može da se isključi mogućnost nastanak incidenata, zbog čega je upravljanje incidentima značajan aspekt okvira sajber bezbednosti. Potrebno je naglasiti da su organizacije koje obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja (možemo reći da su to

47 *Boosting your Organisation's Cyber Resilience, Joint Publication*, CERT-EU and ENISA, Brussels, 2022.

48 *ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines.*

49 http://www.ratel.rs/uploads/documents/empire_plugin/Model%20Akta%20o%20bezbednosti%20lat.pdf, 18.10.2023.

50 "Službeni glasnik RS", br. 94/2016.

organizacije čiji sistemi, mreže, objekti ili njihovi delovi pripadaju kritičnoj infrastrukturi) u obavezi da dostavljaju Nacionalnom CERT-u obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema (uz izuzetak finansijskih institucija i organizacija koja vode registre podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama, koji obaveštenja dostavljaju Narodnoj banci Srbije, odnosno regulatornom telu za elektronske komunikacije ukoliko je organizacija iz oblasti elektronske komunikacije).

Uz stalni razvoj sajber pretnji, postojanja mega napada (koji prema pojedinim autorima pripadaju petoj generacija sajber bezbednosti), napada „nultog dana" i drugih naprednih trajnih pretnji neophodno je razvijati i održavati programe prevencije i odbrane u realnom vremenu na svim nivoima (perimetru mreže, oblaku, data centru, krajnjim tačkama - radne stanice i mobilni uređaji), uz kombinaciju mnogobrojnih savremenih tehnika implementiranih u uređajima i alatima za zaštitu i tehnologija konsolidovanog menadžmenta uz pomoć koje će se upravljati ovim tehnikama i deljenom obaveštavanju o pretnjama. Uz savet da bezbednost IKT sistema treba da bude jednostavna (laka za upravljanje, a teška za ugrožavanje), potrebno je i da način organizacije bezbednosti i procesi budu u skladu sa poslovnim ciljevima organizacije, omogućavajući jedinstven, integrisan bezbednosni okvir bez izuzetaka, uz izgradnju internog normativnog okvira, vršenje redovne procene rizika i ranjivosti, mapiranja rizika prevare, sprovođenje kampanje podizanja svesti, obuke i relevantne sertifikacije zaposlenih.

U cilju uspostavljanja adekvatnog sistema zaštite IKT sistema, takođe je bitno dati prioritet razumevanju principa razgraničavanja dužnosti zaposlenih koji sa jedne strane instaliraju, konfigurišu i održavaju bezbednosnu IT infrastrukturu, i sa druge strane dužnosti zaposlenih koji tu infrastrukturu nadgledaju i testiraju na bezbednosne rizike. Pored toga, a iz razloga što se određene aktivnosti sajber zaštite ne nalaze uvek i u potpunosti u okviru organizacije, odnosno što se u današnje vreme dosta operacija informacionih tehnologija ugovara sa trećim licima, potrebno je pažnju usmeriti i na odgovornosti i bezbednost svih outsourcing operacija, uključujući i skladištenje procesa/podataka u "oblaku". U tom smislu, neophodno je utvrditi da je servis provajder u stanju da zadovolji važeće bezbednosne politike kako bi bila ostvarena poverljivost, planiranje nepredviđenih situacija i druge okolnosti u vezi sa bezbednosnim nadzorom ugovornog aranžmana.

Zbog značaja vršenja procene ranjivosti ističemo važnost izgradnje programa penetracionog testiranja (eng. *penetration testing* (ili kraće *pen test*)), a kao pomoć u

uspostavljanju i upravljanju tim programom za potrebe ovog Priručnika izdvajamo vodič[51] izdat od strane reprezentativnog međunarodnog neprofitnog članskog tela koje predstavlja globalnu industriju sajber bezbednosti - *CREST*. Dizajniran je sa ciljem da pomogne organizacijama u preduzimanju efektivnog testiranja penetracije u celom preduzeću, ukazujući na elemente pripreme, faze sprovođenja i druge prateće aktivnosti, bez obzira da li organizacije nabavljaju usluge pen testa od eksternih dobavljača ili same sprovode testiranje. Potrebno je uspostaviti takvu praksu da uslov za spoljnjeg pružaoca usluga bude da zapošljava profesionalne, etičke i visoko tehnički kompetentne i pouzdane osobe, što dokazuje sertifikatom/akreditacijom od strane zvanične nadležne institucije. Kako je navedeno u vodiču, penetraciono testiranje sa svojim ograničenjima i izazovima ne predstavlja „lek za sve bolesti", ali uz preduzimanje uravnoteženog pristupa tehničkog i netehničkog testiranja može da ukaže na ranjivosti i obezbedi opšti integritet bezbednosnih kontrola. Kvalitet testiranja primarno zavisi od količine relevantnih informacija koje dobijaju osobe koje će da vrše testiranje, kao i od količine vremena i resursa koje mogu da utroše tokom testiranja.

Celoviti sistem upravljanja sajber bezbednošću podrazumeva i procenu dostignutog nivoa zrelosti sopstvene sajber bezbednosti, odnosno bitno je da organizacija dokumentuje da li primenjene mere, kontrole, ponašanje i procesi mogu da dosledno proizvedu željene rezultate. Kao primer za procenu zrelosti navodimo alate date u smernicama[52] američke federalne organizacije, koje u zavisnosti od postignutog i održavanog stanja sajber bezbednosti, ukazuju na postojanje pet nivoa zrelosti organizacije, i to:

- osnovni,
- evoluirajući,
- srednji,
- napredni i
- inovativni.

Efikasnost primene zahteva relevatnih bezbednosnih standarda u izgradnji i održavanju programa sajber bezbednosti iskazana je i u *Okviru za unapređenje*

51 *A guide for running an effective Penetration Testing programme*, CREST, Coventry UK, April 2017.

52 *Cybersecurity Assessment Tool*, FFIEC, Washington DC, 2017.

"sajber bezbednosti kritične infrastrukture[53], koji navodi sledeće referentne standarde: COBIT 5[54], ISO/IEC 27001, NIST SP 800-53[55], CIS CSC[56] i ISA 62443[57]. Pomoć organizacijama u određivanju prihvatljive i bezbedne upotrebe informacionih tehnologija mogu dati i principi predviđeni internacionalnim standardima ISO/IEC 38500[58], ISO/IEC 27032[59] i drugi iz serije ISO/IEC 27000.

Saglasili bi se sa stavom da

> *„formulisanje bezbednosne politike u oblasti zaštite IKT sistema ne treba posmatrati kao izolovan proces, nezavisan od ostalih segmenata bezbednosne zaštite korporacije. Holistički pristup organizacionoj bezbednosti korporacije podrazumeva višedimenzionalno sagledavanje heterogenih, ali međuzavisnih rizika, gde zaštita IKT sistema predstavlja integralni deo jedinstvenog i dinamičnog sistema bezbednosnog menadžmenta. U vezi s tim, formulisanje smernica za izradu bezbednosne politike treba da počne od indentifikacije opasnosti i procene rizika, jer se svaka razumna i delotvorna strategija zaštite zasniva na njima."*[60]

U praksi se često nailazi na nedostatak svesti i razumevanja scenarija sajber pretnji, a kako je potrebno određeno vreme za izgradnju sposobnosti, kompetencije i iskustava, naglašavamo neophodnost permanentnog rada na izgradnji i jačanju svesti i kulture sajber bezbednosti, ne samo zaposlenih kojima je u delokrugu sajber i ukupna bezbednost informacija, već bez izuzetka i svih ostalih zaposlenih u organizaciji. Zato ponavljamo i apostrofiramo tezu da se i prilikom izgradnje sajber bezbednosti ne sme zanemariti holistički princip koji uključuje upravljanje rizicima

53 *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg MD, 2018.

54 *A Business Framework for the Governance and Management of Enterprise IT*, ISACA, Schaumburg IL, 2012.

55 *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, NIST Special Publication 800-53, NIST, Gaithersburg MD, 2020.

56 *Critical Security Controls*, Version 8, Center for Internet Security, East Greenbush NY, 2016.

57 *ISA-62443-2-1-2009, Security for industrial automation and control systems, Part 2-1: Establishing an industrial automation and control systems security program i ANSI/ISA-62443-3-3-2013, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels.*

58 *ISO/IEC 38500:2015, Information technology — Governance of IT for the organization.*

59 *ISO/IEC 27032:2023, Cybersecurity — Guidelines for Internet security.*

60 Putnik Nenad, „Sistem korporativne bezbednosti: informacioni aspekti", u: Keković Zoran, Domitrijević R. Ivan, Šekarić Nevena, *Korporativna bezbednost – hrestomatija*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2018., str. 72.

koji se odnose kako na ljude i procese, tako i na tehnologiju. Takođe, neophodno je imati na umu i voditi računa o međusobnoj povezanosti fizičkog i digitalnog sveta, odnosno da se bezbednosna pitanja, kao što je i navedeno u zaključku Strategije bezbednosti EU[61], sada moraju posmatrati iz mnogo šire perspektive nego u prošlosti, kao i da je potrebno prevazići lažne razlike između fizičkog i digitalnog.[62]

Zaštita poslovne tajne

Uzimajući u obzir značaj poverljivih informacija u savremenom poslovanju (kao što je receptura, formula, rezultat istraživanja ili studije, cena koje će se ponuditi na tenderu, poslovni plan, proizvodni postupak, skica, crtež, projekat i dr.), nesporno je da kompromitacija takvih osetljivih poslovnih podataka i informacija može bitno da ugrozi ostvarivanje ciljeva korporacije. Kao i prilikom zaštite drugih vrednosti, a posebno u okviru mera bezbednosti celokupnih poslovnih podataka i informacija, zaštita poslovne tajne zahteva kompleksan, dubinski, slojevit i integrisan tretman raznorodnim merama i kontrolama.

Zakon o zaštiti poslovne tajne definiše poslovnu tajnu na način koji jasno ukazuje da ako držalac poslovne tajne, kao fizičko ili pravno lice pod čijom je zakonitom kontrolom, ne preduzme odgovarajuće normativne i druge razumne mere za očuvanje tajnosti informacija od neovlašćenog pribavljanja, otkrivanja i saopštavanja, data informacija neće uživati sudsku zaštitu. Takođe, potrebno je imati u vidu da se krivičnopravna zaštita poslovne tajne ogleda i u tome što njeno otkrivanje, pod određenim uslovima, predstavlja krivično delo iz člana 141. KZ (Neovlašćeno otkrivanje tajne). Nadovezujući se na izlaganje o poslovnoj tajni u delu *1. Ugrožavanje bezbednosti i otpornosti korporacije - Odavanje poslovne tajne („industrijska špijunaža") i nelojalna konkurencija*, pri njenoj zaštiti ističu se mere za postupanje sa pravnim rizicima koji mogu nastati usled neodgovarajućeg postupanja pravne službe, odnosno drugih organizacionih celina ili pojedinaca zaduženih za preduzimanje pravnih mera zaštite. Kao primeri ovih rizika, osim odavanja poslovne tajne od strane zaposlenog (umišljajnog ili nehatnog), ističu se i oni koji nastaju usled propusta vezanih za zaključenje i sadržaj sporazuma o poverljivosti sa poslovnim partnerima ili pružaocima usluga. Zato bi poslovi korporativne bezbednosti, u zavisnosti od

61 *EU Security Union Strategy, COM/2020/605 final, V. Conclusions*, European Commission, Brussels, 2020.

62 Značaj i napori koje EU sprovodi u cilju primene holističkog okvira za suočavanje sa složenim sajber-fizičkim pretnjama najbolje se mogu videti u različitim programima zaštite kritične infrastrukture EU, kao što su: PRAETORIAN, 7SHIELD, INFRASTRESS i dr.

postojeće interne organizacije i sistematizacije, trebalo da budu usmereni na preduzimanje mera za iniciranje ili donošenje opštih i pojedinačnih akata (pravilnika, odluka, procedura i sl.) kojima se uređuje zaštita poslovne tajne, kontrolu unošenja adekvatnih zaštitnih ugovornih klauzula, monitoring ugovora, sporova i drugih postupaka koje korporacija vodi. Na ovo nas upućuje i standard *SRPS A.L2.003* koji u okviru zahteva za identifikaciju, analizu i ocenu pravnih rizika ukazuje procenitelju na neophodnost utvrđivanja mogućnosti nastupanja negativnih posledica na osnovu prethodno navedenih elemenata.

Klasifikacija i označavanje dokumenata oznakom „poslovna tajna" ili sličnom oznakom, ograničavanje pristupa prostorijama i datotekama u kojima se nalaze informacije koje se smatraju poslovnom tajnom, kao i mere fizičke ili elektronske zaštite pristupa i rukovanja poslovnom tajnom spadaju u red elementarnih razumnih mera za očuvanje tajnosti tih informacija.

Postojanje tamne brojke kada je u pitanju delo odavanja poslovne tajne, kao i nepostojanje razvijene sudske prakse, upućuje nas na neophodnost dosledne primene razumnih mera, ali ostaje konstanta da bez izgradnje odgovarajuće kulture poslovne zaštite, odnosno bezbednosne kulture kao sastavnog dela korporativne kulture, nema adekvatne zaštite ni jedne vrednosti korporacije, pa tako ni poslovne tajne koja organizaciji daje konkurentu prednost na tržištu. Program edukacije mora da ide u pravcu povećanja svesti zaposlenih i ukazivanja na značaj i obaveze vezane za ne otkrivanje poverljivih informacija licima koja potencijalno mogu da dođu u posed poslovne tajne. Takav program mora da bude odobren i realno podržan od strane najvišeg rukovodstva, i nikako nesme da bude posmatran kao trošak u poslovanju, jer, konačno, ukoliko poslovna tajna bude otkrivena manje će biti značajno što će vinovnik biti zakonski gonjen kada je organizacija već pretrpela štetu, koju je u pojedinim slučajevima teško ili nemoguće povratiti.

Zaštita tajnih podataka

Bez obzira da li je pripada javnom ili privatnom sektoru, svaka organizacija koja koristi tajne podatke dužna je da ih štiti u skladu sa merama koje su propisane *Zakonom o tajnosti podataka*, propisom donesenim na osnovu ovog zakona i međunarodnim sporazumom. Naravno, i fizičko lice koje koristi tajni podatak ili lice koje se upoznalo sa njegovom sadržinom dužno je da taj podatak čuva bez obzira na način na koji je za takav podatak saznalo, a obaveza čuvanja ostaje i posle prestanka

radnog odnosa, funkcije ili obavljanja dužnosti ili članstva u organu javne vlasti ili odgovarajućem telu.

Takođe, zakonom je predviđeno da tajni podatak[63] koji je neophodan za obavljanje poslova iz delokruga njegovog rada može koristiti fizičko ili pravno lice kome je izdat potreban sertifikat, odnosno bezbednosna dozvola za pristup tajnim podacima u slučaju stranog fizičkog ili pravnog lica, a na osnovu zaključenog međunarodnog sporazuma (izuzetak su jedino predsednik Narodne skupštine, predsednik Republike i predsednik Vlade koji u cilju obavljanja poslova iz njihove nadležnosti mogu pristupiti tajnim podacima i korišćenju podataka i dokumenata bilo kog stepena tajnosti bez izdavanja sertifikata). Uz određene specifičnosti ovlašćenje za pristup tajnim podacima bez bezbednosne provere imaju državni organi koje bira Narodna skupština, rukovodioci državnih organa koje bira Narodna skupština, sudije Ustavnog suda i sudije.

I pored dugogodišnjeg postojanja zakonskog okvira u praksi postoje određeni problemi u primeni, počevši od segmenta objektivne i u skladu sa zakonom primene kriterijuma za određivanje i označavanje tajnih podataka, a koji mogu bitisledećeg stepena tajnosti: „DRŽAVNA TAJNA", „STROGO POVERLJIVO", „POVERLJIVO", „INTERNO". Sudeći prema podacima iz publikacije[64] koja obrađuje pitanja nadzora nad primenom zakona i sudske prakse u predmetima u vezi sa primenom zakona od 2015. godine, ministarstvo nadležno za pravosuđe zapravo i ne sprovodi nadzor u ovoj oblasti, a sudska praksa nije zaživela s obzirom na podatke da prekršajni sudovi u periodu istraživanja nisu vodili ni jedan postupak, dok su viši sudovi vodili dva postupka, od kojih je jedan okončan na drugostepenom apelacionim sudu osuđujućom presudom, tj. uslovnom jednogodišnjom osudom.

Bez obzira na prisutnu problematiku primene zakona u praksi, organizacije koje su korisnici tajnog podatka dužne su da uspostave sistem postupaka i mera zaštite tajnih podataka, u čemu im pomoć može pružiti i *Kancelarija Saveta za nacional-*

63 Shodno Zakonu o tajnosti podataka, tajni podatak predstavlja «podatak od interesa za Republiku Srbiju koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenom u skladu sa zakonom, određen i označen određenim stepenom tajnosti». U skladu sa članom 9. Zakona tajnost podatka mogu da odrede samo ovlašćena lica, a to su: predsednik Narodne skupštine, predsednik Republike, predsednik Vlade, rukovodilac organa javne vlasti, izabrani, postavljeni ili imenovani funkcioner organa javne vlasti koji je za određivanje tajnih podataka ovlašćen zakonom, odnosno propisom donesenim na osnovu zakona, ili ga je za to pismeno ovlastio rukovodilac organa javne vlasti, te lice zaposleno u organu javne vlasti koje je za to pismeno ovlastio rukovodilac tog organa.

64 *Primena Zakona o tajnosti podataka u Republici Srbiji*, *Nadzor i sudska praksa*, Fondacija za otvoreno društvo, Beograd, jun 2021.

nu bezbednost i zaštitu tajnih podataka u čijem je delokrugu i organizovanje obuke korisnika tajnih podataka u skladu sa nacionalnim i međunarodnim standardima i propisima. Izgradnja sistema zaštite uslovljena je stepenom tajnosti, prirodom dokumenta u kome je sadržan tajni podatak i procenom pretnje, odnosno rizika od stvarne mogućnosti narušavanja bezbednosti tajnih podataka. Zarad sprečavanja nastanka štete zakonom je uređeno da mere zaštite mogu biti opšte i posebne, odnosno mere koje se odnose na ostvarivanje administrativne, informatičko-telekomunikacione, personalne i fizičke bezbednosti tajnih podataka i stranih tajnih podataka.

Dok je organ javne vlasti dužan da primenjuje opšte (određivanje stepena tajnosti, procenu pretnje za bezbednost tajnog podatka, određivanje rukovaoca tajnim podacima i dr.) i posebne mere zaštite, pravna ili fizička lica čuvaju tajne podatke koji su im dostavljeni po osnovu ugovornog odnosa shodno posebnim merama zaštite (organizacionih i tehničkih) propisanih *Uredbom o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa*[65]. Pre zaključenja poverljivog ugovora sa pravnim ili fizičkim licem potrebno je da ovlašćeno lice organa javne vlasti utvrdi ispunjenost organizacionih i tehničkih uslova za čuvanje tajnih podataka označenih stepenom tajnosti „DRŽAVNA TAJNA", „STROGO POVERLJIVO" ili „POVERLJIVO", a pravno ili fizičko lice dužno je da, pored ostalog, kao prilog ugovoru, izradi uputstvo o merama zaštite tajnih podataka.

Pored primene opštih mera zaštite tajnih podataka organizacije su dužne da zarad efikasnosti sprovode i posebne mere zaštite, pa tako one koje se odnose na fizičko-tehničku zaštitu (određivanje administrativnih ili bezbednosnih zona, primena odgovarajuće bezbednosno tehničke opreme i dr.) utvrđene su *Uredbom o posebnim merama fizičko-tehničke zaštite tajnih podataka*[66], a one koje služe za zaštitu tajnih podataka u informaciono-telekomunikacionim sistemima (tehničke i organizacione) *Uredbom o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima*[67].

U kontekstu poslova upravljanja bezbednosnim događajima i incidentima, kontinuiteta poslovanja i sprovođenja internih istraga bitno je istaći da je organizacija dužna da bez odlaganja preduzme sve potrebne mere za utvrđivanje okolnosti ukoliko je došlo do gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka, izvrši procenu prouzrokovane štete, kao i

65 "Službeni glasnik RS", br.63/2013.

66 "Službeni glasnik RS", br. 97/2011.

67 "Službeni glasnik RS", br. 53/2011.

da preduzme potrebne mere u cilju otklanjanja štete i sprečavanja ponovnog gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka.

I prilikom zaštite tajnih podataka primena standarda i tehničkih uputstava je ne samo poželjna, već i propisana podzakonskim aktima koji određuju da kase i prostor ili prostorije bezbednosne zone I stepena moraju ispunjavati odgovarajuće *SRPS/EN* tehničke standarde, prostorije u kojima se postavljaju serveri i telekomunikaciona oprema moraju zadovoljavati *SRPS*, odnosno odgovarajuće *ISO* standarde, a primenjivanje novih tehničkih i programskih sredstava u sistemu potrebno je da bude u skladu sa odgovarajućim tehničkim kontrolama standarda *SRPS ISO/IEC 27001* i *SRPS ISO/IEC 27002*.

Zaštita podataka o ličnosti

U modernom svetu i poslovanju sve je veći izazov sačuvati privatnost pojedinca, i zato je veoma bitno u kontekstu ukupne bezbednosti informacija zaštititi podatke o ličnosti, koji prema *Zakonu o zaštiti podataka o ličnosti* predstavljaju

> *„svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta".*

Naći balans između bezbednosti i privatnosti je naročito značajno prilikom obrade posebnih vrsta podataka o ličnosti među kojima su i rasno ili etničko poreklo, političko mišljenje, versko uverenje, biometrijski podatak, podatak o zdravstvenom stanju, seksualnoj orijentaciji i sl. Iz razloga senzitivnosti ovih podataka i posledica koje mogu da nastanu u slučaju njihove zloupotrebe mnoge zemlje propisuju visoke kazne za kršenje zakonskih odredbi, a jedna od najvećih na prostoru EU je ona izrečena od strane luksemburškog nadzornog tela kojom je kompanija *Amazon* kažnjena sa 746 miliona evra za obradu ličnih podataka suprotno propisima.[68]

68 https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach, 02.09.2021.

Iako *Zakon o zaštiti podataka o ličnosti* proizilazi iz *Ustava Republike Srbije*[69], možemo reći da je on donet u procesu usklađivanja sa pravom EU i da je ekvivalent tzv. *General Data Protection Regulation (GDPR)*, odnosno *Opštoj uredbi o zaštiti podataka (Regulation (EU) 2016/679)*[70] kao opšteg pravnog akta na kojem se temelji pravni sistem zaštite podataka u EU.

Po uzoru na *GDPR* zakon uvodi brojne novine, ali propisuje i obavezu rukovaocima i obrađivačima da sprovode odgovarajuće tehničke, organizacione i kadrovske mere zaštite kako bi dostigli odgovarajući nivo bezbednosti podataka o ličnosti u odnosu na rizik. U kontekstu ostvarivanja bezbednosti klasifikovanih informacija, među kojima se obavezno ubrajaju podaci o ličnosti, organizacija je dužna da sprovede naročito sledeće mere:

- pseudonimizacija i kriptozaštita podataka o ličnosti;
- obezbeđivanje trajne poverljivosti, integriteta, raspoloživosti i otpornosti sistema i usluga obrade;
- obezbeđivanje uspostavljanja ponovne raspoloživosti i pristupa podacima o ličnosti u slučaju fizičkih ili tehničkih incidenata u najkraćem roku;
- postupak redovnog testiranja, ocenjivanja i procenjivanja delotvornosti predviđenih mera bezbednosti obrade.

Sve primenjene mere zaštite podataka o ličnosti neophodno je da budu opisane i evidentirane na način propisan *Uredbom o obrascu za vođenje evidencije i načinu vođenja evidencije o obradi podataka o ličnosti*[71].

Kao što je potrebno vršiti procenu odgovarajućeg nivoa bezbednosti, posebno uzimajući u obzir rizike od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti, tako je neophodno izvršiti procenu uticaja na zaštitu podataka o ličnosti (eng. *Data Protection Impact Assessment*) i tražiti mišljenje Poverenika za radnje obrade podataka o ličnosti određene *Odlukom o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti*[72] (npr. u slučaju obrade biometrijskih podataka u cilju jedinstvene identifikacije zaposlenih od strane poslodavca). Pored

69 „Službeni glasnik RS“, br. 98/2006, 115/2021 - Amandmani I-XXIX i 16/2022.

70 OJL 119, 4.5.2016, p. 1.

71 “Službeni glasnik RS” br. 50/2009.

72 “Službeni glasnik RS”, br. 45/2019 i 112/2020.

ostalog, procena uticaja mora da sadrži i opis mera koje se nameravaju preduzeti u odnosu na postojanje rizika, uključujući mehanizme zaštite, kao i tehničke, organizacione i kadrovske mere u cilju zaštite podatka o ličnosti i obezbeđivanja dokaza o poštovanju odredbi zakona, uzimajući u obzir prava i legitimne interese lica na koje se podaci odnose i drugih lica.

Ukoliko lice za zaštitu podataka o ličnosti (eng. *Data Protection Officer*) iz razloga nezavisnosti u radu, zbog organizacionih ili drugih potreba ne pripada sektoru korporativne bezbednosti, neophodno je izgraditi dokumentovan odnos nadležnosti kako bi zaštita podataka o ličnosti zadovoljila holistički princip ostvarivanja bezbednosti. Primera radi, podizanje svesti i obuke zaposlenih koji učestvuju u radnjama obrade je jedna od zakonskih obaveza *DPO*-a, koja je neophodno da bude deo celovitog programa podizanja nivoa ukupne bezbednosne kulture zaposlenih. Neophodna integracija se uočava i potrebna je i prilikom procene rizika, u upravljanju incidentima vezanim za podatke o ličnosti (bez obzira da li su u elektronskom ili papirnom obliku), u procesu obezbeđenja kontinuiteta pristupa podacima, kao i u ostalim dubinskim merama i kontrolama koje se odnose na zaštitu podataka o ličnosti.

U integrisanoj primeni zaštitnih mera i kontrola od velike pomoći može biti primena priznatih standarda koji na sistematičan način ukazuju na način upravljanja bezbednošću, u ovom slučaju sa akcentom na zaštitu podataka o ličnosti. U tom smislu izdvajamo standarde iz serije *SRPSISO/IEC 29100*[73] (*SRPS EN ISO/IEC* 29101[74] i *SRPSISO/IEC 29151*[75]) koji daju smernice za definisanje uloga u obradi ličnih podataka, opisuju aspekte zaštite i utvrđuju ciljeve, kontrole i procedure kako bi se ispunili zahtevi identifikovani procenom rizika i uticaja u vezi sa zaštitom podataka o ličnosti. Značaj holističkom pristupu u postupanju sa rizicima po bezbednost privatnosti daju i zahtevi smernica *SRPS ISO/IEC 27701*[76] koji pružaju uputstvo za uspostavljanje, primenu, održavanje i kontinuirano poboljšanje sistema menadžmenta informacijama o privatnosti u formi proširenja *ISO/IEC 27001* i *ISO/IEC 27002* za upravljanje privatnošću u kontekstu organizacije.

73 *SRPS ISO/IEC 29100:2019, Informacione tehnologije – Tehnike bezbednosti – Okvir privatnosti.*

74 *SRPS EN ISO/IEC 29101:2021, Informacione tehnologije – Tehnike bezbednosti – Okvir arhitekture privatnosti.*

75 *SRPS EN ISO/IEC 29151:2022, Informacione tehnologije – Tehnike bezbednosti – Pravila dobre prakse za zaštitu ličnih identifikacionih informacija.*

76 *SRPS ISO/IEC 27701:2019, Tehnike bezbednosti – Proširenje ISO/IEC 27001 i ISO/IEC 27002 za menadžment informacijama o privatnosti – Zahtevi i smernice.*

Sa aspekta funkcije korporativne bezbednosti interesantna je obrada i zaštita podataka o ličnosti prilikom korišćenja sistema video obezbeđenja za potrebe ukupne zaštite lica, imovine i poslovanja korporacije, a možemo napomenuti da naša zemlja nema poseban zakon koji bi regulisao oblast video obezbeđenja, odnosno oblast obrade podataka o ličnosti putem sistema video obezbeđenja, posebno dela koji se odnosi na njegovu sofisticiranu kategoriju kojom se vrši obrada biometrijskih podataka. U tom smislu potrebno je imati u vidu i smernice donesene od strane *European Data Protection Supervisor*[77] koje se odnose na video-nadzor koji sprovode institucije ili druga strana u njihovo ime za bilo koju svrhu u kojoj kamere snimaju lične podatke, kao i preporuke Komiteta ministara država članica koje se odnose na obradu ličnih podataka u kontekstu zapošljavanja[78]. Zbog značaja, ali i osetljivosti upotrebe video obezbeđenja neophodno je prilikom projektovanja ovog sistema pridržavati se odredaba *Zakona o privatnom obezbeđenju*, ne dovodeći u pitanje i ne narušavajući profesionalni integritet zaposlenih neopravdanom, neosnovanom ili prekomernom upotrebom kamera kako je propisano *Pravilnikom o pravilima ponašanja poslodavaca i zaposlenih u vezi sa prevencijom i zaštitom od zlostavljanja na radu*[79].

Kao pomoć u poslovanju i sprečavanju nastanka štete, odnosno u cilju usklađivanja postupanja organizacije sa propisima koji uređuju zaštitu podataka o ličnosti, *Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti* je sačinio i na svojoj internet stranici (www.poverenik.rs u sekciji pod nazivom *„Zaštita podataka*“) objavio kontrolnu listu za rukovaoce, koja može da posluži organizaciji u samoproveri ispunjenosti zahteva iz kontrolne liste i samoproceni rizika.

Pored do sada navedenog, bitno je napomenuti da kao što su, primera radi, *Poverenik* ili *DPO* dužni da kao profesionalnu tajnu (eng. *professional secrecy*) čuvaju sve podatke do kojih su došli u obavljanju svojih funkcija, odnosnou izvršavanju obaveza, tako je potrebno i da lekari, advokati i druga lica, u skladu sa zakonom ili profesionalnim pravilima (tzv. granskim kodeksima[80]) čuvaju kao tajnu podatke i

77 Detaljnije: *The EDPS Video-Surveillance Guidelines*, European Data Protection Supervisor, Brussels, 17 March 2010.

78 Videti: *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States*, Council of Europe, Strasbourg FR, 1 April 2015.

79 „Službeni glasnik RS“, br. 62/2010.

80 Npr. etička načela u obavljanju profesionalnih dužnosti članova Lekarske komore Srbije utvrđena su *Kodeksom medicinske etike Lekarske komore Srbije* (“Službeni glasnik RS”, br. 104/2016), a postupanja policijskih službenika u Ministarstvu unutrašnjih poslova *Kodeksom policijske etike* (“Službeni glasnik RS”, br. 85/2023).

informacije koje su saznali u vršenju svog poziva, a njihovo neovlašćeno otkrivanje sankcionisano je i članom 141. KZ.

Zaštita intelektualne i industrijske svojine

Pojam intelektualna svojina (eng. *Intellectual Property*) se odnosi na posebna, specifična prava koja imaju autori, pronalazači i ostali nosioci prava u tom području. Intelektualna svojina ne podrazumeva konkretno, materijalno vlasništvo nad određenim predmetom, već pravo odnosno skup ovlašćenja koje pravni poredak države priznaje nosiocu prava intelektualne svojine.[81] Koja su to ovlašćenja i na koji način se ostvaruju, zavisi od vrste dela koje se štiti i pravnog sistema u kojem se zaštita traži. Zahvaljujući multilateralnim konvencijama od kojih su neke donete pre pola veka, područje intelektualne svojine jedna je od retkih grana prava koja uživa visok stepen usaglašenosti u većini nacionalnih pravnih sistema.

Osnovna svrha prava intelektualne svojine je podsticanje inovacija i kreativnosti kroz omogućavanje da pronalazači, autori i drugi kreatori intelektualnih dobara dobiju pravednu nagradu za svoj rad i da mogu da žive od rezultata svog rada, a takođe i da zaštite ulaganja u reputaciju brenda. Prava intelektualne svojine omogućavaju svojim nosiocima da spreče druge da kopiraju ili koriste njihova zaštićena prava bez dozvole. Ta prava daju mogućnost isključivog korišćenja, a njihovi nosioci mogu da ostvare i prihod kroz naknade od prodaje ili korišćenja svoje intelektualne svojine od strane drugih lica. Ovi prihodi mogu pomoći u finansiranju daljeg istraživanja i razvoja, a time i podržati rast poslovnog subjekta. Ovaj vid ekonomske sigurnosti podstiče kompanije i istraživače da ulažu u razvoj inovacija, drugih kreacija i brendiranje proizvoda i usluga, od kojih i društvo i životna sredina mogu imati koristi.

Sam izraz „Intellectual Property" prvi put se pominje u sačuvanoj presudi okružnog suda američke savezne države Masačusets iz 1845. godine. U pravnoj francuskoj teoriji i literaturi iz 1846. godine javlja se izraz *propriété intellectuelle*, koji je upotrebio Alfred Nion u svom delu *Droits civils des auteurs, artistes et inventeurs* (Građanska prava autora, umetnika i izumitelja), što ukazuje na mogućnost da je taj izraz bio u upotrebi i ranije.

U međunarodnom pravu se termin „intelektualna svojina" definiše Konvencijom o osnivanju Svetske organizacije za intelektualnu svojinu (*World Intellectual Property Organisation – WIPO*), usvojenom 14. jula 1967. godine u Stokholmu.

81 Moberly D. Michael, *Safeguarding Intangible Assets*, Butterworth-Heinemann, Oxford UK 2014, pp. 33-35.

Prema odredbama Konvencije, pojam intelektualne svojine označava prava koja se odnose na književna, umetnička i naučna dela, interpretacije umetnika interpretatora i izvođenja umetnika izvođača, fonograme i radio emisije, pronalaske u svim oblastima ljudske aktivnosti, naučna otkrića, industrijske uzorke i modele, fabričke, trgovačke i uslužne žigove, kao i trgovačka imena i trgovačke nazive, zaštitu od nelojalne utakmice i sva druga prava vezana za intelektualnu aktivnost u industrijskoj, naučnoj, književnoj i umetničkoj oblasti. Ipak, ovaj termin u svetskoj pravnoj praksi još uvek nije opšteprihvaćen. Premda je preovlađujuće pravno stanovište da je intelektualna svojina zajednički naziv za industrijsku svojinu i autorsko pravo, neretko se govori o „pravu industrijske svojine i autorskom pravu" umesto „pravu intelektualne svojine".

Pravo intelektualne svojine je relativno mlada grana prava, koja se brzo razvija u skladu sa aktuelnim tempom tehnološkog razvoja i napretka, a u cilju pravne zaštite intelektualnih dela od neovlašćenog iskorišćavanja.[82] U praksi, problem je utoliko veći što je povreda prava intelektualne svojine najčešće povezana sa organizovanim, sajber i korporacijskim kriminalitetom.

Zaštita prava intelektualne svojine nije obavezna, ali za dobrobit onoga koji je stvorio neko intelektualno dobro, poželjno je razmotriti, u skladu sa strategijom iskorišćavanja takvog dobra, konkurentnošću proizvoda/usluge, troškovima zaštite, kao i sa drugim aspektima poslovanja ili komercijalizacije, relevantnost zaštite nekim od prava intelektualne svojine.

U pogledu zaštite dela autorskog prava u inostranstvu, treba imati u vidu da je Republika Srbija potpisnica Bernske konvencije, koja predviđa obavezu za sve zemlje potpisnice da strancima pruže istu zaštitu kao i svojim državljanima. Iz tog razloga, autorsko delo domaćeg autora će uživati zaštitu u drugim državama po zakonima tih zemalja, kao što će i autorsko delo stranog autora uživati zaštitu u Srbiji po njenim unutrašnjim zakonima.

U glavi XX *Krivičnog zakonika* propisana je grupa krivičnih dela protiv intelektualne svojine, koju čine:

- povreda moralnih prava autora i interpretatora (član 198 KZ);
- neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava (član 199 KZ);

82 Goldstein Paul, Reese R. Anthony, *Copyright, Patent, Trademark and Realated State Doctrines: Cases and Materials on the Law of Intellectual Property*, Foundation Press, New York NY 2008, pp. 18-19.

- neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskim i srodnim pravima (član 200 KZ);
- povreda pronalazačkog prava (član 201 KZ) i neovlašćeno korišćenje tuđeg dizajna (član 202 KZ).

Krivičnopravna zaštita intelektualne svojine u Srbiji se ne ostvaruje samo inkriminacijama iz glave XX Krivičnog zakonika, budući da je krivičnim delom

> *„Neovlašćena upotreba tuđeg poslovnog imena i druge posebne oznake robe ili usluga"*

iz člana 238 KZ, koje nominalno spada u grupu krivičnih dela protiv privrede (glava XXII KZ), propisana zaštita prava žiga, prava geografskih oznaka porekla i prava zaštite topografija integrisanih kola.

Pravo industrijske svojine (eng. *Industrial Property*) podrazumeva pravo proizvođača da isključivo koristi svoj patentom zaštićen pronalazak, da označava sebe kao proizvođača određenih proizvoda, da u tom cilju koristi žigove za obeležavanje robe, zaštitni znak, oznake geografskog porekla proizvoda, pravo uzorka i modela, da od toga ostvaruje prihode i da uživa druga prava koja spadaju u domen industrijske svojine. Zaštita ovih prava u Republici Srbiji je uređena *Zakonom o patentima*[83], *Zakonom o oznakama geografskog porekla*[84], *Zakonom o pravnoj zaštiti industrijskog dizajna*[85] i drugim zakonima i propisima kojima se ova materija pravno reguliše.

Po svojoj prirodi, patentno pravo i pravo na zaštitu industrijskog dizajn su sastavni delovi prava industrijske svojine. Osim ova dva prava, u prava industrijske svojine spadaju još i prava žiga, prava geografskih oznaka porekla i prava zaštite topografije integrisanih kola.

Krivičnopravna zaštita prava industrijske svojine ima pre svega ekonomski značaj za nosioca ovog prava jer se njome osigurava korišćenje ovog prava i bolje plasiranje zaštićenih proizvoda na tržištu na osnovu utvrđenog kvaliteta određenog proizvoda, a time i bolji uspeh u privrednom poslovanju i ostvarivanju ekonomske dobiti.

83 „Službeni glasnik RS", br. 99/2011, 113/2017 - dr. zakon, 72/2009 - dr. zakon, 95/2018, 66/2019 i 123/2021.

84 „Službeni glasnik RS", br. 18/2010 i 44/2018 - dr. zakon.

85 „Službeni glasnik RS", br. 104/2009, 45/2015 i 44/2018 - dr. zakon.

Za zaštitu industrijske svojine je karakteristična teritorijalna ograničenost, koja se po pravilu odnosi na područje pojedine države. Drugo ograničenje u zaštiti industrijske svojine odnosi se na njeno trajanje, koje je s izuzetkom zaštite žiga (trademark, brand) vremenski ograničeno. Stoga pri izvozu proizvoda i usluga treba unapred voditi računa o strategiji međunarodne zaštite uzimajući i u obzir potencijalna tržišta, zemlje dobavljača sirovina i materijala, kao i zemlje u kojima potencijalna konkurencija može organizovati sličnu proizvodnju. Takođe, važan aspekt zaštite industrijske svojine je i pravovremenost njenog pokretanja.

Prava industrijske svojine, uključujući patent, žig i industrijski dizajn kao najčešće zastupljena, jesu teritorijalna prava i imaju dejstvo na teritorijama zemalja gde su registrovana. Ako se želi proširenje zaštite na druge zemlje, Republika Srbija je potpisnica različitih međunarodnih ugovora, tako da se zaštita može ostvariti i van Srbije nekim od mehanizama za međunarodnu registraciju ili pojedinačno u zemljama koje su podnosiocu od interesa za ostvarivanje zaštite. Pritom treba voditi računa da je za određena prava, kao što su patent i industrijski dizajn, to neophodno uraditi u određenom roku od datuma podnošenja nacionalne prijave zbog priznavanja datuma prioriteta i zadržavanja uslova novosti u tom roku.

Sa stanovišta korporativne bezbednosti, zaštita intelektualne i industrijske svojine je neophodna iz nekoliko razloga:

- Očuvanje konkurentske prednosti: krađa intelektualne svojine može dovesti do gubitka kritičnog znanja i inovacija koje kompaniji daju prednost u tržišnoj utakmici;
- Očuvanje tržišne pozicije: neovlašćeno otkrivanje ili korišćenje intelektualne svojine može dovesti do stvaranja falsifikovanih proizvoda ili usluga, te narušavanja poverenja kupaca i reputacije brenda;
- Obezbeđivanje kontinuiteta poslovanja: krađa intelektualne i industrijske svojine može da poremeti poslovne operacije, prouzrokujući finansijske gubitke i pravne bitke, i da potencijalno ugrozi opstanak organizacije.

Zaštita intelektualne i industrijske svojine uključuje različite prepreke, a menadžeri bezbednosti informacija (CISO) i stručnjaci za sajber bezbednost se suočavaju sa brojnim bezbednosnim izazovima u tom području, uključujući:

- Razvoj sajber pretnji: nosioci visokotehnološkog kriminala kontinuirano prilagođavaju svoje taktike, tehnike i procedure kako bi narušili bezbednosnu odbranu i iskoristili ranjivosti u strategijama zaštite intelektualne svojine;

- Napredne trajne pretnje (Advanced persistent threat - ART): specijalizovane grupe, često sponzorisane od strane nacionalnih država, učestvuju u dugoročnim tajnim operacijama usmerenim na krađu intelektualne svojine radi ekonomske, političke ili vojne dobiti;
- Insajderske pretnje: zaposleni ili insajderi od poverenja sa pristupom osetljivim informacijama mogu da zloupotrebe svoje privilegije ili nenamerno odaju podatke vezane za intelektualnu i industrijsku svojinu, što predstavlja značajan rizik za poslovni subjekt;
- Nedostatak svesti i obuke: nedovoljna svest o sajber bezbednosti među zaposlenima, promene u infrastrukturi tokom korporacijskih spajanja i akvizicija, kao i nevoljnost da se promene radne prakse, mogu uzrokovati nenamerno deljenje osetljivih informacija.

Posledice krađe intelektualne i industrijske svojine mogu biti dalekosežne, obuhvatajući i:

- Finansijske gubitke: ukradena intelektualna i industrijska svojina može rezultirati značajnim finansijskim gubicima zbog troškova istraga, pravnih postupaka i negativnog uticaja na tržišni udeo i prihod, kao i zbog gubitka vrednosti same ukradene imovine;
- Ugrožavanje reputacije: krađa intelektualne i industrijske svojine može narušiti ugled kompanije, umanjiti poverenje kupaca i dovesti do gubitka poslovnih prilika;
- Slabljenje konkurentnosti: neovlašćeno korišćenje ili otkrivanje intelektualne svojine može omogućiti konkurentskim kompanijama da kopiraju ili kompromituju do tada jedinstvene proizvode, usluge ili tehnologije organizacije, narušavajući njen tržišni udeo;
- Pravne i regulatorne posledice: organizacije se mogu suočiti sa tužbama, regulatornim kaznama i drugim pravnim posledicama ako ne uspeju da zaštite svoju intelektualnu i industrijsku svojinu na adekvatan način.

Da bi zaštitile intelektualnu svojinu od sajber pretnji, korporacije treba da usvoje sveobuhvatan pristup koji podrazumeva naročito sledeće strategije:

- Implementacija robusnih kontrola pristupa: neophodna je implementacija kontrole pristupa zasnovane na ulogama (Role-based access control - RBAC) kako bi se ograničio pristup osetljivim informacijama. U tom

smislu, pristup nultog poverenja pretpostavlja da nijednom korisniku ili uređaju ne treba automatski verovati, bez obzira na njihovu lokaciju unutar ili van perimetra mreže. Implementacijom tog principa, organizacije primenjuju detaljne kontrole pristupa, autentifikaciju i kontinuirano praćenje, obezbeđujući da samo ovlašćeni entiteti mogu da pristupe resursima. Ovaj pristup takođe minimizira potencijal za bočno kretanje unutar mreže, smanjuje površinu napada i smanjuje rizik od insajderskih pretnji. Nulto poverenje obezbeđuje proaktivan i prilagodljiv bezbednosni okvir koji je u skladu sa okruženjem pretnji i koji se razvija i efikasno štiti kritična sredstva. Takođe, nužni su jaki mehanizmi autentifikacije (višefaktorska autentikacija za sprečavanje neovlašćenog pristupa, šifrovanje osetljivih podataka radi zaštite od neovlašćenog presretanja).

- Ublažavanje insajderskih pretnji: sprovođenje striktnog praćenja pristupa korisnika i revizije je moderna potreba i najbolja praksa u korporativnoj bezbednosti, uključujući i provere prošlosti zaposlenih sa pristupom kritičnoj intelektualnoj svojini.
- Kontinuirano upravljanje ranjivostima: redovno sprovođenje procena ranjivosti i testiranja potencijalnih upada radi identifikovanja i adresiranja bezbednosnih slabosti daje organizacijama i taktičku prednost u zaštiti bezbednosti intelektualne svojine;
- Obrazovanje i svest zaposlenih: obezbeđivanje sveobuhvatne obuke zaposlenih o sajber bezbednosti, sa fokusom na važnost zaštite intelektualne svojine, pretnje socijalnog inženjeringa i najbolje prakse za rukovanje podacima, predstavlja proaktivni standard u korporativnoj bezbednosti. To uključuje i sprovođenje redovnih kampanja podizanja svesti radi jačanja bezbednosnih protokola i podsticanja prijavljivanja sumnjivih aktivnosti.[86]

86 Ramcharan Robin, *International Intellectual Property Law and Human Security*, Asser Press, The Hague NL 2013, pp. 259-262.

Spremnost na nepredviđeno i planiranje kontinuiteta poslovanja

Zaštita i spasavanje (elementarne nepogode ili tehničko-tehnološke nesreće)

I pored mnogih deklarativnih mera i strategija na globalnom, nacionalnom i lokalnom nivou, i u manjem obimu preduzimanih konkretnih radnji i realizovanih planova, svedoci smo mnogobrojnih vanrednih događaja i katastrofa uzrokovanih elementarnim nepogodama (zemljotresom, poplavom, bujicom, olujom, sušom, klizištem, pandemijom i dr.) ili tehničko-tehnološkim nesrećama (požarom, eksplozijom, havarijom itd.), čije posledice ugrožavaju bezbednost, život i zdravlje ljudi, materijalna i kulturna dobra ili životnu sredinu. Mnogi autori objašnjavaju takva dešavanja kroz sve veće narušavanje odnosa između prirode i ljudskog društva pojavama kao što su:

- migracije,
- rast gradskih naselja i sve veća koncentracija stanovništva oko njih,
- povećana proizvodnja otpada,
- stalni rast potreba za električnom i drugim vidovima energije,
- nekontrolisana eksploatacija prirodnih resursa (nafte, gasa i drugih energetskih i neenergetskih materijala) i drugo.

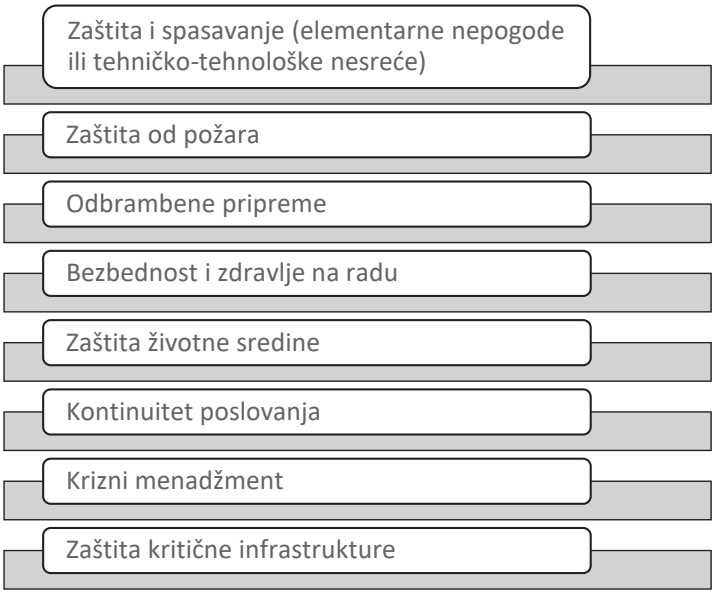
Zato je i na mikroplanu bitno da svaka organizacija u okviru svog poslovanja preduzima aktivnosti kojima umanjuje negativne uticaje na uzroke nastanka opasnosti, ali i da sprovodi mere na jačanju svoje otpornosti i zaštiti kako bi sprečila ili u što većoj meri smanjila negativne posledice.

Iako se generalno uzev RS ubraja u države malog rizika od humanitarnih kriza i katastrofa (sa stabilnim rejtingom indeksa 3,0)[87], ima kao i ostale države, primarnu odgovornost da spreči i smanji rizik od katastrofa, što je i jedan od osnovnih principa *Okvira za smanjenje rizika od katastrofa*[88] koji je donet na Trećoj svetskoj konferenciji UN održanoj u Sendaju 2015. godine. Kako je smanjenje rizika od katastrofa

87 *INFORM REPORT 2022, Shared evidence for managing crises and disasters*, United Nations Office for the Coordination of Humanitarian Affairs, New York NY, 2022.

88 *Sendai Framework for Disaster Risk Reduction 2015-2030*, The Third UN World Conference, Sendai JP, 2015.

zajednička odgovornost svih aktera, pored obaveza vladinih institucija, navedenim okvirom je istaknuta dužnost organizacija iz poslovnog, odnosno privatnog sektora da integrišu upravljanje rizikom od katastrofa (uključujući kontinuitet poslovanja) u poslovne modele i prakse kroz ulaganja zasnovana na riziku od katastrofa, permanentno se angažujući na obuci i podizanju svesti zaposlenih, kao i svojih korisnika, odnosno kupaca.



Slika 2.4. Spremnost na nepredviđeno i planiranje kontinuiteta poslovanja

Uostalom, u interesu svake organizacije je da zaštiti svoje zaposlene, imovinu i poslovanje od opasnosti, počevši od adekvatne procene rizika od katastrofa, koju su shodno zakonu dužni da izrađuju i donose ne samo Republika Srbija, autonomna pokrajina i jedinica lokalne samouprave, već i širok spektar organizacija i to:

- subjekti od posebnog značaja za zaštitu i spasavanje, izuzev saveza, klubova i udruženja;
- privredna društva, zdravstvene ustanove izuzev apoteka;
- predškolske i školske ustanove i fakulteti za sve objekte u kojima borave deca, odnosno objekte u kojima se odvija nastava;
- ustanove socijalne zaštite za objekte u kojima borave korisnici.

Takođe, procenu rizika od katastrofa izrađuju i donose i pravna lica koja upravljaju poslovnim, trgovačkim, sportskim, ugostiteljskim i smeštajnim objektima i objektima za razonodu kapaciteta više od 100 lica, a ako su objekti namenjeni za boravak dece do 14 godina, nezavisno od kapaciteta. Pored navedenog, štab za vanredne situacije jedinice lokalne samouprave može da preporuči da određena privredna društva i druga pravna lica (koja nisu direktno navedena zakonom) izrađuju svoju procenu rizika od katastrofa. U svakom slučaju, sve organizacije donose procenu rizika od katastrofa po pribavljenoj saglasnosti MUP-a, a za njenu izradu dužni su da angažuju privredna društva odnosno druga pravna lica koja imaju ovlašćenje za izradu predmetne procene rizika i imaju u stalnom radnom odnosu zaposlena lica koja poseduju licencu za izradu procene rizika od katastrofa i plana zaštite i spasavanja.

Sve organizacije koje imaju obavezu izrade procene rizika od katastrofa dužne su da izrade i donesu plan zaštite i spasavanja[89], kojim se planiraju mere i aktivnosti za sprečavanje i umanjenje posledica katastrofa, kao i radi organizovanja i koordiniranja aktivnosti u vezi sa angažovanjem i delovanjem sopstvenih snaga i sredstava u vanrednim situacijama, a s ciljem postizanja zaštite i spasavanja zaposlenih i drugih lica koja se zateknu u kompanijskim objektima, odnosno radi zaštite imovine i obezbeđenja osnovnih uslova za nastavak poslovanja u vanrednim situacijama.

Kao i na plan zaštite i spasavanja, saglasnost MUP-a je neophodna i na plan zaštite od udesa[90], koji je dužan da izradi privredno društvo i drugo pravno lice koje obavlja aktivnosti u kojima je prisutna ili može biti prisutna jedna ili više opasnih supstanci u propisanim količinama[91].

Bez obzira na navedeno, svako privredno društvo i drugo pravno lice dužno je shodno *Zakonu o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama* da u okviru svoje delatnosti preduzima sve mere prevencije i smanjenja rizika, kao i da se odazove zahtevu nadležnog štaba i uzme učešće u sprovođenju mera zaštite i spasavanja. Posebne obaveze imaju privredna društva i druga pravna lica koji predstavljaju subjekte od posebnog značaja za zaštitu i spasavanje, odnosno koja se bave delatnošću iz sledećih oblasti:

89 Metodologija izrade i sadržaj procene rizika od katastrofa i planova zaštite i spasavanja svih subjekata koji imaju obavezu izrade tih dokumenata uređena je *Uputstvom o Metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja*.

90 Način izrade i sadržaj plana zaštite od udesa propisan je *Pravilnikom o načinu izrade i sadržaju Plana zaštite od udesa* ("Službeni glasnik RS", br. 41/2019).

91 Vrsta i količina opasnih supstanci propisana je *Pravilnikom o vrsti i količini opasnih supstanci na osnovu kojih se sačinjava Plan zaštite od udesa* ("Službeni glasnik RS", br. 34/2019).

- telekomunikacija,
- rudarstva i energetike,
- transporta,
- meteorologije,
- hidrologije,
- seizmologije,
- zaštite od jonizujućeg zračenja i nuklearne sigurnosti,
- zaštite životne sredine, vodoprivrede, šumarstva i poljoprivrede, zdravstva,
- zbrinjavanja lica,
- veterine,
- komunalne delatnosti,
- građevinarstva,
- ugostiteljstva, i
- drugi koji raspolažu resursima za smanjenje rizika od katastrofa[92].

Širokoj lepezi organizacija, koja shodno zakonu imaju posebne obaveze u prevenciji i jačanju otpornosti i spremnosti zajednice za reagovanje na posledice katastrofa, pripadaju i privredna društva i druga pravna lica koja su vlasnici i korisnici elektronskih komunikacionih mreža i informacionih sistema i veza, zaliha vode, hrane, medicinskih sredstava i lekova, energenata, odeće, obuće, građevinskih i drugih proizvoda neophodnih za izvršavanje zadataka zaštite i spasavanja. Takođe, određena prava i obaveze imaju i humanitarne organizacije i udruženja, udruženja i druge organizacije civilnog društva, kao i visokoškolske ustanove i druge organizacije koje se bave naučno-istraživačkim radom, što sve zajedno ukazuje na kompleksnost sistem smanjenja rizika od katastrofa i upravljanja vanrednim situacijama, ali i ističe dužnosti mnogih organizacija iz javnog i privatnog sektora na sprovođenju preventivnih i operativnih mera i izvršavanju zadataka zaštite i spasavanja ljudi i dobara od posledica katastrofa, uključujući i mere oporavka od tih posledica.

Kada je reč o planu zaštite i spasavanja privrednih društava i drugih pravnih lica bitno je istaći da je pored uvodnog dela, *Uredbom o sadržaju, načinu izrade i*

92 Privredna društva i druga pravna lica od posebnog značaja za sprovođenje mera zaštite i spasavanja u Republici Srbiji određeni su *Odlukom o određivanju subjekata od posebnog značaja za zaštitu i spasavanje u Republici Srbiji* ("Službeni glasnik RS", br. 69/2019).

obavezama subjekata u vezi sa izradom procene rizika od katastrofa i planova zaštite i spasavanja[93] predviđeno uređenje mera civilne zaštite, sa ciljem zaštite i spasavanja zaposlenih i korisnika njihovih usluga. Uz organizovanje uzbunjivanja, evakuacije i ostalih elemenata, neophodno je i da direktor ili drugo ovlašćeno lice imenuje poverenike i zamenike poverenika civilne zaštite, čiji su zadaci propisani *Pravilnikom o radu poverenika i zamenika poverenika civilne zaštite i kriterijumima za njihovo imenovanje*[94].

Kao što funkcija korporativne bezbednosti ima obavezu da putem poslova zaštite i spasavanja koordinira radom poverenika civilne zaštite, tako je potrebno da kroz celu kompaniju uskladi i nadzoriše primenu kompleksnih mera i kontrola za smanjenje rizika i jačanje veština i kapaciteta za delovanje u vanrednim situacijama. Pored uspostavljanja dobre unutrašnje organizacije i opremljenosti, jedna od najefikasnijih mera, a koja značajno ima uticaj i na povećanje svesti i kulturu zaštite, jeste redovno održavanje vežbi[95] evakuacije i drugih elemenata zaštite. Podaci i informacije koje se dobiju tokom faze analize i evaluacije vežbi mogu ukazati na postojeću percepciju opasnosti, vrednosti i bezbednosnu kulturu, što ima presudan uticaj na ponašanje ljudskog resursa u vanrednim situacijama.

Efikasna pomoć organizacijama u izgradnji kontinuiranog procesa implementacije, održavanja i poboljšanja programa upravljanja vanrednim situacijama i kontinuitetom, može doći kroz primenu zahteva priznatih standarda, i u tom smislu možemo za potrebe ovog Priručnika navesti standard kanadske asocijacije za standardizaciju *Z1600-17*[96], a koji se bavi komponentama prevencije i ublažavanja, pripravnošću, reagovanjem i oporavkom. Preporuka njegove primene proizilazi ne samo iz razloga što je primenljiv na bilo koju organizaciju, bez obzira da li pripada javnom ili privatnom sektoru, odnosno nezavisno od njene veličine ili delatnosti, već i zbog činjenice da je razvijen u saradnji sa istaknutom američkom asocijacijom *NFPA* putem unapređenja njihovog standarda za spremnost na katastrofe *NFPA 1600*[97], kao i da je usklađen sa međunarodno priznatim standardima i smernicama

93 "Službeni glasnik RS", br. 102/2020.

94 "Službeni glasnik RS", br. 102/2020.

95 Za planiranje, sprovođenje i unapređenje projekata vežbi mogu se koristiti smernice date u *ISO 22398:2013, Societal security — Guidelines for exercises*.

96 *Z1600-17, Emergency and continuity management program*, Canadian Standards Association, Torontto CA, 2017.

97 *NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs*, National Fire Protection Association, Quincy MA, 2016.

profesionalne prakse - *ISO 22301, DRII Professional Practices for Business Continuity Practitioners* i *BCI Good Practice Guidelines.*

Zaštita od požara

Da li je potrebno naglašavati ulogu i značaj poslova zaštite od požara? Složićemo se da nema potrebe, i to ne samo iz razloga što smo svakodnevno svedoci požara koji posledično nanose manju ili veću materijalnu i nematerijalnu štetu, već i zbog činjenice da predstavlja najstarije uređenu oblast zaštite - prve pisane odredbe koje se odnose na oblast zaštite od požara u srpskoj državi nalazimo u Dušanovom Zakoniku iz 1349. godine, a osnov za razvoj moderne pravne regulative u oblasti zaštite od požara potiče iz 1834. godine kada je Đorđe Protić, ministar unutrašnjih poslova tadašnje Srbije, na zahtev kneza Miloša Obrenovića, sačinio i potpisao Uredbu o gašenju požara koja je imala odredbe o organizaciji gašenja požara, kao i odredbe koje su imale karakter preventive od požara.

Zakonom o zaštiti od požara[98] propisane su, pored ostalog, prava i obaveze državnih organa, organa autonomne pokrajine i organa jedinica lokalne samouprave, privrednih društava i drugih pravnih lica kao subjekata zaštite od požara, a odredbe ovog zakona shodno se primenjuju i na zaštitu od eksplozija. Polazni osnov za način organizacije poslova zaštite od požara privrednih društava, odnosno drugih pravnih lica jeste njihova ugroženost od požara, a shodno kategorizaciji njihovi objekti, delatnost i zemljište mogu pripadati prvoj, drugoj ili trećoj kategoriji ugroženosti od požara. Razvrstavanje po kategorijama vrši Ministarstvo unutrašnjih poslova na osnovu merila i uslova shodno odredbama *Uredbe o razvrstavanju objekta, delatnosti i zemljišta u kategorije ugroženosti od požara*[99].

Kategorija ugroženosti od požara uslovljava složenost tehničke opremljenosti i druge elemente zaštite od požara, pa su tako *Pravilnikom o organizovanju zaštite od požara prema kategoriji ugroženosti od požara*[100] propisani uslovi tehničke opremljenosti vatrogasne jedinice i broj pripadnika vatrogasne jedinice koje je obavezan da obezbedi subjekat iz prve kategorije ugroženosti od požara, kao i broj lica stručno osposobljenih za sprovođenje i organizovanje preventivnih mera i stalnog dežurstva u subjektima prve i druge kategorije ugroženosti od požara. Za obavljanje ovih poslova organizacija se može opredeliti za angažovanje ovlašćenog privrednog društva

98 „Službeni glasnik RS“, br. 111/2009, 20/2015, 87/2018 i 87/2018 - dr. zakoni.

99 „Službeni glasnik RS”, br. 76/2010.

100 „Službeni glasnik RS”, br. 6/2021.

koje ispunjava uslove propisane *Pravilnikom o bližim uslovima koje moraju ispunjavati pravna lica za obavljanje poslova organizovanja zaštite od požara u subjektima prve, druge i treće kategorije ugroženosti od požara*[101].

Bazni dokument za subjekte iz prve i druge kategorije ugroženosti jeste plan zaštite od požara koji se izrađuje na način i sadrži elemente propisane *Pravilnikom o načinu izrade i sadržaju Plana zaštite od požara autonomne pokrajine, jedinice lokalne samouprave i subjekata razvrstanih u prvu i drugu kategoriju*[102]. Za razliku od prethodno navedenih subjekata, organizacije koje su vlasnici ili korisnici objekata iz treće kategorije ugroženosti od požara dužni su shodno zakonu da donesu pravila zaštite od požara, a zajedničko za subjekte iz sve tri kategorije jeste da poseduju plan evakuacije i uputstva za postupanje u slučaju požara koji se ističu na vidljivom mestu.

Smatramo da nije potrebno posebno naglašavati značaj primene propisanih mera zaštite od požara prilikom projektovanja, izgradnje, rekonstrukcije i dogradnje objekata sa svim pripadajućim instalacijama, opremom i uređajima, kao ni u slučajevima kada organizacija u poslovanju primenjuje tehnološke procese u kojima se koriste ili proizvode zapaljive tečnosti i gasovi ili eksplozivne materije. Inače, nacionalne tehničke komisije[103] pri *Institutu za standardizaciju Srbije*, koji se formiraju u skladu sa međunarodnim i evropskim tehničkim komitetima, donele su spektar standarda koji se odnose na različite segmente zaštite od požara, od onih koji se odnose na tehničke mere zaštite od požara u zgradama do standarda za ispitivanje opasnosti od požara.

Požari iz prošlosti koji su se dogodili organizacijama različite delatnosti, kao i stečena saznanja tokom prakse, ukazuju da i pored zakonske uređenosti široke palete mera, radnji i normativa iz oblati zaštite od požara (zajedničkih za sve subjekte zaštite od požara ili usmerenih samo na subjekte iz određene delatnosti), i bez obzira na sprovođenje nadzora nad primenom mera, u praksi se kod mnogobrojnih pravnih lica javljaju propusti u različitim elementima organizacije i sprovođenja mera zaštite od požara, koji mogu biti uzročnici požara ili predstavljati slabe karike u sprovođenju sopstvenih politika prevencije i smanjenja rizika od požara, odnosno prilikom unapređenja zaštite i preduzimanja reaktivnih radnji (evakuacije, gašenja i dr.).

101 „Službeni glasnik RS", br. 6/2021.

102 „Službeni glasnik RS", br. 73/2010.

103 U okviru ISS funkcionišu komisije za standarde *Z021, Z021/PKS U092* i *N089* koje rade na donošenju srpskih standarda iz različitih oblasti zaštite od požara.

Upravo zato, ako bi morali navesti jednu meru koja ima istaknutu ulogu kako u preventivnom, tako i u reaktivnom pogledu, izdvojili bi obuku i jačanje svesti o sprovođenju mera zaštite od požara svih zaposlenih bez izuzetka, a posebno onih koji rade na poslovima zaštite od požara i koji su dužni da pohađaju posebnu obuku iz oblasti zaštite od požara. Zakonska je obaveza da se osnovna obuka iz oblasti zaštite od požara organizuje za sve zaposlene odmah po stupanju na rad, a najkasnije u roku od 30 dana od dana stupanja na rad, a program se sastoji od opšteg[104] i posebnog dela koji sadrži specifičnosti zaštite od požara za delatnost kojom se pravno lice bavi (provera znanja zaposlenih vrši se jednom u tri godine). Sa jačanjem ove mere, uz stalnu i stvarnu podršku top menadžmenta, možemo se nadati unapređenju zaštite od požara i pravovremenim akcijama na sprečavanju nastanka požara, kao i adekvatnim reakcijama prilikom gašenja i spasavanja ljudi i imovine, uz utvrđivanje i otklanjanje uzroka požara, umanjujući posledice i omogućavajući kontinuitet poslovanja.

Odbrambene pripreme

Od vrste, značaja i delatnosti korporacije zavisi i mesto, uloga i obaveze koje će shodno *Zakonu o odbrani* i *Zakonu o vojnoj, radnoj i materijalnoj obavezi*[105] imati u sistemu odbrane Republike Srbije, odnosno u određenoj funkciji zaštite suverenosti, nezavisnosti, teritorijalne celovitosti i bezbednosti RS u miru, vanrednom stanju i ratu. Kako bi mogli da ostvare svoju funkciju, odnosno da izvršavaju svoje obaveze i zadatke privredna društva, druga pravna lica i preduzetnici od značaja za odbranu, uz državne organe i druge subjekte sistema odbrane, moraju činiti organizovanu strukturu subjekata sistema odbrane, i u tom smislu dužni su da vrše i poslove odbrane zemlje koji se odnose na planiranje, organizovanje, pripremanje i osposobljavanje za rad u ratnom i vanrednom stanju, a ostali, koji nemaju tu obavezu, da na zahtev Ministarstva odbrane dostavljaju podatke od značaja za odbranu.

Neophodno je navesti da organizacije, tj. Subjekti od značaja za odbranu svoje planove odbrane izrađuju u skladu sa nizom podzakonskih propisa (koji su javnog ili poverljivog karaktera), a od kojih možemo istaći *Uputstvo o jedinstvenoj metodologiji za izradu planova odbrane i merama bezbednosti u izradi planova odbrane*, koje je poverljive prirode. Zaposleni koji obavljaju poslove planiranja i rukovaoci planova

104 Minimum sadržine opšteg dela programa za obuku zaposlenih propisan je *Pravilnikom o minimumu sadržine opšteg dela Programa obuke radnika iz oblasti zaštite od požara* („Službeni glasnik SRS", br. 40/1990).

105 „Službeni glasnik RS", br. 88/2009, 95/2010 i 36/2018.

odbrane u tim organizacijama podležu bezbednosnoj proveri i izdaje im se odgovarajući sertifikat u skladu sa zakonom kojim se uređuje zaštita tajnosti podataka[106].

U slučaju da korporacija predstavlja veliki tehničko-tehnološki sistem[107] ili poseduje objekat u kojima se proizvodi, skladišti ili čuvaju predmeti ili vrše usluge[108] za potrebe odbrane, kao i ukoliko je organizacija državni organ ili pravno lica od posebnog značaja za odbranu zemlje[109], odnosno predstavlja određeni infrastrukturni objekat, objekti u kojima su smeštene te organizacije ili u njima vrše navedene delatnosti predstavljaju objekte od posebnog značaja za odbranu zemlje. Dok je MUP nadležan za pripremanje mera bezbednosti i zaštite navedenih objekata u ratnom i vanrednom stanju, organizacije kojima pripadaju objekti od posebnog značaja za odbranu dužne su da u mirnodopskim uslovima realizuju organizovanje i sprovođenje mera za njihovu zaštitu od oštećenja ili uništenja, odnosno otkrivanja tajnih podataka o objektima ili samih objekata – lokacija.

Ne ulazeći dublje u benefite, ali i problematiku realizacije propisanih mera priprema za odbranu, napominjemo da su organizacije od značaja za odbranu dužne da o određenim radnjama (npr. prilikom izgradnje vitalnih, odnosno kapitalnih objekata i razvoja velikih tehničkih sistema od značaja za odbranu, odnosno nabavke tehničkih sredstava od značaja za funkcionisanje tih sistema) obaveštavaju Ministarstvo odbrane, odnosno pribave njihovu saglasnost prilikom standardizacije i tipizacije proizvoda i usluga, objekata i uređaja od posebnog značaja za odbranu zemlje kako bi ti proizvodi i usluge, odnosno objekti i uređaji bili prilagođeni potrebama odbrane zemlje. Takođe, prethodna saglasnost Ministarstva odbrane potrebna je i za pristup i građenje u rejonu uz objekte od posebnog značaja za odbranu, a koji su određeni *Odlukom o objektima od posebnog značaja za odbranu*[110].

106 Bliže uređeno članom 4. *Uredbe o podacima i poslovima značajnim za sistem odbrane koji se moraju* čuvati *i* štititi *u skladu sa zakonom kojim se uređuje zaštita tajnosti podataka i o kriterijumima za popunu radnih mesta na kojima se ti zadaci i poslovi obavljaju* („Službeni glasnik RS", br. 8/2020).

107 Shodno *Odluci o određivanju velikih tehničkih sistema od značaja za odbranu* ("Službeni glasnik RS", br. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019 i 67/2021).

108 U skladu sa *Odlukom o određivanju proizvoda i usluga od posebnog značaja za odbranu Republike Srbije* („Službeni glasnik RS", br. 58/2008 i 26/2019).

109 *Odluka o određivanju pravnih lica od značaja za odbranu Republike Srbije* („Službeni glasnik RS", br. 52/2008).

110 „Službeni glasnik RS", br. 112/2008.

Bezbednost i zdravlje na radu

Osnovna uloga sprovođenja mera bezbednosti i zdravlja na radu (eng. *occupational health and safety* (*OH&S*)) ogleda se u sprečavanju povreda na radu, profesionalnih bolesti i bolesti u vezi sa radom lica koja učestvuju u radnim procesima, odnosno lica koja se zateknu u radnoj sredini (npr. volonteri, učenici i studenti na praksi, lica koja su upućena na dodatno obrazovanje i obuku, posetioci dr.). Izlišno je u modernom poslovanju apostrofirati značaj preduzimanja ovih mera, koja spadaju u red „klasičnih" *safety* poslova. O visini rizika koji su u vezi sa radnim procesima i radnoj sredini dovoljno je ukazati na podatke iz godišnjih izveštaja o radu *Uprave za bezbednost i zdravlje na radu*, koji za 2023. godinu pokazuju da je u RS ukupno bilo 13 406 povreda na radu, od čega 14 sa smrtnim ishodom[111]. Shodno pregledu povreda na radu prema delatnosti uočava se da je tokom 2023. godine najviše povreda bilo u prerađivačkoj industriji, zatim trgovini na veliko i na malo, popravci motornih vozila i motocikala, potom u sektoru zdravstvene i socijalne zaštite itd. Uporednim pregledom unazad nekoliko godina možemo zaključiti da broj povreda dominira u prerađivačkoj industriji, sledi delatnost saobraćaja i skladištenja, dok je građevinarstvo uvek u vrhu liste. Imperativ svakog poslodavca jeste da ima zdrave i radno motivisane zaposlene, što se, pored ostalog, postiže obezbeđivanjem takvih uslova na radu kojima se, u najvećoj mogućoj meri, smanjuju povrede na radu, profesionalne bolesti i bolesti u vezi sa radom u cilju ostvarivanja fizičkog, psihičkog i socijalnog blagostanja zaposlenih. Bezbednost radne sredine (radnih mesta, radnih uslova, radnih postupaka i sredstava za rad) postiže se, pre svega, beskompromisnom primenom mera u skladu sa *Zakonom o bezbednosti i zdravlju na radu*, propisima donetim na osnovu zakona, kao i primenom važećih standarda koji pospešuju primenu mera iz ove oblasti.

Zakonodavac je propisao poslodavcu dužnost organizovanja poslova bezbednosti i zdravlja na radu, preduzimanja opštih i posebnih obaveza, kao i sprovođenja obuke zaposlenih za bezbedan i zdrav rad, ali je uredio i prava i obaveze zaposlenih. Iz razloga što opasnosti i štetnosti u radnoj sredini mogu da budu pojedinačnog i kolektivnog karaktera i da rezultiraju velikim posledicama, ističemo da se preduzimanje mera bezbednosti i zdravlja na radu, posebno onih preventivnih, ne sme smatrati isključivo delokrugom funkcije korporativne bezbednosti, već odgovornost pripada svakoj organizacionoj celini i svakom zaposlenom, počevši od top menadžmenta pa nadalje.

111 *Izveštaj o radu za 2023. godinu*, Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, Uprava za bezbednost i zdravlje na radu, Beograd, 2024.

Važeći *Zakon o bezbednosti i zdravlju na radu*, koji je stupio na snagu tokom 2023. godine, pored usaglašavanja sa evropskim standardima, ima za cilj značajno podizanje nivoa bezbednosti na radu od strane poslodavaca, ali i veću odgovornost zaposlenih u primeni zaštitnih mera. Zakon je doneo mnoge inovacije kao što je:

- obezbeđivanje bezbednosti i zdravlja na radu od kuće i radu na daljinu,
- uređenje preventivnih mera za visokorizične poslove,
- uvođenje savetnika,
- odnosno saradnika za bezbednost i zdravlje na radu,
- periodične obuke za bezbedan i zdrav rad zaposlenog koji radi na radnom mestu sa povećanim rizikom itd.

Složićemo se da problematika upravljanja poslovima bezbednosti i zdravlja na radu iziskuje poseban priručnik, pa ćemo za potrebe ovog napomenuti samo značaj sprovođenja postupka procene rizika[112] i obavezu donošenja akta o proceni rizika u pisanoj formi za sva radna mesta u radnoj sredini i utvrđivanje načina, mera i rokova za otklanjanje ili smanjenje rizika na najmanju moguću meru (praksa ukazuje da je delotvorno grupisati „srodna" radna mesta i po tim grupama proceniti rizik). Istakli bi i važnost uloge zaposlenih, koji imaju jasna zakonska prava i obaveze, kao i značaj adekvatnog delovanja Odbora za bezbednost i zdravlje na radu, koji je neophodno da bude većinski obrazovan od predstavnika zaposlenih u odnosu na broj predstavnika poslodavca. Potvrdu poštovanja nivoa primene odredbi zakona, propisa donetih na osnovu zakona, tehničkih i drugih mera koje se odnose na bezbednost i zdravlje na radu pružiće i inspektor rada putem sprovođenja poslova inspekcijskog nadzora u skladu sa zakonskim ovlašćenjima i dužnostima, a postupke usklađuje i sa *Instrukcijom o postupanju inspektora rada prilikom vršenja inspekcijskog nadzora u oblasti radnih odnosa i bezbednosti i zdravlja na radu*[113].

Sa ciljem unapređenja načina primene i upravljanja merama bezbednosti i zdravlja na radu, proaktivnog poboljšanja svojih *OH&S* performansi, ali i zarad dokazivanja privrženosti kompanije sprovođenju tih poslova, mnoge organizacije implementiraju zahteve međunarodnog standarda *ISO 45001*[114]. Kao i ostali stan-

112 O načinu i postupku procene rizika videti: *Pravilnik o načinu i postupku procene rizika na radnom mestu i u radnoj okolini* ("Službeni glasnik RS", br. 72/2006, 84/2006 - ispravka, 30/2010 i 102/2015).

113 Pogledati: *Oblast bezbednosti i zdravlja na radu, Drugi deo*, Inspektorat za rad, Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, Beograd, 2018.

114 *ISO 45001:2018, Occupational health and safety management systems — Requirements with*

dardi koji se odnose na sistem menadžmenta i ovaj dokument specificira zahteve sistema menadžmenta bezbednošću i zdravljem na radu, i uspostavlja kriterijume za *OH&S* politiku, ciljeve, planiranje, implementaciju, rad, proveru i preispitivanja, a sve u skladu sa procesnim pristupom po modelu *Plan-Do-Check-Act (PDCA)*[115]. Kao što se *Izmenom 1*[116] navedenog standarda ukazuje na značaj preispitivanja uticaja klimatskih promena, tako se i objavljenim smernicama *ISO 45003*[117] ističe važnost psihološkog zdravlja i bezbednosti na radu, kao i značaj upravljanja psihosocijalnim rizicima, koji su u prethodnom periodu, moramo priznati, bili zanemareni u odnosu na fizičke. Pored primene navedenih standarda organizacije mogu sprovoditi i druge smernice i preporuke koje pospešuju mere bezbednosti i zdravlja u okviru njihove delatnosti, i imaju uticaj na sprečavanje povreda u vezi sa radom i obolevanje zaposlenih i ostalih zainteresovanih strana. Primera radi, ukoliko je poslovanje organizacije vezano za drumski saobraćaj poželjno je da ima izgrađen sistem upravljanja bezbednošću drumskog saobraćaja u skladu sa *ISO 39001*[118], čime bi nastojala da utiče na smanjenje broja poginulih i teško povređenih u nezgodama.

U okviru celovite brige o bezbednosti i zdravlju na radu zaposlenih potrebno je da organizacija procenjuje i upravlja rizicima prilikom njihovog putovanja, kako u zemlji, tako i u inostranstvo, a posebno u slučajevima postojanja različitih kriznih situacija (npr. pandemija izazvana virusom SARS-CoV-2, teroristički napad, demonstracije, zemljotres, poplava ili druga elementarna nepogoda ili tehničko-tehnološka nesreća i dr.). Svi zaposleni koji putuju (uključujući i top menadžment) moraju da dobiju saznanja i budu svesni bezbednosnih rizika na putu, kako onih koji mogu izazvati štetne posledice po podatke i sredstva kompanije (uticaj na poverljive informacije, IT opremu, platne kartice itd.), tako i onih koji mogu ugroziti zdravlje ili izazvati povredu (povreda, bolest ili oštećenje zdravlja usled izloženosti opasnostima ili štetnostima). Jasne procedure u slučaju nastupanja bezbednosnog incidenta

guidance for use.

115 *Plan-Do-Check-Act (srp. Planiraj-Uradi-Proveri-Deluj)* model je poznat i pod nazivom „Demingov krug" koji je razvio američki teoretičar poslovanja William Edwards Deming. Metodologija stalnog poboljšavanja se temelji na procesnom pristupu koji se bazira na postavci da je za uspešno funkcionisanje sistema nužno utvrditi njene međusobno povezane (procese), te njima upravljati na jednostavan, uspešan i efikasan način.

116 *ISO 45001:2018/Amd 1:2024, Occupational health and safety management systems — Requirements with guidance for use; Amendment 1: Climate action changes.*

117 *ISO 45003:2021, Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks.*

118 *ISO 39001:2012, Road traffic safety (RTS) management systems — Requirements with guidance for use.*

ili događaja (npr. bolest, povreda, teroristički napad, zemljotres itd.), između ostalog, moraju sadržati način interne komunikacije, kontakt listu, a po potrebi saradnju sa nadležnim državnim organima i medijima, pravnu i drugu vrstu pomoći[119].

Ono što praksa pokazuje jeste da je veoma bitno već prilikom pravljenja organizacije poslova i sistematizacije radnih mesta voditi računa i inkorporirati mere i radnje koje se odnose na bezbednost i zdravlje na radu. Isto je bitno prilikom izgradnje objekata, nabavci sredstava, novim procesima i proizvodima itd., zašta je potrebno da bezbednosna kultura bude na progresivnom nivou, kada se od početnog planiranja do realizacije izrazito vodi računa o OH&S merama. Reaktivni nivo kulture koji se svodi samo na brigu o bezbednosti kada se već desi neki incident može da bude „krpljenje rupa" koje je možda i nemoguće zakrpiti. Davanje prednosti kolektivnim nad pojedinačnim merama bezbednosti i zdravlja na radu spada u osnovno načelo prevencije, a *OH&S* mere nipošto ne smeju da se svedu isključivo na administrativne poslove i formalno zadovoljenje odredbi zakonskih propisa i zahteva standarda.

Svakoj organizaciji kojoj je stalo do društveno odgovornog poslovanja izrazito vodi računa o bezbednosti i zdravlju zaposlenih, što predstavlja jedan od elemenata međunarodnog standarda za društvenu odgovornost *SA8000*[120], koji postavlja određene zahteve koje treba da ispune organizacije, uključujući i one koji se odnose na uslove u radnoj okolini. Pored ostalog, zahtevi upućuju na obavezu organizacije za pružanjem bezbednog i zdravog okruženja u radnoj sredini i na preduzimanje efikasnih mera za sprečavanje potencijalnih zdravstvenih i bezbednosnih incidenata i povreda na radu ili profesionalne bolesti koji proizilaze iz, u vezi sa ili se javljaju u toku rada.

Zaštita životne sredine

Životna sredina predstavlja skup prirodnih i stvorenih vrednosti čiji kompleksni međusobni odnosi čine okruženje, odnosno prostor i uslove za život. Kvalitet životne sredine je stanje te sredine koje se iskazuje fizičkim, hemijskim, biološkim, estetskim i drugim indikatorima. U tom kontekstu, prirodne vrednosti su prirodna

119 Primer smernica za osnovne principe, mere i druge elemente upravljanja rizicima putovanja zaposlenih pogledati više: *Aufbau und Struktur Eines Reise-Risikomanagements*, ASW Bundesverband, Berlin DE, 2016.

120 *Social Accountability International 8000*, SAI, New York NY, June 2014.

bogatstva koja čine vazduh, voda, zemljište, šume, geološki resursi, biljni i životinjski svet.

Geodiverzitet (geološka raznovrsnost) se odnosi na prisustvo ili rasprostranjenost raznovrsnih elemenata i oblika geološke građe, geoloških struktura i procesa, geohronoloških jedinica, stena i minerala različitog sastava i načina postanka i raznovrsnih paleoekosistema menjanih u prostoru pod uticajima unutrašnjih i spoljašnjih geodinamičkih činilaca tokom geološkog vremena. Druga prirodna vrednost - biodiverzitet (biološka raznovrsnost) predstavlja raznovrsnost organizama u okviru vrste, među vrstama i među ekosistemima i obuhvata ukupnu raznovrsnost gena, vrsta i ekosistema na lokalnom, nacionalnom, regionalnom i globalnom nivou.

Aktivnost koja utiče na životnu sredinu je svaki zahvat (stalni ili privremeni) kojim se menjaju i/ili mogu promeniti stanja i uslovi u životnoj sredini, a odnosi se na korišćenje resursa i prirodnih dobara, procese proizvodnje i prometa, distribuciju i upotrebu materijala, ispuštanje (emisiju) zagađujućih materija u vodu, vazduh ili zemljište, upravljanje otpadom i otpadnim vodama, hemikalijama i štetnim materijama, buku i vibracije, jonizujuće i nejonizujuće zračenje, kao i udese.

Pod zagađivanjem životne sredine se podrazumeva unošenje zagađujućih materija ili energije u životnu sredinu, izazvano ljudskom delatnošću ili prirodnim procesima koje ima ili može imati štetne posledice na kvalitet životne sredine i zdravlje ljudi. Pojam zagađivača je vezan za pravno ili fizičko lice koje svojom aktivnošću ili neaktivnošću zagađuje životnu sredinu.

Degradacija životne sredine je proces narušavanja njenog kvaliteta koji nastaje prirodnom ili ljudskom aktivnošću ili je posledica nepreduzimanja mera radi otklanjanja uzroka narušavanja kvaliteta ili štete po životnu sredinu, prirodne ili radom stvorene vrednosti. Sanacija, odnosno remedijacija jeste proces preduzimanja mera za zaustavljanje zagađenja i dalje degradacije životne sredine do nivoa koji je bezbedan za buduće korišćenje lokacije uključujući uređenje prostora, revitalizaciju i rekultivaciju.

U savremenom dobu svaka ljudska delatnost u većoj ili manjoj meri utiče na životnu sredinu. Zagađivači okoline nisu samo velike korporacije, budući da i srednje i manje kompanije svojim aktivnostima značajno utiču na degradaciju prirodnog okruženja. Istovremeno, svaki poslovni subjekt može doprineti smanjenju negativnog uticaja na životnu sredinu tako što će smanjiti ispuštanje štetnih materija, redukovati količine proizvedenog otpada i racionalnije koristiti skupe i neobnovljive resurse. Iako na prvi pogled ne deluje tako, korporacija koja se opredeli za delovanje

u pravcu unapređenja svog odnosa prema prirodnom okruženju može da ostvari i finansijske uštede, te da poveća svoju konkurentnost i ugled na tržištu.

U novije vreme je primetan rast ekološkog kriminala, odnosno radnji počinjenih sa namerom da se načini ili potencijalno prouzrokuje šteta ekološkim i/ili biološkim sistemima radi sticanja poslovnog ili privatnog preimućstva.

Ugrožavanje životne sredine se odražava i na klimatske promene, čije se posledice (globalno zagrevanje i porast nivoa mora, porast temperatura, nestašice hrane, siromaštvo itd.) kao bumerang vraćaju u vidu opasnosti po život i zdravlje ljudi/zaposlenih, odnosno na ukupno poslovanje korporacija. Po prvi put uvedena skraćenica *ESG* od termina *Environmental* (životna sredina), *Social* (društvo) i *Governance* (rukovođenje) u izveštaju Ujedinjenih nacija *„Ko se brine, taj pobeđuje"*[121] ukazuje na značaj implementacije principa koja doprinose održivom razvoju globalnog društva. Uočavajući pogubnost višedecenijskog uticaja škole ekonomske misli koje je isticalo finansijski rezultat kao jedino merilo poslovnog uspeha, Ujedinjene nacije supreduzele aktivnosti na usklađivanju potreba za ekonomskim rastom uz održivi razvoj, uobličavajući ih kroz *Agendu za održivi razvoj*.[122] Naslanjajući se na ciljeve iz navedene agende EU je krajem 2022. godine uvela obavezu izveštavanja o korporativnoj održivosti, odnosno donela je pravila (*Directive EU 2022/2464*) koja zahtevaju da velike kompanije, kao i mala i srednja preduzeća koja su na berzi (osim navedenih mikro preduzeća), objavljuju redovne izveštaje o društvenim i ekološkim rizicima sa kojima se suočavaju, kao i o tome kako njihove aktivnosti utiču na ljude i životnu sredinu.[123]

Regulatorni okvir u Republici Srbiji još uvek u potpunosti ne uređuje izveštavanje o održivom razvoju, ali je *Zakonom o računovodstvu*[124] uvedena obaveza nefinansijskog izveštavanja. Osim određenih izuzetaka, velika pravna lica koja su društva od javnog interesa i koja na datum bilansa prelaze kriterijum prosečnog broja od 500 zaposlenih tokom poslovne godine, dužna su da u godišnji izveštaj o poslovanju uključe nefinansijski izveštaj, a koji, pored ostalog, sadrži informacije neophodne za

121 Videti: *Who Cares Wins*, Swiss Federal Department of Foreign Affairs & United Nations, Bern CH-New York NY, 2004.

122 *Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1*, United Nations, New York NY, 2015.

123 *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU() No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainibility reporting*, (OJ L 322, Brussels, 16.12.2022, pp. 15–80).

124 "Službeni glasnik RS", br. 73/2019 i 44/2021 - dr. zakon.

razumevanje razvoja i rezultata njegovih aktivnosti koje se odnose na zaštitu životne sredine. Regulatorni pritisak u vezi s *ESG* će biti sve veći, a poželjno je, i u praksi je zastupljeno, da izveštaji o održivom razvoju budu usaglašeni sa *GRI* univerzalnim i sektorskim standardima[125], odnosno standardima drugih priznatih organizacija kao što su *ISSB (International Sustainability Standards Board), EFRAG (European Financial Reporting Advisory Group)* i *TCFD (Task Force on Climate-related Financial Disclosures).*

Poslednjih decenija se govori i o principu društvene odgovornosti korporacija (*Corporate Social Responsibility - CSR*), čiji je sadržaj obuhvaćen akronimom *HSEC (Health, Safety, Environment, Management, Community Relations*). Osnovne komponente *HSEC* su:

- zdravlje (*Health*), što znači promovisanje i poboljšanje kvaliteta zdravlja zaposlenih u kompaniji i okolnog stanovništva;
- sigurnost (*Safety*), odnosno ustanovljenje zaštitnih vrednosti i obezbeđivanje radnog okruženja za bezbedan i siguran rad zaposlenih;
- životna sredina (*Environment*), pod čime se podrazumeva promovisanje efikasnog korišćenja poslovnih resursa uz smanjenje zagađenja životne sredine i očuvanje biološke raznolikosti;
- društvena zajednica (*Community*), što uključuje poštovanje etičkih principa, doprinos ekonomskom prosperitetu i održivom razvoju društvene zajednice u okruženju i poštovanje ljudskih prava.

Zagovornici društvene odgovornosti korporacija polaze od hipoteze da poslovni subjekti sa boljom reputacijom imaju konkurentnu prednost nad kompanijama sa manjom ili nedovoljno dobrom reputacijom. Naime, ukazuje se da bolja reputacija donosi profit, štiti korporaciju u vremenima kriza i sprečava njeno uvlačenje u političke sporove u društvu. Shodno tome, osnovna ideja korporativne društvene odgovornosti je jednostavna - korporacije su društveni identiteti, zbog čega treba da učestvuju u aktuelnim pitanjima zajednice, da ozbiljno shvataju svoju obavezu prema društvu i da nastoje da je ispune. Prema nekim istraživanjima, društvena odgovornost, kvalitetno upravljanje i stabilne finansije korporacije čine osnovne atribute reputacije, što je istovremeno povezano sa dobrim finansijskim poslovanjem.

125 Univerzalni i sektorski standardi reprezentativne međunarodne neprofitne organizacije *Global Reporting Initiative (GRI)* omogućavaju svakoj organizaciji da razume i izveštava o svom uticaju na privredu, životnu sredinu i ljude na uporediv i kredibilan način, čime se povećava transparentnost njihovog doprinosa održivom razvoju.

Nasuprot tome, ima mišljenja da se iza politike korporativne društvene odgovornosti, a naročito javnih izjava kojima kompanije same sebe hvale, kriju nastojanja da se strategija određene korporacije predstavi kao dobra i uspešna i da se samim tim izbegnu kritike na njen račun. O tome svedoče i marketinški potezi poput nagrada koje kompanije dodeljuju same sebi, uz čestitke na navodnoj korporativnoj društvenoj odgovornosti. S tim u vezi, postavlja se pitanje da li to predstavlja dobru praksu upravljanja ili nastojanja korporacije da se na lak način pozicionira na tržištu.

Prisutna su i zagovaranja ekološkog, odnosno zelenog kapitalizma, prema kojima kapital postoji u prirodi kao „prirodni kapital" (ekosistemi koji imaju ekološki prinos), a od koga zavisi celokupno društveno bogatstvo. Shodno tome, vlade treba da koriste tržišne instrumente politike (porez na emisije ugljen-dioksida i slično) za rešavanje ekoloških problema. Kritičari ovakve teze ocenjuju kao desničarski ekvivalent savremenih ekoloških/zelenih pokreta.[126]

Korporativna ekološka odgovornost (*Corporate Ecological Responsibility - CER*) se odnosi na obaveze kompanije da se suzdržava od oštećenja prirodnog okruženja. Termin potiče od korporativne društvene odgovornosti (*CSR*).

O ekološkom aspektu korporativne društvene odgovornosti se raspravljalo u poslednjih nekoliko decenija, s obzirom da zainteresovane strane sve više zahtevaju od korporacija da postanu ekološki svesnije i društveno odgovorne. U tradicionalnom poslovnom modelu, zaštita životne sredine se razmatrala samo u odnosu na „javni interes", pri čemu su vlade imale osnovnu odgovornost za obezbeđivanje upravljanja i očuvanja životne sredine. Javni sektor je fokusiran na izradu propisa i izricanje sankcija kao sredstva za podsticanje zaštite životne sredine. U novije vreme je privatni sektor usvojio pristup suodgovornosti prema prevenciji i ublažavanju štete po životnu sredinu.[127]

Svetska komisija za životnu sredinu je 1987. godine objavila Bruntland izveštaj 1987. godine posvećen pitanjima održivog razvoja. Od tada menadžeri, stručnjaci i vlasnici kompanija istražuju načine i modalitete da korporacije uključe aspekte zaštite životne sredine u svoje politike.

Glavni elementi korporativne ekološke odgovornosti se odnose na:

126 Guttmann Robert, *Eco-Capitalism: Carbon Money, Climate Finance, and Sustainable Development*, Palgrave Macmillan, London UK 2018, pp. 252-256.

127 Mazurkiewicz Piotr, *Corporate Environmental Responsibility: Is a common CSR framework possible?*, World Bank, Wachington DC 2004, pp. 4-6.

- bezbedno odlaganje otpada i smanjenje emisije gasova sa efektom staklene bašte;
- efikasno korišćenje resursa i unapređenje produktivnosti.

Među glavnim pokretačima *CER-a* su vladine politike i propisi. Mnoge države su donele nacionalne zakone, propise i politike, koje su bitne za stvaranje pozitivnog odnosa kompanija prema životnoj sredini. Subvencije, tarife i porezi igraju vitalnu ulogu u sprovođenju ovih politika. Drugi značajan faktor je konkurentsko okruženje među kompanijama koje uspostavljaju mediji, javnost, akcionari i NVO, koji su takođe glavni pokretači *CER-a*. Značajan podsticaj korporativnoj ekološkoj odgovornosti je i stav da je privatni sektor u velikoj meri odgovoran za razvoj zelene tehnologije i obnovljivih izvora energije, što doprinosi ublažavanju klimatskih promena, a ne utiče negativno na poslovanje.

Izazovi uključuju troškove regulacije i poteškoće u predviđanju ekonomske dobiti, što bi moglo postati problematično za menadžment korporacija. Pored toga, nove tehnologije su često preskupe za mnoge kompanije. Drugi problem je odsustvo harmonizacije nacionalnih propisa, što dovodi do nejasnih strategija i ponašanja prema životnoj sredini, što je posebno prisutno kod multinacionalnih korporacija. Dalji izazovi *CER-a* su da li korporacije imaju odgovornost da idu dalje od postojećeg zakonodavstva i da li su one prvenstveno odgovorne za stvaranje profita za akcionare i proizvodnju robe za kupce.

Ideja korporativne ekološke odgovornosti je da ljudi budu svesniji uticaja na životnu sredinu i da se suprotstave najakutnijem zagađenju (ugljeničnom otisku) životne sredine. Jedan od glavnih faktora je smanjenje ugljičnog otiska i emisije ugljenika, pri čemu se različite studije fokusiraju na pokušaj pronalaženja ravnoteže između ekonomskog rasta i smanjenja otpada i čistije životne sredine.[128]

U Republici Srbiji je problematika životne sredine normativno regulisana *Zakonom o zaštiti životne sredine*[129]. Inače, prema članu 74. *Ustava Republike Srbije*, svako ima pravo na zdravu životnu sredinu i na blagovremeno i potpuno obaveštavanje o njenom stanju (to bi trebalo da čini Zavod za zaštitu zdravlja Republike Srbije). Očuvanje životne sredine je i jedna od mera predviđenih *Strategijom nacionalne*

128 Kennard Amanda, „The Enemy of My Enemy: When Firms Support Climate Change Regulation", *International Organization*, Vol. 74, Issue 2, Cambridge University Press, Cambridge UK 2020, pp. 211-215.

129 „Službeni glasnik RS", br. 135/2004, 36/2009, 36/2009 - dr. zakon, 72/2009 - dr. zakon, 43/2011 - odluka US, 14/2016, 76/2018, 95/2018 - dr. zakon i 95/2018 - dr. zakon.

bezbednosti Republike Srbije[130] čijim se preduzimanjem sprovodi politika nacionalne bezbednosti. U tom kontekstu, sva pravna lica bi trebala da pomognu u dostizanju ciljeva predviđenih navedenom strategijom kao što su zaštita od poplava i požara, unapređenje kvaliteta životne sredine, efikasno upravljanje opasnim otpadom i drugo.

Zakonom o zaštiti životne sredine se uređuje integralni sistem zaštite životne sredine kojim se obezbeđuje ostvarivanje prava čoveka na život i razvoj u zdravoj životnoj sredini i uravnotežen odnos privrednog razvoja i životne sredine u Srbiji. Sistem zaštite životne sredine čine mere, uslovi i instrumenti za:

- održivo upravljanje, očuvanje prirodne ravnoteže, celovitosti, raznovrsnosti i kvaliteta prirodnih vrednosti i uslova za opstanak svih živih bića;
- sprečavanje, kontrolu, smanjivanje i sanaciju svih oblika zagađivanja životne sredine.

Taj sistem, u okviru svojih ovlašćenja, obezbeđuju Republika Srbija, autonomna pokrajina, opština, odnosno grad, preduzeća, druga domaća i strana pravna lica i preduzetnici koji u obavljanju privredne i druge delatnosti koriste prirodne vrednosti, ugrožavaju ili zagađuju životnu sredinu, naučne i stručne organizacije i druge javne službe, građani, grupe građana, njihova udruženja, profesionalne ili druge organizacije. Svi subjekti sistema zaštite životne sredine dužni su da čuvaju i unapređuju životnu sredinu.[131]

Pravna i fizička lica dužna su da u obavljanju svojih delatnosti obezbede: racionalno korišćenje prirodnih bogatstava; uračunavanje troškova zaštite životne sredine u okviru investicionih i proizvodnih troškova, primenu propisa, odnosno preduzimanje mera zaštite životne sredine, u skladu sa zakonom.

Saglasno Zakonu, održivi razvoj je usklađeni sistem tehničko-tehnoloških, ekonomskih i društvenih aktivnosti u ukupnom razvoju u kojem se na principima ekonomičnosti i razumnosti koriste prirodne i stvorene vrednosti Republike Srbije sa ciljem da se sačuva i unapredi kvalitet životne sredine za sadašnje i buduće generacije. Održivi razvoj ostvaruje se donošenjem i sprovođenjem odluka kojima se obezbeđuje usklađenost interesa zaštite životne sredine i interesa ekonomskog razvoja.

Pravno ili fizičko lice koje svojim nezakonitim ili neispravnim aktivnostima dovodi do zagađenja životne sredine odgovorno je u skladu sa zakonom. Zagađivač

130 „Službeni glasnik RS“, br. 94/2019.

131 Član 4. Zakona o zaštiti životne sredine.

je odgovoran za zagađivanje životne sredine i u slučaju likvidacije ili stečaja preduzeća ili drugih pravnih lica, u skladu sa zakonom. Promene vlasništva preduzeća i drugih pravnih lica ili drugi oblici promene svojine obavezno uključuju procenu stanja životne sredine i određivanje odgovornosti za zagađenje životne sredine, kao i namirenje dugova (tereta) prethodnog vlasnika za izvršeno zagađivanje i/ili štetu nanetu životnoj sredini.

Zagađivač plaća naknadu za zagađivanje životne sredine kada svojim aktivnostima prouzrokuje ili može prouzrokovati opterećenje životne sredine, odnosno ako proizvodi, koristi ili stavlja u promet sirovinu, poluproizvod ili proizvod koji sadrži štetne materije po životnu sredinu. Pravno i fizičko lice koje degradira životnu sredinu dužno je da izvrši sanaciju i remedijaciju degradirane životne sredine, u skladu sa projektom sanacije i remedijacije.[132]

Zagađivač koji prouzrokuje zagađenje životne sredine odgovara za nastalu štetu po načelu objektivne odgovornosti. Za zagađivanje životne sredine odgovorno je i pravno i fizičko lice koje je nezakonitim ili nepravilnim delovanjem omogućilo ili dopustilo zagađivanje životne sredine. Zagađivač koji svojim činjenjem ili nečinjenjem prouzrokuje zagađivanje životne sredine dužan je da, bez odlaganja, preduzme mere utvrđene planom zaštite od udesa i sanacionim planom, odnosno da preduzme neophodne mere radi smanjenja šteta u životnoj sredini ili uklanjanja daljih rizika, opasnosti ili sanacije štete u životnoj sredini. Ako šteta naneta životnoj sredini ne može da se sanira odgovarajućim merama, lice koje je prouzrokovalo štetu odgovorno je za naknadu u visini vrednosti uništenog dobra.[133]

Održivo korišćenje i zaštita prirodnih vrednosti obezbeđuju se u okviru Strategije prostornog razvoja Republike Srbije i Nacionalne strategije održivog korišćenja prirodnih resursa i dobara, koje donosi Vlada.

Procena uticaja projekta na životnu sredinu vrši se za projekte koji se planiraju i realizuju u prostoru, uključujući promene tehnologije, rekonstrukciju, proširenje kapaciteta ili prestanak rada koji mogu dovesti do značajnog zagađivanja životne sredine ili predstavljaju rizik po zdravlje ljudi. Procena uticaja vrši se za projekte iz oblasti industrije, rudarstva, energetike, saobraćaja, turizma, poljoprivrede, šumarstva, vodoprivrede, upravljanja otpadom i komunalnih delatnosti, kao i za projekte koji se planiraju na zaštićenom prirodnom dobru i u zaštićenoj okolini nepokretnog kulturnog dobra. Procena uticaja projekta na životnu sredinu je sastavni deo tehnič-

132 Član 16. Zakona o zaštiti životne sredine.

133 Član 104. Zakona o zaštiti životne sredine.

ke dokumentacije bez koje se ne može pristupiti izvođenju projekta i vrši se u skladu sa postupkom propisanim posebnim zakonom.[134]

U Republici Srbiji primenjuju se srpski standardi za upravljanje i sertifikaciju sistema upravljanja zaštitom životne sredine. Pravna lica, preduzetnici i organizacije mogu sertifikovati svoj sistem upravljanja zaštitom životne sredine u skladu sa standardom *SRPS ISO 14001*[135]. Pravna lica, preduzetnici i organizacije, koja imaju uspostavljen sistem upravljanja zaštitom životne sredine mogu se uključiti u sistem upravljanja zaštitom životne sredine i provere (Sistem EMAS).[136]

Pravno i fizičko lice dužno je da u obavljanju svoje aktivnosti obezbedi zaštitu životne sredine, i to:

- primenom i sprovođenjem propisa o zaštiti životne sredine;
- održivim korišćenjem prirodnih resursa, dobara i energije;
- uvođenjem energetski efikasnijih tehnologija i korišćenjem obnovljivih prirodnih resursa;
- upotrebom proizvoda, procesa, tehnologija i prakse koji manje ugrožavaju životnu sredinu;[137]
- preduzimanjem mera prevencije ili otklanjanja posledica ugrožavanja i štete po životnu sredinu;
- vođenjem evidencije na propisani način o potrošnji sirovina i energije, ispuštanju zagađujućih materija i energije, klasifikaciji, karakteristikama i količinama otpada, kao i o drugim podacima i njihovo dostavljanje nadležnim organima;
- kontrolom aktivnosti i rada postrojenja koji mogu predstavljati rizik ili prouzrokovati opasnost po životnu sredinu i zdravlje ljudi, te drugim merama u skladu sa zakonom.[138]

134 Član 36. Zakona o zaštiti životne sredine.

135 *SRPSISO 14001:2015, Sistemi menadžmenta* životnom *sredinom — Zahtevi sa uputstvom za korišćenje.*

136 Član 44. Zakona o zaštiti životne sredine.

137 Član 104. Zakona o zaštiti životne sredine.

138 Primera radi, izmenama i dopunama *Zakona o javnim nabavkama* ("Službeni glasnik RS", br. 01/2019 i 92/2023) uređeno je da Kancelarija za javne nabavke propisuje vrste dobara, usluga i radova za koje su naručioci u obavezi da primenjuju ekološke aspekte prilikom određivanja tehničkih specifikacija, kriterijuma za izbor privrednog subjekta, kriterijuma za dodelu ugovora ili uslova za izvršenje ugovora o javnoj nabavci. Takođe, uređeno je da je naručilac

Kontinuitet poslovanja

Generalno gledano, planiranje kontinuiteta poslovanja predstavlja dizajniranje sa zadatkom obezbeđenja nastavka poslovnih procesa i operacija u privremenim ili eventualno stalnim hitnim situacijama i katastrofama. Plan kontinuiteta poslovanja svake organizacije treba da ima za cilj garantovanje nastavka kritičnih, ključnih poslovnih aktivnosti u hitnim, vanrednim situacijama i katastrofama, odnosno dovoljno brz povratak poslovanja kako bi se izbegao gubitak prihoda i očuvala reputacija.

Upravljanje kontinuitetom poslovanja je neophodno, pre svega, organizacijama koje predstavljaju kritičnu infrastrukturu, ali i svim drugim organizacijama od čije su usluge ili proizvoda zavisni drugi subjekti. Konačno, svakoj organizaciji (bez obzira da li pripada javnom ili privatnom sektoru, nezavisno od veličine ili delatnosti) u interesu je da omogući oporavak i nastavak aktivnosti na nivou koji se prethodno odredi, ne samo zarad očuvanja sopstvenog opstanka i ugleda, već i zbog sve značajnije društvene odgovornosti.

Poslednjih godina poslovi kontinuiteta poslovanja su se ustalili kao delokrug funkcije korporativne bezbednosti, posebno od kada je nacionalna komisija (*A292 - Bezbednost i otpornost*), odnosno komisija međunarodne organizacije za standardizaciju *ISO/TC 292 Security and resilience*, promenila naziv i pored bezbednosti svom delokrugu i imenu dodala otpornost, a u čijoj nadležnosti je donošenje određenih grupa standarda među kojima je i ona koja se odnosi na upravljanje kontinuitetom poslovanja.

Prema definiciji datoj međunarodnim standardom *ISO 22301*[139] koji se odnosi na zahteve u vezi sa sistemom upravljanja kontinuitetom poslovanja, kontinuitet poslovanja predstavlja

> *„sposobnost organizacije da tokom prekida/poremećaja nastavi sa isporukom proizvoda i usluga u unapred određenom kapacitetu i u okviru prihvatljivog vremenskog okvira".*

Da bi uspešno uspostavili sistem koji će omogućiti nastavak proizvodnje dobara ili pružanja usluga neophodno je preduzeti niz aktivnosti i postupaka, a elemen-

dužan da nabavlja dobra, usluge ili radoveodgovarajućeg kvaliteta, a imajući u vidu ne samo svrhu, namenu i vrednost javne nabavke, već i da predmet nabavke minimalno utiče na životnu sredinu.

139 *ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.*

tarnu fazu predstavlja identifikacija kritičnih poslovnih funkcija i procesa, tj. analiza uticaja na poslovanja (eng. *Business Impact Analysis - BIA*). Svaka organizacija mora da identifikuje koji su to glavni, kritični procesi od kojih zavisi njeno ukupno poslovanje (bez obzira na delatnost) i koji moraju biti posebno analizirani i tretirani. Pomoć prilikom uspostavljanja, primene i održavanja procesa analize uticaja na poslovanje, možemo potražiti i u smernicama koje su date u tehničkoj specifikaciji *SRPS ISO/TS 22317:2018, Društvena bezbednost – Sistem menadžmenta kontinuitetom poslovanja – Smernice za analizu uticaja na poslovanje (BIA)*[140].

Dalji redosled upravljanja sistemom kontinuitetom poslovanja (eng. *business continuity management system - BCMS*) okvirno sadrži:

- Identifikaciju pretnji i opasnosti, i definisanje scenarija koji bi ukazali na pravac odgovora na incidente u slučaju realizacije pretnji i opasnosti;
- Donošenje odluka top menadžmenta kojima se određuje koje funkcije, procesi ili aktivnosti moraju biti zaštićeni, od kojih pretnji i opasnosti, i to na osnovu procene rizika i analize očekivane koristi u odnosu na cenu koštanja (*cost–benefit analysis*);
- Identifikaciju i određivanje organizacionih, kadrovskih, tehničkih i drugih mera za postizanje očuvanja poslovanja, odnosno donošenje plana kontinuiteta poslovanja;
- Redovno preispitivanje celokupnog *BCMS* u cilju praćenja i razmatranja promena u procesima i pretnjama, održavanje i unapređenje.

Podaci koji se dobiju putem sprovedene *BIA* služe kao osnova za izbor najoptimalnije strategije oporavka koja će se primeniti u slučaju prekida poslovanja, a koja sadrži prioritete oporavka poslovnih procesa, ciljna vremena oporavka (eng. *recovery time objective - RTO*), ciljne tačke oporavka (eng. *recovery point objective - RPO*) i druge potrebne mere i radnje. Praktično posmatrano, utvrđivanje najdužeg prihvatljivog prekida (eng. *maximum acceptable outage - MAO*) pojedinačnih poslovnih procesa može biti mereno u minutima, satima, danima, pa i mesecima. Svaka organizacija mora za sopstvene potrebe da odredi potrebne mere i vremenske intervale, koji mogu biti i unapred određeni važećim smernicama i principima, kao što je, primera radi, slučaj sa organizacijama koje učestvuju u finansijskom tržištu i koje treba da se prdržavaju principa koje propisuju međunarodno priznate organiza-

140 Ovaj nacionalni standard je identičan sa međunarodnim *ISO/TS 22317:2015, Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA).*

cije iz te oblasti *Bank for International Settlements (BIS) i International Organization of Securities Commissions (IOSCO).*

Ti principi[141], pored ostalog, navode da finansijske organizacije treba da, u okviru uspostavljenog sistema upravljanja kontinuitetom poslovanja i plana za njegovu realizaciju, formiraju sekundarnu lokaciju u slučaju štetnih događaja širih razmera ili koji mogu izazvati velike poremećaje. Rezervna lokacija mora biti stavljena u operativnu upotrebu i treba da bude dizajnirana na način koji osigurava da kritični sistemi informaciono-komunikacionih tehnologija mogu da nastave sa radom u roku od dva sata od štetnog događaja. Čak šta više, principi navode da plan treba da bude dizajniran tako da omogući da organizacija može da sprovede usluge koje pruža do kraja dana kada je nastao prekid, čak i u slučaju ekstremno otežanih uslova rada.

Plan kontinuiteta poslovanja (eng. *Business Continuity Plan*) prema standardu *ISO 22301* predstavlja

> *„dokumentovane informacije koje usmeravaju organizaciju da odgovori na poremećaj i nastavi sa radom, da se oporavi i povrati isporuku proizvoda i usluga u skladu sa svojom ciljevima kontinuitet poslovanja*".

Sastavni delovi plana čine pojedinačni planovi - planovi organizacionih celina korporacije sa kritičnim poslovnim funkcijama, koji moraju biti sinhronizovani sa krovnim planom kontinuiteta poslovanja korporacije. Pojedine organizacije imaju zakonsku obavezu posedovanja plana kontinuiteta poslovanja, kao na primer banke i druge finansijske institucije koje su shodno *Odluci o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*[142] dužne da donesu plan kontinuiteta poslovanja, ali i plan oporavka aktivnosti u slučaju katastrofa (eng. *Disaster Recovery Plan*) kojim se prevashodno uređuje stvaranje uslova za oporavak i raspoloživost resursa informaciono-komunikacionih sistema potrebnih za odvijanje kritičnih poslovnih procesa.

U sklopu planiranja kontinuiteta poslovanja neophodno je preduzeti organizacione i tehničke mere koje će da garantuju adekvatan odziv i automatski nastavak poslovanja u okviru strategije upravljanja incidentima i kriznom situacijom. Ali pošto je nemoguće da se zaštitimo od svih mogućih pretnji, određeni rezidualni rizici moraju biti prihvaćen, što je u nadležnosti i mora da bude odobreno od strane top menadžmenta. Inače, kada su u pitanju poslovi upravljanja kontinuitetom poslova-

141 *Principles for financial market infrastructures*, BIS and IOSCO, Basel CH-Madrid ES, 2012.

142 "Službeni glasnik RS", br. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 i 100/2023 - dr. odluka.

nja preko je potrebno unapred odrediti uloge i odgovornosti, gde je za određivanje *BCMS* strategije odgovoran top menadžment, a za njeno sprovođenje, počevši od analize uticaja na poslovanje, do sprovođenja metodologije i izveštavanja, po pravilu zadužena funkcija korporativne bezbednosti. Sve druge organizacione celine korporacije dužne su da razrađuju i primenjuju sopstvene planove kontinuiteta poslovanja i izveštavaju sektor korporativne bezbednosti o statusu implementacije i nastalim promenama. Još jedna od neophodnih radnji u planiranju kontinuiteta poslovanja jeste realizacija obuke i sprovođenje redovnog parcijalnog i celovitog testiranja i vežbi kako bi planirani odgovor na prekid bio što realniji, pravovremen i adekvatan.

Pored postojanja adekvatnog plana odgovora na incidente kao obaveznog elementa planiranja kontinuiteta poslovanja, svi ostali planovi u okviru sistema korporativne bezbednosti (propisani zakonom ili predviđeni različitim smernicama i standardima), a koji su u funkciji odgovora i oporavka od nepredviđenih događaja i iznenadnih, hitnih situacija, prestavljaju nedeljiv i sastavni deo plana kontinuiteta poslovanja. Obaveza bezbednosnog menadžmenta je da izvrši njihovu inkorporaciju i sinhronizaciju širom organizacije, jer samo na takav način možemo dobiti jedinstven sistem upravljanja korporativnom bezbednošću koji će omogućiti visok nivo zaštite i otpornosti organizacije na raznovrsne pretnje i opasnosti.

Jedna od osetljivijih elemenata planiranja kontinuiteta poslovanja je obezbeđivanje ostvarenja adekvatne komunikacije za potrebe kritičnih procesa, uključujući i komunikaciju u okviru tima za sprovođenje plana i tima za upravljanje krizama, što se najefikasnije obezbeđuje putem dodatne komunikacione infrastrukture i usluga, kao i kroz obezbeđenje rezervnih/*backup* rešenja. *BCMS* nije tehnički standard, ni IT proces, ali s obzirom da se današnje poslovanje za većinu delatnosti umnogome oslanja na informaciono-komunikacione tehnologije, upravljanje kontinuitetom servisa IKT sistema mora da bude podrška i nezaobilazni proces upravljanja kontinuitetom poslovanja, i u tom smislu potrebno je stvarati rezervne kopije podataka, formiranje rezervnih centara za prikupljanje podataka, kao i obezbeđivanja dodatne infrastrukture, napajanja, mreže i drugih elemenata IKT sistema potrebnih za ostvarenje kontinuiteta. Takođe, mora se uspostaviti ugovorni odnos sa isporučiocima različitih usluga o očekivanom nivou usluga prilikom incidenta i drugih prekida, kao i obezbeđenje redudanse za eksterne dobavljače/provajdere, a u zavisnosti od delatnosti i procene rizika i potpuno opremljene rezervnei DR (eng. *Data Recovery*) lokacije.

U ostvarenju komunikacije neophodno je omogućiti i kontinuitet protoka informacija i to na bezbedan način, što predstavlja i deo zahteva spektra standarda koji se odnose na bezbednost informacija. U okviru njih kontinuitet poslovanja ima za cilj da omogući neophodni menadžment bezbednošću informacija u nepovoljnim, poremećenim situacijama, ali takođe, mora biti ugrađen u celokupan *BCMS* organizacije. Standardi *ISO/IEC 27001*i *ISO/IEC 27002* sadrže zahteve i kontrole koji se odnose na kontinuitet poslovanja, a *SRPS ISO/IEC 27031*[143] daje smernice najbolje prakse kako bi se obezbedio kontinuitet poslovanja za informacione i komunikacione tehnologije.

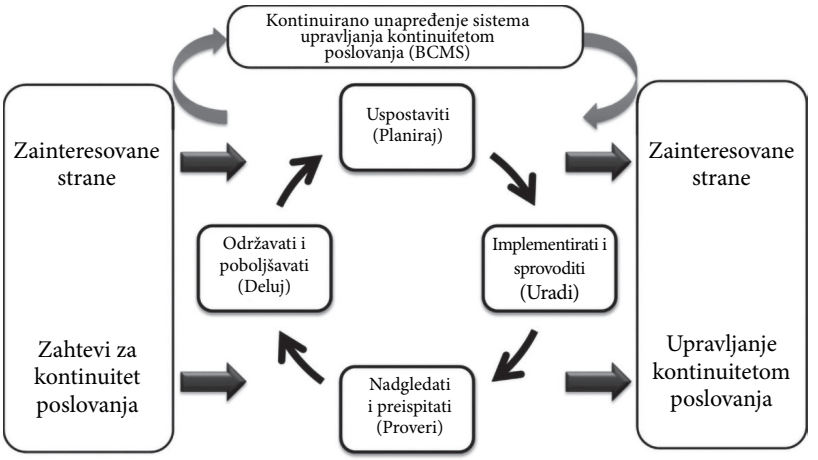
Kao i kod drugih sistema upravljanja, životni ciklusa *BCMS* mora da se redovno, ali i vanredno proverava, analizira i preispituje, kako od strane zaposlenih odgovornih za njegovo sprovođenje, tako i od funkcije interne revizije, kao i od strane nezavisnih spoljnih revizora, odnosno nadležnih državnih organa kada su u pitanju zakonom određene aktivnosti koje utiču na nastavak poslovanja (plan zaštite i spašavanja, bezbednosni plan operatora za upravljanje rizikom, plan obezbeđenja itd.).

Ovakav način upravljanja sistemom kontinuiteta poslovanja, pored ostalog, zadovoljava elementarni zahtev svih standarda sistema menadžmentom – procesni pristup zasnovan na modelu *Plan-Do-Check-Act (PDCA)*. Navedeni model Planiraj-Uradi-Proveri-Deluj primenjen na *BCMS* procese slikovito je prikazan na Slici 2.5.

Politika kontinuiteta poslovanja, procena rizika, planovi i drugi elementi *BCMS* moraju biti sinhronizovani i integrisani, pre svega, sa drugim bezbednosnim politikama, planovima, procenama, merama i kontrolama, a onda i sa drugim (nebezbednosnim) sistemima upravljanja koji su zastupljeni u korporaciji.

Ovako uređen sistem *BCM* je garant obezbeđenja nastavka ciljanog poslovanja, ali, ukoliko je to potrebno, i dobijanja sertifikata o ispunjenosti zahteva standarda koji izdaje akreditovano sertifikaciono telo. Posedovanje navedenog sertifikata nije zakonska obaveza, ali je svakako poželjna, pa i neophodna opcija organizacijama koje pružaju određene usluge ili proizvode dobra, kako bi mogli da dokažu da njihov sistem može da odgovori izazovima nepredviđenih prekida u poslovanju, a ujedno im omogućuje učestvovanje na domaćim i međunarodnim tenderima, odnosno ostvarivanje konkurentske prednosti.

143 *SRPS ISO/IEC 27031:2013, Informacione tehnologije — Tehnike bezbednosti — Smernice za spremnost informacionih i komunikacionih tehnologija za kontinuitet poslovanja.*



Slika 2.5. - PDCA model primenjen na BCMS procese[144]

Svakako da je preporučljivo da zaposleni koji obavljaju poslove iz domena upravljanja kontinuitetom poslovanja poseduju posebne veštine i znanja iz te oblasti, što mogu da dokažu i posedovanjem određenih sertifikata izdatih od priznatih međunarodnih organizacija, kao što su primera radi *Business Continuity Certified Planner, Business Continuity Certified Expert, Certified Business Continuity Professional* i drugi.

Krizni menadžment

U prethodnom izlaganju obrađeno je upravljanje kontinuitetom poslovanja koje je prevashodno proaktivnog karaktera, a koje se nadovezuje i veoma je blisko sa upravljanjem krizama kao poslovima pretežno reaktivne prirode.

Generalno gledano, kriza (eng. *crisis*) označava svaki neobičan događaj koji ima značajan negativan uticaj na život i zdravlje zaposlenih i drugih lica, na nastavak ostvarenja zadataka i ciljeva, kao i štetan uticaj na integritet i ugled korporacije.

> *„Za organizaciju je kriza okruženje u kojem ne može normalno da deluje. Kriza ugrožava sposobnost preživljavanja organizacije, onemogućava ostvarivanje ciljeva, pa ponekad i sam opstanak organizacije. Čak i kad kriza na prvi pogled*

144 Prikazani model je predviđen međunarodnim standardom *ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*, odakle je i preuzeta slika.

> *nema tako dramatične razmere, njen negativni uticaj na dobrobit organizacije često je tako veliki da ona ne bi mogla dugo opstati. Kriza ne utiče negativno samo na javni lik preduzeća ili organizacije. Ona takođe utiče na njenu sposobnost daljeg normalnog delovanja, na njene temelje i takođe na lični imidž vodećih menadžera."*[145]

Svaka kriza predstavlja jedinstven izazov, a njen pravac kretanja je veoma dinamičan i obično nepredvidiv, te stoga ne mogu postojati posebni operativni planovi, ali svakako mora postojati adekvatan odgovor, odnosno sistem upravljanja krizama. Kao i u slučaju poslova kontinuiteta poslovanja, a zbog negativnog uticaja koji kriza može da ima na organizaciju i gde upravljanje njome može da doprinese otpornosti korporacije, rukovođenje sistemom kriznog menadžmenta se sve više poverava funkciji korporativne bezbednosti, kao organizacionoj celini odgovornoj za organizovanje svih aktivnosti u vezi obezbeđenja spremnosti korporacije na nepredviđeno. Upravo ta neočekivanost sa nespremnošću i vremenskim pritiskom predstavljaju tri karakteristike zajedničke za sve krize.

Iako ne postoji univerzalna definicija krize, koja zavisi od discipline u kojoj se koristi, za potrebe ovog Priručnika možemo koristiti onu koja je datau smernicama međunarodne organizacije profesionalaca bezbednosti *ASIS International (American Society for Industrial Security*), gde navode da je kriza „bilo koji globalni, regionalni ili lokalnidogađaj izazvan prirodnim ili ljudskim delovanjem, ili poslovni prekid koji prouzrokuje rizik od

(1) eskalacije intenziteta,

(2) negativnog uticaja na vrednosti po akcionare ili na finansijsku poziciju organizacije,

(3) nanošenja štete ljudima, imovini ili životnoj sredini,

(4) potpadanja u sferu posebnog interesovanja medija ili nadležnih državnih organa,

(5), ometanja normalnog rada i gubljenja značajnog vremena na upravljanje i/ili finansijskih sredstava,

(6) negativnog uticaja na moral zaposlenih, ili

145 Keković Zoran, Kešetović Želimir, *Krizni menadžment I, Prevencija krize*, Univerzitet u Beogradu, Fakultet bezbednosti, 2006., str. 27.

(7) ugrožavanja reputacije organizacije, proizvoda, ili njenih predstavnika, a samim tim negativnog uticaja na njenu budućnost".[146]

Iz ovako date definicije možemo videti svu kompleksnost krize čiji uzročnici mogu biti i internog i eksternog karaktera, prouzrokovani različitim događajima, od opšte promene na tržištu ili prekida isporuka usluga u dužem periodu (električne energije, telekomunikacionih i drugih usluga) do požara, poplava ili drugih elementarnih nepogoda ili tehničko-tehnoloških nesreća ili katastrofa, terorističkih napada, epidemija, sajber ili medijskih napada, kao i realizacijom mnogih drugih pretnji i opasnosti kao što su razbojništvo, otmica, štrajk, ulični neredi itd.

Zbog svega navedenog neophodno je upravljati krizom, što je različito i nije namenjeno za upravljanje vanrednim situacijama ili kao odgovor na incidente, niti obuhvata menadžment kontinuitetom poslovanja - to zahteva primenu operativnih planova i radnih procedura, dok se upravljanje kriznim situacijama zasniva na prilagođenom, brzo donetom, fleksibilnom strateškom odgovoru. Kako je određeno standardom *ISO 22300* krizni menadžment predstavlja

> *„holistički proces upravljanja koji identifikuje potencijalne uticaje koji prete organizaciji i pruža okvir za izgradnju otpornosti, sa mogućnošću efikasnog odgovora u cilju zaštite interesa ključnih zainteresovanih strana organizacije, reputacije, brenda i aktivnosti koje kreiraju vrednosti, kao i za efikasno obnavljanje operativnih sposobnosti".*[147]

Upravljanje krizom, kao krajnja odgovornost top menadžmenta, neophodno je da ima svoje timove, gde je potrebno da centralni tim bude sastavljen od generalnog menadžera, menadžera za korporativnu bezbednost i drugih menadžera najvišeg nivoa upravljanja i odlučivanja, i koji moraju da se fokusiraju na brze analize i odluke, pravovremenu komunikaciju i koordinaciju sa drugim kriznim timovima i ostalim timovima za nepredviđene situacije, kao što je tim za odgovor na incidente, tim za sprovođenje plana kontinuiteta poslovanja, tim za zaštitu i spasavanje i drugim timovima, ali i sa nadležnim državnim organima i ostalim učesnicima u rešavanju krize. Primarna, odnosno sekundarna mesta okupljanja timova moraju bitu unapred planirana i određena, kao i opremljenost tih prostora svim neophodnim sredstvima i uređajima, od informaciono-komunikacione opreme i predviđenog rezer-

146 *Business Continuity Guideline - A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*, GDL BC 01, ASIS, Alexandria VA 2005, p. 7.

147 *ISO 22300:2021, Security and resilience – Vocabulary,* 3.60.

vnog energetskog napajanja do opreme za odmor, održavanja higijene i predviđene ishrane članova timova za mogući dvadeset četvoročasovni i višednevni boravak.

Koncept kriznog menadžmenta mora da obuhvati celovitu organizacionu strukturu, uloge i odgovornosti, procedure, sve elemente krizne komunikacije, potrebnu dokumentaciju, edukaciju i druge neophodne elemente, dok interni priručnici kao smernice za krizno upravljanje moraju sadržati detaljne kontakt podatke, planove lokacija, potrebne ček liste i templejde kako bi odgovor mogao da zadovolji izuzetno dinamičan i kompleksan događaj kakva je kriza sa svim svojim brojnim varijablama i parametrima. Krizna komunikacija je izuzetno osetljiv segment kriznog upravljanja, pa je potrebno unapred odrediti odgovornosti, način i tokove interne i eksterne komunikacije, naročito one koje se odnose na medije i javnost (obratiti pažnju na sve značajniji uticaj društvenih mreža). Ne sme se zanemariti činjenica da svaka kriza znači ogroman mentalni stres za one koji učestvuju u njenom rešavanju, a takođe predstavlja kompleksan problem koji treba rešiti u isto vreme, iz kog razloga je potrebno posebno obratiti pažnju na obuku svih učesnika u upravljanju krizama kako bi stekli izvesnu otpornost na stres i samouverenost, i bili sposobni da adekvatno odreaguju i donose optimalne odluke, razumevajući njihove efekte koje mogu imati ne samo finansijske i reputacione posledice po organizaciju, već mogu direktno ili indirektno uticati i na živote zaposlenih i drugih lica[148].

Za rešavanje kriznih situacija sa strateškog nivoa od pomoći može biti primena nacionalnog standarda[149] iz oblasti upravljanja krizama, a koji je u vezi, odnosno identičan je sa međunarodnim standardom *ISO 22361:2022, Security and resilience — Crisis management — Guidelines*, i koji olakšava svakoj organizaciji, bez obzira na njenu veličinu ili vrstu delatnosti koju obavlja, razvijanje sposobnosti upravljanja krizom. Ono što je bitno naglasiti jeste da kapaciteti upravljanja krizom ne predstavljaju deo normalnog, rutinskog upravljanja organizacijom, te da je s toga potrebno uložiti dodatni napor za svesno i ciljano izgrađivanje, održavanje i unapređivanje materijalnih, kadrovskih, organizacionih i drugih resursa i investicija kako bi korporacija spremno dočekala nastanak krize. Posebno je potrebno voditi računa o prepoznavanju kompleksnosti obaveza kriznih timova, čije delovanje umnogome zavise od uspešno ostvarene komunikacije tokom trajanja krizne situacije, kao i od uvežbanosti i obučenosti, odnosno razmatranja i izvlačenja „pouka“ od prethodnih kriza koje su se dogodile u sopstvenoj korporaciji ili drugoj organizaciji koja se bavi istom ili sličnom delatnošću. U nedostatku takvih iskustava, za edukaciju članova timova

148 *BSI Standard 100-4: Business Continuity Management*, Version 1.0, London UK, 2009., pp. 78 - 83.

149 *SRPSENISO 22361:2023, Bezbednost i otpornost – Krizni menadžment – Smernice.*

za upravljanje krizama mogu se posmatrati i analizirati krize koje su realizovane u različitim pravnim licima na teritoriji RS, regiona ili šire, od kojih su mnogi primeri bili značajno propraćeni u sredstvima javnog informisanja.

Zaštita kritične infrastrukture

Iako Zakon o kritičnoj infrastrukturi (koji je stupio na snagu 2018. godine) predviđa identifikaciju, određivanje i zaštitu kritične infrastrukture(KI), a što je navedeno i u Strategiji nacionalne bezbednosti Republike Srbije kao najvišem strateškom dokumentu, postupak utvrđivanja sistema, mreža, objekata ili njihovih delova u određenom sektoru još nije realizovan. Imajući to u vidu, funkcija korporativne bezbednosti budućih operatora kritične infrastrukture mora percipirati predstojeće poslove zaštite tih sistema, mreža, objekata ili njihovih delova kao skup aktivnosti i mera koje shodno zakonu imaju za cilj

> *„osiguranje funkcionisanja kritične infrastrukture u slučaju ometanja ili uništenja, odnosno zaštitu u slučaju pretnji i sprečavanje nastanka posledice ometanja ili uništenja".*[150]

Nesporno je da će operatori kritične infrastrukture (bez obzira da li si uz redova državnih organa, organa autonomne pokrajine, organa jedinice lokalne samouprave, javnih preduzeća, privrednih društava ili drugih pravnih lica koja upravljaju sistemima, mrežama, objektima ili njihovim delovima koji će biti određeni kao kritična infrastruktura) biti iz sledećih sektora: energetika; saobraćaj; snabdevanje vodom i hranom; zdravstvo; finansije; telekomunikacione i informacione tehnologije; zaštita životne sredine; funkcionisanje državnih organa[151]. Takođe, osim prethodno navedenih sektora, kritična infrastruktura može biti određena i u drugim sektorima, a na osnovu predloga ministarstva nadležnog za određenu oblast. Imajući u vidu ovako široku lepezu oblasti, može se očekivati da će veliki broj organizacija (bez obzira da li pripada javnom ili privatnom sektoru) imati obavezu implementacije zaštitnih mera propisanih zakonom, kao i očekivanim podzakonskim aktima. Zbog prednosti i benefita koji sa sobom nosi holistički pristup u proceni bezbednosnih rizika i primeni mera za tretman rizika, potrebno je imati u vidu da su i *Zakonom*

150 Član 2. tačka 4. *Zakona o kritičnoj infrastrukturi* ("Službeni glasnik RS", br. 87/2018).

151 Određeno članom 4. *Uredbe o kriterijumima za identifikaciju kritične infrastrukture i načinu izveštavanja o kritičnoj infrastrukturi Republike Srbije* ("Službeni glasnik RS", br. 69/2022).

o informacionoj bezbednosti prepoznate određene delatnosti[152] od opšteg interesa u kojima se koriste IKT sistemi od posebnog značaja, i to u oblastima koji se faktički podudaraju sa sektorima u kojima se vrši identifikacija i određivanje kritične infrastrukture shodno zakonu kojim se uređuje zaštita *KI*. Takođe, možemo reći da su isti sektori, odnosno delatnosti (energetika, saobraćaj, zdravstvo, finansije i dr.) prepoznati kao kritična infrastruktura i prema *Zakonu o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama*, pa subjekti koji imaju sisteme, mreže, objekte ili njihove delove, čiji prekid funkcionisanja ili prekid isporuke roba, odnosno usluga može imati ozbiljne posledice na nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje RS, imaju obavezu izrade procene rizika od katastrofa i planova zaštite i spasavanja, kojim planiraju mere i aktivnosti u cilju zaštite i spasavanja zaposlenih i drugih lica, materijalnih dobara i obezbeđenja osnovnih uslova za život i dalje poslovanje. Sveobuhvatna analiza rizika i primena mera za smanjenje rizika potrebna je i pri neophodnoj zaštiti obavezno obezbeđenih objekata shodno *Zakonu o privatnom obezbeđenju*, koja se obavlja kao poslovna funkcija pravnog lica kome pripadaju objekti od strateškog značaja za RS i njene građane, kao i objekti od posebnog značaja čijim oštećenjem ili uništenjem bi mogle nastupiti teže posledice po život i zdravlje ljudi ili koji su od interesa za odbranu zemlje.

Ključne aktivnosti za uspešno funkcionisanje *KI* jesu i poslovi koji se sprovode sa ciljem njene zaštite. Pri utvrđivanju potreba za zaštitu *KI* potrebno je imati u vidu njen značaj, moguće oblike, izvore i nosioce ugrožavanja, posledice koje mogu nastati za određeni sektor, kao i međusektorski uticaj. Zbog ovako složenog uticaja različitih faktora neophodna je adekvatna analiza posledica, kao i preduzimanje mera i aktivnosti na sprečavanju ugrožavanja ili ublažavanju posledica pretnji i opasnosti, kao i mera za brz oporavak i nastavak funkcionisanja *KI*. U tom smislu, procena rizika i mere zaštite *KI* predstavljaju veoma složene i izazovne radnje koje zahtevaju stručna znanja iz različitih oblasti, multidisciplinarni pristup, kao i implementaciju raznovrsnih preventivnih, proaktivnih i reaktivnih, interventnih mera i kontrola.

Operator kritične infrastrukture je dužan da shodno zakonu izradi bezbednosni plan za upravljanje rizikom, kojim se definišu bezbednosni ciljevi i mere operatora na osnovu analize rizika. Tim planom je potrebno utvrditi mere za smanjenje rizika, definisati odgovornosti i odrediti dužnosti, kao i uspostaviti okvir za postupanje

152 Lista delatnosti je utvrđena *Uredbom o utvrđivanju Liste delatnosti u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja* („Službeni glasnik RS“, br. 94/2019).

u cilju otklanjanja, odnosno smanjenja posledica bezbednosnih pretnji. Pozitivan doprinos je i taj što su operatori kritične infrastrukture dužni da na izrađeni bezbednosni plan za upravljanje rizikom dobiju saglasnost MUP-a, sa kojim kontaktiraju putem licenciranog oficira za vezu i koji je odgovoran za obezbeđenje stalne kontrole rizika i pretnji, obaveštavanje o promenama u odnosu na kritičnu infrastrukturu, kao i za druge poslove vezane za zaštitu kritične infrastrukture.

Do donošenja zvanične domaće metodologije za procenu rizika u zaštiti kritične infrastrukture od koristi može biti i analiza iz studije[153] slovenačkog Instituta za studije korporativne bezbednosti (*ICS Institut*), čiji rezultat ukazuje na primenu kombinacije metodologija *MOSAR (Method organised systematic analysis of risk)* i *FMEA (Failure mode and effect analysis)* kao najpogodnije prilikom proceni rizika *KI*. U svakom slučaju, kritični subjekti kao pružaoci osnovnih usluga koji imaju nezamenljivu ulogu u održavanju vitalnih društvenih funkcija ili ekonomskih aktivnosti, moraju ne samo da se zaštite, već, kako je navedeno u novoj tzv. *CER* direktivi EU kojom se uređuju mere u cilju postizanja visokog nivoa otpornosti kritičnih subjekata *(Directive (EU) 2022/2557)*, treba da budu u poziciji da ojačaju svoju sposobnost da spreče, reaguju, da se odupru, ublaže, apsorbuju, prilagode i oporave od incidenata koji imaju potencijal da poremete pružanje osnovnih usluga.

Koncept *Zakona o kritičnoj infrastrukturi Republike Srbije* se u znatnoj meri oslanja na Direktivu Evropskog saveta *2008/114/EC*[154] iz 2008. godine. Evaluacijom te Direktive sprovedenom 2019. godine utvrđeno je da je kontekst u kome KI funkcioniše znatno promenjen od njenog stupanja na snagu. S obzirom na promene i razvoj u sferi tehnologije, ekonomije, društva, politike i okruženja, koji uzrokuju nove i evoluirajuće rizike, Direktiva je tek delimično relevantna. Zaključak je da je nužno preusmeriti pristup EU na obezbeđenje većeg uvažavanja rizika, boljeg definisanja i koherentnosti uloge i obaveza kritičnih subjekata kao pružalaca ključnih usluga, te na donošenje pravila EU za jačanje njihove otpornosti. Kako je tzv. *CER* direktivom (usvojenom 14. decembra 2022. godine) stavljana van snage Direktiva *2008/114/ES*[155], očekuje se da će države članice i zemlje kandidati za pridruživanje EU unaprediti postojeći koncept zaštite *KI*, u smislu prelaska sa mera zaštite poje-

153 Čaleta Denis, Vršec Milan, Bertoncelj Brane, Vršec Miran, Kandžič Aljoša, Podgoršek Žiga, Študija *"Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture"*, ICS Institut, Ljubljana, 2019.

154 *OJ L 345*, 23.12.2008, pp. 75–82.

155 Države članice su dužne da do 17. oktobra 2024. godine donesu i objave potrebne mere za usklađivanje sa tzv. *CER* direktivom i da o tome obaveštavaju Komisiju. Te mere se primenjuju od 18. oktobra 2024. godine, kada se Direktiva 2008/114/EC stavlja van snage.

dinačne kritične imovine na preventivni pristup koji je zasnovan na proceni rizika i fokusiran na jačanje otpornosti kritičnih subjekata i sposobnosti pružanja usluga.

Iako se rok do oktobra 2024. godine koji je dat u tzv. *CER* direktivi odnosi na članice EU, nesumnjivo je da će i za RS proisticati određene obaveze koje će biti vezane za Poglavlje 24 pregovaračkog procesa o pridruživanju EU. Za RS je situacija na tom planu unekoliko komplikovanija jer se radi o daljem usklađivanju nacionalnog zakonodavstva sa evropskim standardima, a da ni važeći *Zakon o kritičnoj infrastrukturi* još uvek nije u primeni.

Nadajmo se da će nadležni državni organi RS, po uzoru na razvijene zemlje EU, ubrzo nakon identifikacije i određivanja kritične infrastrukture, raditi i na izgradnji raznovrsnih platformi za podršku i pomoć subjektima u njihovim aktivnostima vezanim za poslove zaštite. Kao primer dobre prakse možemo navesti internet platformu *UP KRITIS*[156] razvijenu od strane nadležnih nemačkih organa, a namenjenu podršci i asistenciji njihovim subjektima KI u okviru javno-privatnog partnerstva.

Fizička bezbednost

Osnovni oblik ostvarivanja bezbednosti organizacije jeste fizička bezbednost (eng. *physical security*), koja prema domaćoj terminologiji i pravnoj regulativi podrazumeva fizičko-tehničku zaštitu, i shodno *Zakonu o privatnom obezbeđenju* definiše se kao

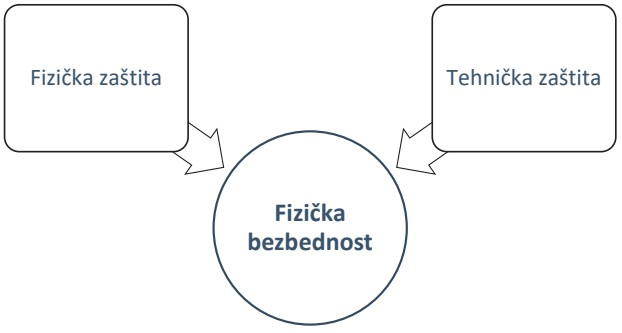
> *„obezbeđenje lica i imovine primenom fizičke zaštite i korišćenjem sredstava tehničke zaštite“.*[157]

Ovako određene poslove obezbeđenja mogu vršiti samo pravna lica (uključujući i ona koja su obrazovala unutrašnji oblik organizovanja obezbeđenja za sopstvene potrebe - samozaštitna delatnost) i preduzetnici koji ispunjavaju zakonom propisane uslove i poseduju adekvatnu vrstu licence. Fizička bezbednost, pored ostalog, ima za cilj: onemogućavanje neovlašćenog pristupa objektu; signaliziranje neovlašćenog ulaska u štićeni prostor i dojavu; onemogućavanje unošenja u objekat oružja, eksplozivnih, radioaktivnih, bioloških i drugih opasnih predmeta i materija;

156 Platforma je izrađena shodno nemačkoj *Nacionalnoj strategiji za zaštitu kritične infrastrukture*, sa ciljem razmene iskustava i koordinacije, analize pretnji i incidenata, sprovođenja vežbi, razvijanja komunikacionih struktura i drugo, a u skladu je sa Evropskim programom zaštite kritične infrastrukture.

157 Član 3. tačka 21. *Zakona o privatnom obezbeđenju*.

zaštitu vrednosti pomoću sistema elektrohemijske i drugih načina zaštite (koferi, kontejneri, kase, trezori i dr.); vršenje radnji usmerenih na sprečavanje krivičnih dela i drugih identifikovanih rizika; praćenje kretanja oko i u štićenom prostoru i pojedinačno štićenim prostorijama; kontrolu sprovođenja propisanih mera zaštite i unutrašnjeg reda u objektu i delovima pod posebnim režimom. Navedenim radnjama fizičko-tehničke zaštite prethode poslovi procene rizika (analize i ocene rizika u zaštiti lica, imovine i poslovanja) i planiranja, dok značajan izazov menadžmenta predstavlja uspostavljanje, održavanje i poboljšanje kvaliteta i funkcionalnosti svih navedenih aktivnosti.



Slika 2.6. Fizička bezbednost

Poslovi i nosioci fizičke bezbednosti, odnosno pravna lica, preduzetnici i fizička lica koja vrše poslove privatnog obezbeđenja (uključujući i samozaštitnu delatnost) bitni su ne samo za bezbednost korporacija i drugih organizacija iz javnog i privatnog sektora, već imaju i nacionalni značaj, s obzirom da su Strategijom nacionalne bezbednosti Republike Srbije ti poslovi uvršteni u sistem unutrašnje bezbednosti kao elementa izvršnog dela sistema nacionalne bezbednosti.

Fizička zaštita

Prema *Zakonu o privatnom obezbeđenju* fizička zaštita je

> *„usluga obezbeđenja koja se pruža prvenstveno ličnim prisustvom i neposrednom aktivnošću službenika obezbeđenja u određenom prostoru i vremenu u skladu sa planom obezbeđenja, primenom mera i ovlašćenja službenika obezbeđenja".*[158]

158 Član 3. tačka 20. *Zakona o privatnom obezbeđenju*.

Fizička zaštita se u našem zakonodavstvu pojavljuje i pod pojmom telesna zaštita, kao što je navedeno (ali ne i definisano) u *Zakonu o igrama na sreću*[159], prema kome je priređivač dužan da obezbedi telesnu zaštitu igračima i posetiocima u igračnici. U svakom slučaju, poslove fizičke/telesne zaštite lica (uključujući i lično obezbeđenje i redarsku službu), imovine (samo unutar štićenog objekta ili do granice štićenog prostora, uključujući patrolnu intervenciju i poslove pratnje i obezbeđenja transporta i prenosa novca, vrednosnih i drugih pošiljaka) i poslovanja može vršiti samo službenik obezbeđenja (eng. *security officer/security guard*)[160] koji u skladu sa zakonom poseduje licencu za fizička lica izdatu od strane MUP-a, a dužan je prilikom vršenja poslova kod sebe imati i legitimaciju, osim ako je angažovan kao redar na javnom okupljanju. Samo službenici obezbeđenja koji poseduju važeću *Licencu za vršenje specijalističkih poslova službenika obezbeđenja – sa oružjem*, mogu nositi vatreno oružje, i to poluautomatski pištolj kalibra 7,65 mm i 9 mm, a samo u uslovima ratnog i vanrednog stanja i dugo oružje isključivo za potrebe zaštite obavezno obezbeđenih objekata. Pored propisane uniforme (ili građanskog odela u slučaju ličnog obezbeđenja), službenik obezbeđenja mora prilikom nošenje vatrenog oružja posedovati nalog za nošenje službenog oružja, a kod sebe ne sme imati lično oružje.

U skladu sa procenama, potrebama i drugim zahtevima korporacija može da ima organizovan sopstveni oblik fizičke zaštite (samozaštitna delatnost), angažovani (putem ugovornog odnosa) ili kombinovani. Uz postojanje i zatečenog – zajedničkog organizacionog oblika fizičke zaštite, kao specifičnog, obično nametnutog i uslovljenog deljenjem većih poslovnih objekata od strane više različitih pravnih lica, pri opredeljenju za neki od oblika fizičke zaštite neophodno je preispitati i analizirati sve prednosti i nedostatke, dobre i loše strane[161].

Kao i u slučaju ostalih poslova privatnog obezbeđenja, usluga fizičke zaštite može se vršiti samo na osnovu i u okviru zaključenog pisanog ugovora, koji mora sadržati sve potrebne elemente (predmet ugovora, način vršenja ugovorenih poslova i dr.). Podrazumeva se da se ugovorom ne može odrediti manji nivo usluga obezbeđenja od onih koji su predviđeni aktom o proceni rizika u zaštiti lica, imovine i

159 "Službeni glasnik RS", br. 18/2020.

160 O definiciji službenika obezbeđenja i drugim aspektima industrije privatnog obezbeđenja pogledati više u: Spaninks Louis, Quinn Larry, Byrne John, *European Vocational Training Manual For Basic Guarding*, Leonardo NL/96/2/1136/PI/II.1.1.b/FPC, Brussels, 1999. Termin službenika obezbeđenja je određen i evropskim standardom *EN 15602:2022, Private security services – Terminology*, CEN-CENELEC, Brussels 2022.

161 O organizacionim oblicima, ovlašćenjima i drugim poslovima fizičke zaštite više pogledati: Mandić J. Goran, *Osnovi sistema obezbeđenja pravnih lica*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2012., str. 143 - 196.

poslovanja, a koja se vrši po zahtevima i na način propisan važećim srpskim standardom u oblasti privatnog obezbeđenja - *SRPS A.L2.003*. Shodno poznatoj problematici kvaliteta pružanja ovih usluga, pomoć u odabiru i dobijanju najbolje tržišne ponude možemo potražiti i u evropskom priručniku za organizacije koje dodeljuju ugovore za usluge obezbeđenja[162].

Zbog sada već hroničnih problema[163] u industriji privatnog obezbeđenja (nedostatak kadrova, upitnost kvaliteta, neusklađenost rada sa zakonom, niske zarade i dr.), neophodno je da organizacija, bez obzira da li ima sopstveno, angažovano ili kombinovano obezbeđenje, stalno vrši nadzor nad obavljanjem poslova, kao i da preduzima mere u cilju povećanja kvaliteta. U tom pogledu, od pomoći može biti korišćenje standarda kao vidova uobličene i sistematizovane najbolje prakse, a najpre možemo izdvojiti srpski standard *SRPS A.L2.002*[164] kojim se utvrđuju zahtevi za usluge privatnog obezbeđenja, i čije korišćenje može da pomogne prilikom uspostavljanja ili provere kvaliteta procesa kojima se pružaju i koriste usluge privatnog obezbeđenja. Ukoliko organizacija pripada kritičnoj infrastrukturi, za povećanje kvaliteta usluga privatnog obezbeđenja može da iskoristi i zahteve standarda *SRPS EN 17483-1:2021, Usluge privatnog obezbeđenja – Zaštita kritične infrastrukture – Deo 1: Opšti zahtevi*, koji može da pomogne u optimizaciji zaštite kroz prevenciju. Nedostatak radne snage i veština je identifikovan kao veoma značajan izazov u domenu poslova fizičke bezbednosti kako u regionu, tako i širom EU, koja je iz tih razloga pokrenula zajedničku platformu kroz projekat *INTEL*[165] sa ciljem omogućavanja zainteresovanim stranama iz industrije usluga privatnog obezbeđenja uspešnije razumevanje, predviđanje, pripremu i upravljanje nedostatkom radne snage i veština širom EU.

Iznova naglašavajući značaj kvaliteta u obavljanju poslova fizičke zaštite, ukazujemo na benefite redovnog sprovođenja različitih programa obuke i treninga službenika obezbeđenja. Pored zakonske obaveze sprovođenja kondicione obuke (vežbovna gađanja, borilačke veštinei dr.), važno je da organizacije podstiču razvoj

162 O definisanju zahteva, elementima tenderske dokumentacije i drugim elementima potrebnim za dobijanje što kvalitetnije usluge pogledati više u: *Buying quality private security services*, CoESS & UNI-Europa, Brussels, 2023.

163 O određenim problemima i izazovima u okviru industrije privatnog obezbeđenja pogledati više u: *Bela knjiga:predlozi za poboljšanje poslovnog okruženja u Srbiji*, Savet stranih investitora, Beograd 2022., str. 235 - 237.

164 *SRPS A.L2.002:2015, Društvena bezbednost — Usluge privatnog obezbeđenja — Zahtevi i uputstvo za ocenjivanje usaglašenosti.*

165 Više o projektu pogledati na https://www.securityskills.eu/, 08.11.2023.

programa treninga za različite nivoe obučenosti (osnovni, redovni, dodatni, specijalistički) i poslove koje obavljaju službenici obezbeđenja (za novozaposlene, za specifične zadatke, za određena radna mesta itd.), a koje je potrebno ažurno sprovoditi, kao i voditi adekvatnu evidenciju o istom. Dobar primer organizacije predmetnih programa treninga za službenike obezbeđenja može se pronaći u britanskom standardu *BS 7499*[166] koji predstavlja kodeks prakse, dajući preporuke o načinu pružanja usluge obezbeđenja na objektima i prilikom patroliranja.

Tehnička zaštita

Zakon o privatnom obezbeđenju definiše poslove tehničke zaštite kao

> *„obezbeđenje lica i imovine koje se vrši tehničkim sredstvima i uređajima, njihovim planiranjem, projektovanjem, ugradnjom i održavanjem“,*[167]

i to u cilju zaštite od nedozvoljenog pristupa u prostore i objekte, neovlašćenog iznošenja štićenih predmeta, nedozvoljenog unošenja opasnih i drugih predmeta i materija, provale i ostalih identifikovanih rizika. Način vršenja poslova i korišćenja tehničke zaštite bliže je propisan *Pravilnikom o načinu vršenja poslova tehničke zaštite i korišćenja tehničkih sredstava* [168], kojim su određena sledeća sredstva i uređaji tehničke zaštite: mehanička sredstva, elementi, uređaji ili konstrukcije; elektronska i elektro-mehanička sredstva i uređaji; protivdiverziona i protivsabotažna sredstva i uređaji; sredstva i uređaji za globalno pozicioniranje lica i pokretnih dobara.

Kao i prilikom izrade plana fizičke i fizičko-tehničke zaštite, za implementaciju mera iz akta o proceni rizika u zaštiti lica, imovine i poslovanja, posebnih zahteva organizacije (korisnika), kao i za određivanje elemenata sistema tehničke zaštite, potrebno je izraditi plan sistema tehničke zaštite (kao sastavnog dela plana obezbeđenja), i za tu svrhu pogodno je koristiti se tehničkim izveštajem *SRPS TR A.L2.003-5*[169]. Koncept planiranja treba da bude usklađen sa ciljevima vezanih za zaštitu imovine i poslovanja, ublažavanjem pretnji i sagledavanjem vrednosti sprečene štete. Posao planiranja prate radnje projektovanja, i na osnovu njih poslovi montaže, po-

166 O vrstama i predmetima treninga videti više u: *BS 7499:2013, Static site guarding and mobile patrol service – Code of practice*, The British Standards Institution, London UK 2013.

167 Član 3. tačka 22. *Zakona o privatnom obezbeđenju*.

168 "Službeni glasnik RS", br. 91/2019.

169 *SRPS TR A.L2.003-5:2020, Bezbednost i otpornost društva – Procena rizika – Deo 5: Uputstvo za izradu plana obezbeđenja.*

vezivanja i puštanja u rad sredstava, uređaja i sistema tehničke zaštite, uz obaveznu obuku korisnika, koji je dužan da obezbedi i stručni nadzor nad izvođenjem radova. Nakon obavljenog valjanog tehničkog prijema, praćenog propisanim obrascima (zapisnik o tehničkom prijemu i potvrda da je tehnička zaštita izvedena na propisan način), veoma je bitno da korisnik ugovorno obezbedi i održavanje i servisiranje sredstava, uređaja i sistema tehničke zaštite, što u praksi ponekad izostane i može da stvori problem prilikom eksploatacije.

Zbog značajne društvene opasnosti zakonodavac je za poslovne banke, javnog poštanskog operatora i druge finansijske organizacije, propisao minimalne tehničke uslove kod obavezne ugradnje sistema tehničke zaštite. Složićemo se da *Uredba o minimalnim tehničkim uslovima kod obavezne ugradnje sistema tehničke zaštite u bankama i drugim finansijskim organizacijama*[170] na dosta uopšten način utvrđuju minimalne tehničke uslove, a koji zavise od nivo rizika konstatovanog prilikom sprovođenja postupka procene rizika u zaštiti lica, imovine i poslovanja. Dobar primer detaljnijeg uređenja zaštite finansijskih organizacija pronalazimo u regionu, gde je Republika Hrvatska ne samo donela *Zakon o zaštiti novčarskih institucija*[171], već je u skladu s tim zakonom usvojilla i *Pravilnik o popisu normi i prihvaćenih pravila struke u primjeni zaštite novčarskih institucija*[172], u kojem su taksativno navedene hrvatske, međunarodne i specijalizovane norme i pravila struke koji se odnose na ispitivanje i klasifikaciju otpornosti na mehaničke i balističke prodore za elemente mehaničke zaštite (neprobojne pregrade, protivprovalna vrata, sigurnosne folije, trezore, sefove, kase, ormare, brave, cilindre i okove), te za primenu uređaja i sistema tehničke zaštite (videonadzor, protivprovalna i protivprepadna zaštita, kontrola pristupa) koji se koriste u zaštiti finansijskih organizacija.

Dobar primer domaćeg zakonskog uređenja funkcionalnosti pojedinih sredstava i uređaja tehničke zaštite možemo videti u oblasti video obezbeđenja[173] koje koriste organizacije koje su priređivači igara na sreću shodno *Zakonu o igrama na sreću*. U cilju zaštite i sprečavanja kršenja pravila igre, tim zakonom i podzakonskim aktom jasno su predviđene lokacije kamera, način čuvanja snimaka i druge bitne karakteristike sistema video obezbeđenja, sa posebnim naglaskom na kvalitet siste-

170 "Službeni glasnik RS", br. 9/2021.

171 „Narodne novine", br. 56/2015, 46/2021 i 114/2022.

172 „Narodne novine", br. 102/2016.

173 U domaćoj pravnoj regulativi (pa i u *Zakonu o privatnom obezbeđenju*) i stručnoj literaturi za pojam „video obezbeđenje" koristi se i termin „video nadzor", dok se u stranoj (englesko govorno područje) za ovaj pojam paralelno koriste termini „*video-surveillance*" i „*CCTV*" *(closed-circuit television).*

ma čime je zahtevano da vidno polje kamere mora biti tako izabrano da se obezbedi dovoljan broj piksela snimljenih lica u neposrednoj blizini lokacije, a u cilju njihove nedvosmislene identifikacije.

O sistemu video obezbeđenja u funkciji korporativne bezbednosti izdvojili bi istraživanje australijskog univerziteta Edith Cowan, u kojem taj sistem posmatraju sa dva nivoa. Prvi nivo se odnosi na sveobuhvatne ciljeve sistema video obezbeđenja, razmatrajući elementarna pitanja razloga postojanja sistema (osećaj sigurnosti, zaštita imovine i zakonski zahtevi). Drugi nivo istraživanja razmatra funkcije sistema video obezbeđenja, što uključuje karakteristike koje se odnose na postupke i procese ovog sistema sprovedene za postizanje sveobuhvatnih ciljeva sistema[174]. U svakom slučaju, prilikom planiranja i instaliranja video obezbeđenja (u praksi jednog od najzastupljenijih elektronskih sredstva tehničke zaštite) potrebno je, pored ostalog, imati u vidu i *Mišljenje radne grupe*[175] Evropskog savetodavnog tela za zaštitu podataka i privatnosti, a u vezi obrade podataka na radnom mestu, kao i navode iz *Smernica o obradi podataka o ličnosti putem video uređaja*[176] koje je izdao Evropski odbor za zaštitu podataka. Zbog sve veće zabrinutosti javnosti i drugih zainteresovanih strana o upotrebi veštačke inteligencije (eng. *Artificial intelligence (AI)*) i biometrijske tehnologije u sistemu video obezbeđenja, Britanci su prvi u svetu doneli *Kodeks upotrebe*[177], čija primena bi trebala da pomogne jačanju poverenja u javne ili privatne organizacije koje primenjuju ili nadgledaju tehnologije prepoznavanja lica.

Tehnička komponenta zaštite je veoma dinamična kategorija, uređaji i sistemi se neprekidno usavršavaju (razvoj video analitike, biometrije, upotreba pametnih tehnologija i dr.), kao i način njihove funkcionalne povezanosti (sve veća upotreba *IoT, AI,* korišćenje rešenja u oblaku itd.), što predstavlja poseban izazov za menadžere korporativne bezbednosti i druge nosioce planiranja, budžetiranja i ostalih faza izvođenja i upotrebe elemenata tehničke zaštite. Stalno praćenje tržišta i tehničko usavršavanje su neophodni koraci u radu i razvoju menadžera korporativne bezbednosti, koji je potrebno da ima u vidu i permanentno da analizira nove metode

174 Više pogledati: *CCTV surveillance: The differing aims and functions of CCTV within the corporate stratum*, Research Online, 8th Australian Security and Intelligence Conference, Edith Cowan University, Joondalup AU, 2015.

175 *Opinion 2/2017 on data processing at work – WP 249*, European advisory body on data protection and privacy, Brussels, June 2017.

176 *Guidelines 3/2019 on processing of personal data through video devices*, Version 2.0, European Data Protection Board, Brussels, January 2020.

177 *BS 9347:2024, Facial recognition technology. Ethical use and deployment in video surveillance-based systems. Code of practice.*

napada[178]. Zbog kompleksnosti sredstava, uređaja i sistema tehničke zaštite podrška prilikom planiranja i nabavke može se potražiti i u raznovrsnim smernicama i preporukama priznatih ekspertskih udruženja razvijenih zemalja koji na transparentan način objavljuju publikacije, a koje pomažu u definisanju i u shvatanju prednosti pojedinih sredstava i uređaja, odnosno čitavih sistema, njihove integracije, kao i pratećih elemenata za njihovo optimalno funkcionisanje i korišćenje. Primera radi, ukoliko imate potrebu za integrisanim sistemom tehničke zaštite, u nedostatku domaćih mogu se koristiti smernice istaknutog britanskog udruženja bezbednosne industrije *BSIA (British Security Industry Association)* koje je, pored ostalog, publikovalo i *Vodič za upravljanje integrisanim sistemom bezbednosti*[179]. Svakako da i zasebni sistemi moraju da zadovoljavaju zahteve potrebnih standarda[180], ali i prostor za prijem i obradu alarmnih signala i drugih informacija (kontrolna soba/centar) potrebno je da ispuni kako mere zaštite od neovlašćenog ulaska i kompromitacije, tako i konstrukcijske, ergonomske i druge potrebe u skladu sa principima bezbednosti i zdravlja na radu (ventilacija, rasveta, raspored i položaj opreme itd.).

Prilikom odlučivanja o vrsti i kvalitetu sredstva, uređaja i sistema koji su predmet planiranja i nabavke tehničke zaštite bitno je voditi računa o njenoj pouzdanosti i funkcionalnosti, mogućim nadogradnjama, kao i o troškovima održavanja i servisiranja koji padaju na teret korisnika tehničke zaštite. Sve zajedno utiče na ukupne troškove eksploatacije proizvoda i sistema tehničke zaštite, što je potrebno da imaju u vidu donosioci odluka, kojima početna cena nabavke i ugradnje često predstavlja isključivi faktor u odlučivanju.

Ekonomska bezbednost

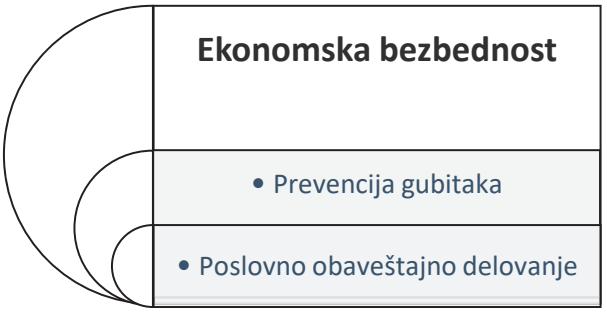
Ekonomska bezbednost, kao integralni deo korporativne bezbednosti, sve je prisutnija kako u društvenim naukama tako i u organizaciji savremenih kompanija i njihovoj poslovnoj praksi. Širi pojam ekonomske bezbednosti se manifestuje kao

178 Napadi bespilotnim letelicama su primeri novijih metoda ugrožavanja koji služe kako za osmatranje i prikupljanje podataka, tako i za uništavanje imovine i druge štetne radnje. Primera radi, napadima bespilotnih letelica sredinom septembra 2019. godine na naftna postrojenja kompanije Saudi Aramco u Saudijskoj Arabiji uništene su znatne količine nafte i prouzrokovan je prekida u njenoj proizvodnji što je izazvalo zabrinutost za stabilnost globalnog snabdevanja naftom i zbog čega su cene sirove nafte porasle dvocifreno.

179 Videti više: *A guide to integrated security management systems*, British Security Industry Association, Worcester UK, 2017.

180 Npr. protivprovalni i protivprepadni alarmni sistemi moraju da zadovolje zahteve standarda *EN 50131*, sistemi kontrole pristupa *EN 60839-11-1* itd.

elemenat bezbednosti države i društva, ali se mnogo češće sreće u svom užem smislu kao ekonomska bezbednost kompanija kada govorimo o ekonomskoj bezbednosti poslovanja.



Slika 2.7. Ekonomska bezbednost

U funkcionalnom smislu, ekonomska bezbednost poslovanja je integralni deo sistema korporativne, odnosno privatne bezbednosti. Predstavlja zaštićenost ekonomskih interesa i poslovne reputacije određenog privrednog subjekta od svih izvora, nosioca i oblika ugrožavanja sa stanovišta ekonomskih interesa. Ekonomska bezbednost je svojstvo privrednog subjekta, ispoljeno kao uspostavljeno, održano i unapređeno stanje i vrednost koja se izražava kao ispunjenost i zaštićenost minimuma bezbednosnih standarda, svojstvenih tom ekonomskom subjektu, bez obzira na nosioce, oblike i mesto ugrožavanja. Ekonomska bezbednost ne stvara materijalne vrednosti, ali bez nje nema opstanka, rasta i razvoja bilo kog ekonomskog (privrednog) subjekta. Pojednostavljeno, ekonomska bezbednost je stanje odsutnosti svih oblika društvene, tehničke ili prirodne opasnosti po ekonomske interese privrednog subjekta, a pre svega njegovu imovinu, poslovanje i sve druge vrednosti. Pod vrednostima privrednog subjekta podrazumeva se sve što je on, dosadašnjim radom, na tržištu ostvario[181].

Značaj ekonomske bezbednosti ogleda se u činjenici da svi ekonomski sistemi društva zavise od uspešnosti kompanija u njima. Stvaranje jakih kompanija i stabilnog makroekonomskog okvira za njihovo poslovanje sistem obezbeđuje mogućnost svog daljeg napretka. Ukoliko su kompanije u jednom sistemu ekonomski bezbedne to znači da će i taj sistem biti uspešan i bezbedan od negativnih uticaja bilo da dolaze spolja bilo iznutra.

181 Stajić Ljubomir, Mandić Goran, *Sistem zaštite imovine i poslovanja*, Pravni fakultet, Novi Sad, 2008., str. 4 – 16.

Rizik od eventualnih gubitaka predstavlja odnos objektivne i konkretne pretnje i stepena ranjivosti organizacije pa je zato neophodna procena obe ove komponente. Svaka organizacija ima manje ili veće slabosti koje pod određenim okolnostima mogu biti zloupotrebljene, pa u tom slučaju govorimo o problemima ranjivosti. Ako pođemo od definicije rizika kao verovatnoće nepovoljnog ishoda onda se rizik ekonomske bezbednosti može opisati kao verovatnoća da će pod uticajem objektivnih činilaca u konkretnom poslovnom procesu ili poslovanju uopšte, nastupiti posredna ili neposredna ekonomska šteta[182].

Brojni rizici od nastajanja ekonomskih gubitaka generišu se u poslovnom ambijentu, ali i izvan njega. Verovatnoća, pretnja ili moguća opasnost od neočekivanog delovanja određenih činilaca na ekonomsko poslovanje može dovesti do gubitka dela resursa preduzeća, nesticanja očekivane dobiti, pojave dodatnih troškova ili odstupanja rezultata od planiranih vrednosti.

Definisanje i procena rizika su početni, važni, ali lakši delovi posla bezbednosnog menadžmenta kompanije. Da bi se ekonomska bezbednost ostvarila u praksi potrebno je mnogo opšteg i specijalističkog znanja, mnogo upornog i sistematskog rada, korporativne odgovornosti i posvećenosti ciljevima kompanije.

Smanjenje rizika poslovnog partnerstva, a samim tim i rizika od eventualnih gubitaka, zahteva visok nivo odgovornosti, stručnog znanja i vrhunskih aktivnosti menadžera koje se u poslovnom žargonu opisuju pojmom „*due diligence*“.[183]

Prevencija gubitaka je ključna oblast i glavni sadržaj rada menadžmenta korporativne bezbednosti na zaštiti ekonomske bezbednosti poslovanja preduzeća. Ostvaruje se: preventivnim sistemom bezbednosnih provera; otkrivanjem, onemogućavanjem, sprečavanjem i otklanjanjem posledica korupcije, kriminala i nesavesnog poslovanja; verifikacijom bezbednosnog kvaliteta zaposlenih, a posebno osoba na rukovodećim pozicijama; pružanjem pomoći menadžmentu organizacije u naplati dospelih potraživanja i otkrivanju i onemogućavanju nelojalnih postupaka konkurencije na tržištu.

Osnovni sadržaj rada menadžera na prevenciji gubitaka u kompaniji je preventivni sistem bezbednosnih provera koji treba da obezbedi pravovremeno otkrivanje, izbegavanje, umanjivanje i otklanjanje ekonomskih rizika od mogućih gubitaka. Ti

182 Stojanović Milan, Pavlović Dejan, *Ekonomska bezbednost poslovanja*, Srpska asocijacija menadžera korporativne bezbednosti i Škola plus, Beograd, 2014., str. 23.

183 „Due diligence“ je engleski termin koji se kod nas koristi u izvornom obliku. Za njega nema adekvatnog prevoda, a najbliži adekvatnom prevodu su termini „dužna pažnja“ i „dubinsko snimanje“.

zadaci se realizuju proverom privrednih društava, preduzetnika i drugih pravnih lica, proverom fizičkih lica, učesnika u poslovnim procesima, proverom ugovornih dokumenata, praćenjem realizacije ugovora u skladu sa utvrđenom dinamikom, upravljanjem procesima za otklanjanje poslovnih problema, smetnji i poteškoća, suzbijanjem koruptivnog i drugog neetičkog ponašanja zaposlenih i organizovanim merama za naplatu dospelih potraživanja.[184]

Provera privrednog društva je skup međusobno sinhronizovanih aktivnosti bezbednosnog menadžmenta na prikupljanju poslovnih informacija sa ciljem procene pouzdanosti tog privrednog društva za uspostavljanje poslovnog partnerstva i bezbednosti projektovanih poslovnih procesa. Zarad menadžera u kompaniji je, sa stanovišta ekonomske bezbednosti, od posebne važnosti procena o ispunjenosti uslova potencijalnog partnera i na bazi te procene zaključak o njegovom ukupnom kapacitetu kao garantu da će biti u stanju da odgovori eventualno preuzetim i ugovorenim obavezama. Pouzdanost preduzeća, kao potencijalnog partnera jednog privrednog društva, može se utvrditi na osnovu njegovih poslovnih, finansijskih, tehničkih i kadrovskih kapaciteta.[185]

Kao što je važna ocena privrednog društva, koja sadrži poslovni, tehnički i kadrovski kapacitet, finansijski bonitet, društveni integritet i poslovni položaj u aktuelnom ekonomskom ambijentu, isto tako je važno upoznati osobu koja zastupa to preduzeće i to u dve komplementarne ravni njenog menadžerskog profila - subjektivnoj i objektivnoj. Subjektivne osobine zastupnika ukazaće nam u njihovoj rezultanti na njegov profesionalizam i poslovni moral, a objektivne proističu iz njegovog formalnopravnog položaja.

Pored provere saugovarača neophodna je i bezbednosna supervizija kako suštine tako i samog teksta ugovora.

Ugovori imaju veliki značaj u poslovanju svake kompanije sa najvećim odrazom na pravni, organizacioni i funkcionalni ambijent. Dobro sačinjen ugovor predstavlja faktor sigurnosti poslovanja, a celokupni supstrat zaključenih ugovora predstavlja projekciju realnog sistema poslovnih procesa u kompaniji.

Za svaki ugovorni dokument je neophodno utvrditi usklađenost odredbi i konzistentnost ugovora, pre svega radi eventualnog otkrivanja skrivenih obaveza. One mogu nastati smišljeno definisanim odredbama kojima se nanosi šteta ekonomskim interesima, nejasno preciziranim odredbama koje ostavljaju mogućnost različitog

184 Stojanović Milan, Pavlović Dejan, op. cit., str. 119.

185 Ibid, str. 119-121.

tumačenja kao i izostavljanjem određenih odredbi kojima se obezbeđuje sigurnost poslovanja ili finansijska disciplina u platnom prometu.

Ukoliko podaci iz ugovora predstavljaju poslovnu tajnu unosi se klauzula o obavezi zaštite poslovne tajne ili se zaključuje poseban ugovor o zaštiti tajnosti. Odluka o tome donosi se u skladu sa klasifikacijom poverljivih podataka i drugim kriterijumima usvojenim od strane upravnih organa kompanije.

Poslovna praksa savremenih kompanija pokazuje da se najbolji rezultati u prevenciji gubitaka ostvaruju sistemskim upravljanjem ugovornim dokumentima. To podrazumeva uspostavljanje jedinstvenog načina pripreme, usaglašavanja, potpisivanja, registrovanja, distribucije i čuvanja ugovornih dokumenata u privrednom društvu[186]. Upravljanje ugovornim dokumentima ukazuje na brojne prednosti procesa međusobnog usaglašavanja nacrta ugovornih dokumenata pre njihovog potpisivanja.

Mere koje se preduzimaju za zaštitu ekonomskih interesa privrednog društva u okviru predugovornih aktivnosti završavaju se usaglašavanjem i zaključivanjem odgovarajućih ugovora. One, međutim, nisu dovoljne da bi se u potpunosti eliminisala pojava neplaniranih gubitaka poslovanja već su neophodne i mere kontinuiranog praćenja realizacije ugovora. Bezbednosni monitoring je integralni deo i važan sadržaj tog procesa. Praćenjem realizacije ugovora otkrivaju se indikatori neposrednog ili očekivanog ugrožavanja ekonomske bezbednosti kompanije. Poslovna praksa na tržištu RS ukazuje da su indikatori povećanog ekonomskog rizika naročito vidljivi u situacijama kad poslovni partner odstupa od uobičajenog poslovnog ponašanja i poslovne komunikacije. Ključne promene su:

- učestala nelikvidnost pri čemu broj dana nelikvidnosti sa vremenom narasta;
- razvojni trend kašnjenja u servisiranju sistematskih ili ugovorenih obaveza;
- česte promene adrese sedišta kompanije kao i brojeva telefona ili elektronske adrese vlasnika, direktora ili drugog ovlašćenog lica;
- neočekivane promene direktora ili drugog ovlašćenog zastupnika;
- neuobičajena kupovina kompanije u procesu privatizacij ili stečaja kao i druge poslovne investicije koje bitno odudaraju od poslovne logike;

186 Pod ugovornim dokumentima se podrazumevaju osnovni ugovori, aneksi ugovora i razni prilozi čiji sadržaj može biti: građansko – pravni ugovor, ugovor o poverljivosti, sporazum o namerama, sporazum o saradnji, sporazum o partnerstvu, memorandum, protokol, tehnički sporazum, sporazum sa državnim organima, zaključnica i dr.

- neopravdana kupovina ili lizing[187] luksuznih automobila, apartmana, nameštaja i dr.

Važne indikatore ekonomskog rizika veoma često možemo prepoznati i u ponašanju vlasnika ili zastupnika partnerskog preduzeća. To su najčešće: luksuzan nakit, upadljiva odeća i pojavljivanje na mestima luksuzne turističke ponude; duže odsustvovanje vlasnika ili direktora bez imenovanja ovlašćenog zastupnika; izbegavanje susreta sa poveriocem; izbegavanje javljanja na telefonske pozive ili odgovora na elektronsku poštu i dr.

Praćenjem indikatora ekonomskog rizika menadžment korporativne bezbednosti privrednog društva će obezbediti blagovremenu identifikaciju mogućih poslovnih problema. U tom cilju je veoma važno poznavanje poslovnog partnera, pre svega poslovnih manira njegovih zastupnika i karakteristika poslovne komunikacije kako bi se na vreme uočila odstupanja od uobičajenog ponašanja. Pravovremena informacija o statusnim promenama ili promenama u poslovanju partnera ima takođe veliki značaj za otklanjanje rizika poslovanja i prevenciju gubitaka.

Proces ostvarivanja ekonomske bezbednosti u okviru pojedinačnog biznis projekta je integrisan u primarni poslovni proces. Počinje prikupljanjem informacija iz primarnih izvora. Pretraživanjem javnih baza interneta, uvidom u privredne adresare, posetama privrednim sajmovima i izložbama, pregledom ekonomskih časopisa i komunikacijom sa pouzdanim poslovnim partnerima, menadžment privrednog društva dolazi do širokog spiska potencijalnih poslovnih partnera u funkciji realizacije usaglašenih biznis projekata. Tim postupkom menadžeri privrednog društva sagledavaju ulogu, značaj, prisustvo na tržištu i aktivnost tih pravnih subjekata kao i određene standarde, tehnologije, cene i druge parametre u okviru određenih poslovnih oblasti. Iz tih razloga ova početna poslovna aktivnost popularno je nazvana istraživanje tržišta.

Istraživanje tržišta je sistematska, uporna i dinamična aktivnost menadžera i izvršilaca poslovnih procesa ili projekata sa ciljem proveravanja relevantnog stanja tržišta i prikupljanja neophodnih informacija zaodlučivanje i planiranje standardizovanih postupaka i konkretnih proceduralnih radnji. Ukoliko dobro upozna uslove na relevantnom tržištu menadžer može da u okviru izabrane strategije pro-

187 Finansijski lizing je jedan od načina finansiranja ulaganja u osnovna sredstva. Predstavlja popularnu alternativu bankarskim kreditima i zaduživanju putem emitovanja dužničkih hartija od vrednosti. Operativni lizing (rent) je kratkoročni ugovor o zakupu pri čemu je period ugovora obično duži od jedne godine, a kraći nego što je korisni ekonomski vek trajanja predmeta zakupa.

ceni: stanje očekivane konkurencije, željeni odnos između cene, kvaliteta i drugih komercijalnih kriterijumima, sadržaj i način pregovaračke aktivnosti kao i druge pogodnosti koje u okviru određenog projekta želi da postigne. Metodologija istraživanja tržišta može se propisati internim procedurama, uputstvima ili instrukcijama. Načelno sadrži tri funkcionalna elementa: prikupljanje poslovnih informacija, segmentaciju tržišta i procenjivanje trendova. Prikupljanje tačnih, aktuelnih i blagovremenih poslovnih informacija je osnovni preduslov kvalitetnog istraživanja tržišta. Kroz proces segmentacije tržišta se uočavaju razlike po osnovu geografskih, psihografskih, tehničko-tehnoloških, strukovnih i drugih karakteristika tržišta za određene poslovne delatnosti, a trendovi na tržištu su veoma važni prvenstveno sa stanovišta primene novih tehnologija, metoda i postupaka.

Nakon istraživanja tržišta, sledeći korak menadžmenta u procesu ekonomske bezbednosti je provera kandidata za poslovno partnerstvo. Predstavlja veoma važnu fazu sprovođenja ekonomske bezbednosti. Realizuje se u više nivoa sa ciljem što objektivnijeg ocenjivanja pouzdanosti potencijalnih partnera i eliminisanja nosilaca visokog ekonomskog rizika.[188]

Pored sistemskih mera na preventivnim bezbednosnim proverama, veoma važna aktivnost bezbednosnog menadžmenta je suzbijanje korupcije, kriminala i kriminalne motivacije zaposlenih.

Suprostavljanje korupciji je složen, slojevit i dugoročan proces. Karakteristike tog procesa mogu se analizirati na društvenom, korporativnom i menadžerskom nivou. Društveni nivo suzbijanja korupcije obuhvata sinhronizovane i osmišljene napore državnih i drugih društvenih sistema usaglašenih sa naporima kredibilnih međunarodnih faktora. Korporativni nivo suzbijanja korupcije obuhvata napore koje preduzima privredno društvo, a menadžerski nivo označava oblast odgovornosti rukovodioca konkretnog organizacionog dela ili poslovnog procesa kojim u skladu sa nadležnostima i ovlašćenjima upravlja.

Dok se prvi (društveni) nivo borbe protiv korupcije sprovodi na nivou države i društva u interakcijskim odnosima sa ključnim činiocima međunarodne zajednice, drugi nivo se organizuje u okviru kompanije. Mnogi politički aktivisti, ekonomski stručnjaci, sociolozi i drugi analitičari društvenih odnosa pokušavaju da odgovore na pitanje: Da li etička kompanija može da izdrži konkurenciju na tržištu koje nije otporno na uticaje korupcije? Iskustva mnogih zemalja, među kojima su zemlje Evropske unije, Ruska Federacija i SAD, ukazuju da je odgovor na ovo pitanje po-

188 Stojanović Milan, Pavlović Dejan, op. cit., str. 164.

tvrdan, naročito ako kompanija radi dobar i društveno koristan posao i ako ulaže napore da promeni situaciju u svom okruženju.[189] Praksa je potvrdila da veće kompanije imaju i veće izglede da njihovo etički korektno poslovanje postane značajan faktor poslovnog marketinga. Takođe je nesporno da su grupe kompanija u kojima se afirmiše etičko poslovanje daleko uspešnije nego napori pojedinačnih preduzeća. U tom cilju svaka etična kompanija ima respektivne saveznike u drugim modernim multinacionalnim kompanijama koje su opredelile svoje investicije na tržištu RS, uspešnim domaćim kompanijama, javnim preduzećima i naravno, najznačajnijeg saveznika ima u Vladi RS i njenim institucijama.

Pored ranije navedenih mera za sprečavanje i otklanjanje mogućnosti nastanka i razvoja korupcije kao najbolja praksa kojom se eliminišu negativni uticaji korupcije preporučuje se: poštovanje zakona u zemljama u kojima kompanija ostvaruje poslovanje; svest rukovodioca kompanije o zakonskim obavezama i odgovornostima; uticaj glavnog menadžmenta kompanije preko nadležnog ministarstva na promenu zakonske regulative ukoliko važeći zakoni stavljaju kompaniju u neravnopravni položaj prema konkurentima; usvajanje kodeksa ponašanja sa adekvatnim antikorupcijskim merama; uticaj menadžera na zaposlene radi poštovanja propisa i kodeksa ponašanja; podržavanje svih antikorupcijskih tela, inicijativa i aktivnosti u zemlji i inostranstvu; saradnja sa partnerskim preduzećima i drugim uglednim kompanijama radi uspostavljanja pravnih i moralnih pravila na tržištu i dr.

Na nivou internog korporativnog polja borbe protiv korupcije, nekoliko oblasti bezbednosnog monitoringa izdvojile su se kao težišne, a to su:

- nabavke roba i usluga,
- prodaja osnovnih proizvoda i
- sistem finansijske kontrole poslovanja.

Kadrovski menadžment, koji po svojoj definiciji artikuliše polje subjektivnog faktora predstavlja četvrti stub tog procesa. Zdrava i na naučnim i iskustvenim osnovama postavljena politika ljudskih resursa je osnovni preduslov bilo kakvog uspeha u suzbijanju korupcije, kriminala i raznih finansijskih prevara.

Da bi proces nabavki roba i usluga na nivou privrednog društva bio otporan na pojavne oblike korupcije neophodno je obezbediti osnovne organizacione i pravne pretpostavke, a pre svega:

189 Ibid, str. 178.

- definisanje standarda, procedura, strogih pravila i dobre poslovne prakse;
- uspostavljanje organizacionih formi i metodoloških principa koji obezbeđuju pošteno i javno nadmetanje potencijalnih dobavljača;
- obezbeđivanje i raspoređivanje stručnih, odgovornih i posvećenih izvršilaca tenderskih postupaka;
- onemogućavanje klime u kojoj se menadžeri na neprikladan način mešaju u konkretne tenderske postupke;
- vođenje odgovarajućih službenih zabeleški o postupcima nabavke kao i odgovarajuće evidencije o dobavljačima, kvalitetu pruženih usluga i drugim kriterijumima vrednovanja njihove pouzdanosti.[190]

Pored javnih i sektorskih naručilaca koji su shodno *Zakonu o javnim nabavkama*[191] u obavezi da postupaju u skladu sa propisanim načelima, poslovna praksa etičnih kompanija iz privatnog sektora je ustanovila osnovna načela (principe) za poštene i efikasne postupke nabavki roba i usluga. Najznačajnija su korporativna odgovornost, ekonomičnost, efikasnost, nepristrasnost i transparentnost.

U okviru poslova prodaje osnovnih proizvoda jednog privrednog društva takođe je naglašena odgovornost menadžmenta korporativne bezbednosti u pogledu obaveze prepoznavanja i otkrivanja određenih manifestacija koje se mogu protumačiti kao indikatori moguće pojave koruptivnog ponašanja zaposlenih. Prilikom praćenja bezbednosnih indikatora pažnja menadžera bezbednosti mora biti kontinuirana sa povećanim oprezom u periodima prodaje koji prema poslovnom iskustvu obiluju većim bezbednosnim rizicima. To su pre svega periodi nestašica i povećanja tražnje pojedinih proizvoda na tržištu, periodi očekivanih promena cene, pojedinih njenih elemenata kao i faktora koji utiču na njeno formiranje i periodi u kojima narasta potražnja usled vremenskih uslova, sezonskih potreba i drugih objektivnih okolnosti koje utiču na stanje prometa.[192]

Preduzimljivi, ali i koruptivno motivisani učesnici u prometu, svaku promenu ili poremećaj tržišnih uslova vide kao šansu za laku i brzu zaradu pa je neophodno povećati nadzor bezbednosnog menadžmenta u tim situacijama. Koruptivni motivi mogu biti i generator nestašica uopšte ili nestašica pojedinih, planski izabranih proizvoda. Ovaj oblik korupcije je povezan sa odavanjem poslovnih informacija o po-

190 Ibid, str. 179.

191 „Službeni glasnik RS", br. 91/2019 i 92/2023.

192 Stojanović Milan, Pavlović Dejan, op. cit., str. 181.

slovanju kompanije i stanju na tržištu. Na bazi realnih informacija o stanju na tržištu privilegovani kupci u saradnji sa izvršiocima komercijalnih poslova u strukturi prodavca mogu obezbediti velike zalihe deficitarne robe da bi ih u periodu nestašice prodavali po većim cenama ili u većim količinama.

Da bi se otklonili uslovi za pojavu neetičkog ponašanja zaposlenih u komercijali bezbednosni menadžment mora da izvrši blagovremene pripreme i poveća monitoring poslovanja u vreme komercijalnih kampanja. Periodična, redovna ili vanredna promena cena osnovnih proizvoda mora biti blagovremeno procenjena, pažljivo pripremljena i planski realizovana uz poštovanje principa zaštite poslovnih informacija.[193]

Da bi se na nivou privrednog društva uspostavio bezbedan poslovni ambijent u kome su primeri neetičkog ili koruptivnog ponašanja lako prepoznatljivi neophodno je obezbediti:

- uputstva, standarde i procedure za organizaciono i metodološko usmeravanje rada izvršilaca komercijalne funkcije; poštovanje zakona, propisa i moralnog kodeksa od strane zaposlenih;
- zaštitu poslovnih informacija;
- organizovan i standardizovan sistem provere i bezbednosne procene kupaca; sprečavanje diskriminacije kupaca;
- stvaranje i negovanje kulture zdrave i poštene konkurencije;
- sankcionisanje pojedinačnih primera zloupotreba ugleda i položaja privrednog društva na tržištu;
- ograničavanje diskrecionih prava pojedinaca i organizacija interne kontrole poslovanja.

Pored navedenih preduslova integritetu privrednog društva doprinose i druge opšte aktivnosti kao što su:

- redovne i vanredne analize poslovanja na opštem, sektorskom i personalnom nivou;
- provera, praćenje, ocenjivanje, edukacija i vođenje karijere komercijalnih menadžera i izvršilaca;

193 Ibid, str. 182.

- kontinuirana, otvorena i konstruktivna saradnja sa funkcijom korporativne bezbednosti;
- saradnja sa nacionalnim i strukovnim udruženjima privrednika, preduzetnika i potrošača;
- javnost poklona i prezentacija, periodično informisanje, interna komunikacija i sprovođenje programa bezbednosne obuke zaposlenih.

Uspostavljanje zdravog finansijskog sistema sa delotvornim računovodstvom uz dobro upravljanje finansijama je veoma moćno i u praksi dokazano sredstvo u borbi protiv korupcije uopšte pa samim tim i u okviru privrednog društva. Kada se podaci i analize finansijske funkcije uporede sa preciznim stručno oformljenim izveštajima unutrašnje i eksterne revizije dolazi se do putokaza za otkrivanje tzv. kriminala belih okovratnika i preduzimanje mera za njegovo suzbijanje ili presecanje. Treći faktor koji upotpunjuje ovu antikorupcijsku strategiju je glavni i izvršni menadžment, opredeljen da energično i efikasno preseče put finansijskim prevarama i njihovo svođenje na sporadične i po značaju zanemarljive pojedinačne slučajeve. Kada se razmišlja o korupciji i finansijskim prevarama najčešće se prvo razmatraju mehanizmi pravne zaštite i drugih funkcija restriktivnog korporativnog organizovanja i delovanja. Donošenjem strogih pravila često se „drakonskim" kaznama doprinosi samo da odgovorni rukovodioci „umire savest", ali poslovna praksa mnogih kompanija ukazuje da su rezultati takve strategije uglavnom skromni. Druga predrasuda je da periodična revizija, najčešće jednom godišnje, obezbeđuje preventivu finansijskih prevara. Takvim stavom se ne uvažava činjenica da su revizori nemoćni u situacijama kada se neadekvatnim vođenjem knjiga prikriju putevi protoka novca koje oni treba da slede pri otkrivanju nepravilnosti i utvrđivanju odgovornosti za njihovo nastajanje. Nepovezan, nekorektan i neažuran sistem knjigovodstva, naročito ukoliko je podvrgnut nejedinstvenom upravljanju predstavlja pogodno tlo ali i ključni indikator finansijskih prevara i malverzacija. Neadekvatan finansijski sistem je ujedno i najveća brana otkrivanju prevara, a ukoliko se postojanje prevare otkrije onda nije moguća identifikacija odgovornih izvršilaca.

Budući da je značajna za kadrovsku strukturu zaposlenih u poslovnim procesima u okviru kojih se izražava težište strategije za suzbijanje prevara i korupcije, kadrovska funkcija u kompaniji i sama postaje važan i autentičan činilac tog složenog procesa. Osnovni zadatak kadrovske politike i prakse je da obezbedi adekvatnu kadrovsku strukturu zaposlenih sa neophodnim bezbednosnim kvalitetom popune

i sa osobinama i sposobnostima primerenim konkretnom radnom mestu kao i ciljevima i poslovnoj strategiji privrednog društva u celini.

Pored opšteg društvenog i posebnog korporativnog nivoa za suzbijanje korupcije odlučujuća je uloga rukovodioca organizacionih delova i procesnih menadžera. Menadžerski nivo je osnovni radni i izvršni nivo korporativnog organizovanja za suzbijanje korupcije i raznih finansijskih prevara.[194] Svaki rukovodilac na osnovu utvrđenih odgovornosti, stručnog znanja, poslovnog iskustva i izgrađenih liderskih osobina ima pravo i obavezu da kroz tekuće poslovanje i upravljanje poslovnim procesima, afirmiše, sprovodi i kontroliše rad podređenih izvršilaca poslovnih funkcija u sklad sa principom zakonitosti. To znači da sistemom monitoringa, ocenjivanja, podsticanja i kontrole, otkriva koruptivno ponašanje zaposlenih, preduzima sistemske mere za onemogućavanje svakog vida zloupotrebe ovlašćenja kao i mere za otklanjanje posledica. Dobar rukovodilac neće dozvoliti da koruptivno ponašanje zaposlenih naruši poslovnu reputaciju i ekonomski interes kompanije već će sistemom preventivnih mera i antikorupcijskih propisa, organizacionih rešenja i metoda upravljanja predupredi moguće rizike. U tom cilju neizostavna je i ključna uloga menadžera korporativne bezbednosti koji će kroz proces bezbednosnog monitoringa pratiti indikatore, procenjivati rizike i predlagati antikoruptivne mere.

Kroz poslovnu praksu su se izdiferencirali pojedini postupci zaposlenih koji se mogu okarakterisati kao rani znaci upozorenja o mogućem postojanju korumpiranog izvršioca. To su pre svega: odbijanje postavljenja, često i na viši položaj; odbijanje korišćenja godišnjeg odmora; redovno prekomerno ostajanje na radnom mestu, često do kasnih časova, bez logičnog opravdanja i poslovnih potreba; česte ili stalne nabavke manjih količina materijalno tehničkih resursa od istog dobavljača; izuzetno brzo ili neopravdano sporo plaćanje određenih finansijskih obaveza; neuobičajeno velike finansijske olakšice; učestali izveštaji o gubljenju ili oštećenju roba, otpisu uskladištenih roba, roba sa isteklim rokom trajanja i dr. Ovom spisku treba dodati i indikatore subjektivnog karaktera kao što su tajno dobijanje poklona, nagla promena materijalnog položaja, kupovina skupocenih predmeta, skupa privatna putovanja i dr.

U oblasti komercijalne funkcije bezbednosni menadžment posebno procenjuje postupke zaposlenih u slučajevima:

- birokratskog i arogantnog odnosa prema kupcima;

194 Ibid, str. 185-189.

- zanemarivanja primedbi, kritika i reklamacija od strane pojedinih kupaca;
- predlaganja ugovora velike vrednosti sa novim, nedavno registrovanim i malim privrednim društvima;
- preuzimanja pojedinih kupaca van svoje organizaciione nadležnosti;
- zanemarivanja problema u naplati potraživanja;
- produžavanja saradnje pod istim ili povoljnijim uslovima uprkos lošeg izmirivanja finansijskih obaveza;
- otpremanja velikih avansno plaćenih količina proizvoda bez zaključivanja ugovora;
- pokušaja izbegavanja usaglašavanja ugovora shodno standardima društva;
- dobijanja neprikladnih poklona;
- pogoršavanja međuljudskih odnosa bez vidljivog logičkog povoda;
- nezainteresovanost za stručne kritike, ocene i razvoj karijere van komercijalne funkcije i dr.

Pored toga saznanja o oticanju poslovnih informacija ili pregovorima za prelazak u konkurentsko ili partnersko preduzeće je važan signal za povećanje pažnje i bezbednosnog monitoringa. Pojedini izvršioci koji moralno opravdavaju provizije i poklone ili izražavaju sklonost ka neumerenom sticanju novca il dobara moraju blagovremeno biti edukovani da se njihove predispozicije ne bi razvile u koruptivno ponašanje.

Rezultanta objektivnih eksternih uticaja na koruptivno ponašanje zaposlenih može se sagledati u okviru interakcijskih odnosa tri ključna činioca: koruptivnih predispozicija izvršilaca konkretnog poslovnog procesa, negativnih uticaja okruženja i pozitivnih uticaja menadžmenta kompanije.

Na kraju se može zaključiti da je verovatnoća za pojavu korupcije, pronevera ili finansijskih prevara u kompaniji srazmerna intenzitetu negativnihuticaja okruženja i ukupnih predispozicija izvršilaca poslovnih procesa, a obrnuto srazmerna pozitivnim uticajima menadžmenta. Iz takvog zaključka proističe potreba menadžera svakog privrednog društva da poznaju svoje zaposlene, prate stanje u okruženju i preduzimaju kontinuirane mere za suzbijanjekorupcije, kriminala i finansijskih prevara u svom organizacionom delu[195].

195 Ibid, str. 289.

Kada govorimo o prevenciji finansijskih gubitaka tipičan primer egzaktnih i potpuno merljivih gubitaka jednog privrednog društva su nenaplaćena potraživanja. U okviru širokog spektra ekonomskih rizika, sa kojima se svakodnevno suočava jedno privredno društvo, rizik kreditiranja kupaca konceptom odloženog plaćanja, predstavlja najveći izazov ekonomske bezbednosti. Iako je stalna briga za tokove platnog prometa integralni deo dnevnog operativnog rukovođenja, poslovna praksa ukazuje da opšti nivo korporativne odgovornosti zaposlenih, pre svega u okviru komercijalne funkcije, najčešće ne obezbeđuje potpunu kontrolu ove vrste rizika.

Velike proizvodne, trgovačke, finansijske i druge poslovne organizacije karakterišu veliki obim poslovanja i dinamični tokovi platnog prometa. Dinamično kretanje novca i obim ukupnog prometa omogućava velikim kompanijama komparativnu prednost na tržištu u vidu mogućnosti poslovanja sa odloženim plaćanjem. Taj komercijalni uslov je veoma privlačan za brojne privredne subjekte koji u uslovima oštre konkurencije sve teže dolaze do gotovog novca za finansiranje osnovnih poslovnih procesa. Razvijen sistem odloženog plaćanja podrazumeva pažljiv odabir instrumenata obezbeđenja plaćanja i proveru finansijskog boniteta poslovnog partnera. Nažalost, specifičnost makroekonomskih uslova i komplikovani interakcijski odnosi među privrednim subjektima usložavaju proveravanje pravnih subjekata i izvođenje zaključaka o njihovoj pouzdanosti. Događa se u praksi da na prvi pogled dobra preduzeća za veoma kratko vreme zapadnu u ozbiljne poslovne ili finansijske poteškoće. Vlasnici ili menadžeri tih preduzeća ponekad vide izlaz iz teškoća u privremenom ili trajnom prekidu poslovanja, a to izaziva finansijske posledice kod poverilaca, odnosno preduzeća koja iskazuju određena finansijka potraživanja. Na taj način etička kompanija može doći u situaciju da i pored brige za ekonomsku bezbednost i preduzetih mera za predhodnu proveru partnera, naglo zapadne u situaciju da bude u redu poverilaca koji čekaju naplatu svojih potraživanja sa neizvesnim konačnim ishodom.

Kontinuiran, sistematski i odgovoran rad sa tekućim potraživanjima je osnovni preduslov svakog uspeha u radu sa eventualnim dospelim potraživanjima. Naplata dospelih potraživanja manifestujes e u praksi kao otklanjanje posledica predhodno zanemarenih principa, sadržaja i oblikae konomskebezbednosti. U metodičkom smislu menadžerima poverilaca se pružaju tri osnovna pravca ka izlaznoj strategiji:

(1) namirenje mirnim (dogovornim) putem;

(2) namirenje u vansudskom postupku izvršenja i

(3) namirenje u sudskom postupku izvršenja.

Dobra poslovna praksa ukazuje na značaj formiranja timskog rada eksperata više funkcija[196], pre svega komercijalne, finansijske, pravne i funkcije korporativne bezbednosti, a u cilju iznalaženja alternativnih načina naplate dospelih potraživanja od nelikvidnih preduzeća. Prednosti timskog rada doprinose boljim rezultatima u naplati dospelih potraživanja prvenstveno zbog toga što: članovi tima učestvuju u postavljanju realnih konkretnih ciljeva; ciljevi tima imaju prioritet nad ličnim ili funkcionalnim ciljevima, razumevanje sopstvene uloge i preuzimanje odgovornosti predstavlja osnovni elemenat radne atmosfere u timu, sinergija stručnih znanja i veština ima veći značaj od zbira pojedinačnih uloga, otvorenost za nove ideje i drugačije perspektive pruža veću šansu poslovnom uspehu, odluke nisu rezultat formalnog autoriteta i statusa rukovodilaca već proizilaze iz procene suštine problema, a greške koje se neminovno javljaju u poslovanju imaju manji negativni uticaj na konačan uspeh poslovnog projekta i jednostavnije se prevazilaze[197].

U poslovnoj praksi savremenih kompanija, a pre svega razvojnih i inovativnih preduzeća, mogu se javiti štete usled raznih nelojalnih, neetičkih i često nezakonitih postupaka konkurencije na tržištu, koji se manifestuju kao umanjena ili izgubljena dobit.

Protokolima o saradnji, pre svega velikih kompanija, sa resornim ministarstvima Vlade RS, finansijskom i komunalnom policijom, carinom, državnim inspekcijskim službama i drugim državnim institucijama, kao i sporazumima o partnerstvu sa drugim etičkim i društveno odgovornim kompanijama, ostvaruje se organizacioni, operativni i metodološki osnov za nametanje zakonitosti i etičnosti poslovanja na tržištu RS.

Pod uticajem kredibilnih inostranih tržišnih faktora, modernih međunarodnih kompanija koje imaju učešće na tržištu RS, ali i pod uticajem kontinuiteta u razvoju tržišta raste broj kompanija koje su usvojile odgovarajuće programe obezbeđivanja korporativne socijalne odgovornosti. Kao deo strategije odgovornog i održivog poslovanja na tržištu, te kompanije nameću svojim dobavljačima kao i svim drugim partnerima specifične kodekse poslovnog ponašanja. Oni, pored ostalog, uvažavaju savremene zahteve poslovnog integriteta, upravljanja zaštitom životne sredine, uslova rada zaposlenih, zdravlja i bezbednosti na radu i drugih oblasti. Na taj način se generišu specifične, savremene i etične zajednice dobavljača, međusobno uvezane

196 Tim predstavlja manju grupu lica, komplementarnih stručnih znanja i veština koji su posvećeni zajedničkom poslovnom procesu ili projektu, imaju osećaj zajedničke korporativne odgovornosti i interaktivno deluju radi postizanja zajedničkog cilja.

197 Stojanović Milan, Pavlović Dejan, op. cit., str. 173.

moralnim kodeksima i standardima poslovnog ponašanja. Podsticaj promotivnom talasu poslovne etike na tržištu RS daje i pojava neprofitnih organizacija za razmenu podataka o dobavljačima stvarajući na taj način široki front otpora svakom vidu protivpravnog i amoralnog postupanja u privredi[198].

Stepen ostvarivanja ekonomske bezbednosti poslovanja proističe iz ukupnog stručnog i poslovnog kapaciteta menadžera, a posebno menadžera korporativne bezbednosti, njihovog individualnog stručnog znanja, ali i neophodne veštine da se usvojena znanja pretoče u odgovarajući poslovni rezultat kao praktičnu korist za kompaniju, njene akcionare i celokupno zaposleno osoblje. Putokaz za ostvarivanje ekonomske bezbednosti poslovanja treba trasirati kroz ključne sadržaje i principe ekonomske bezbednosti, metodologiju proveravanja potencijalnih učesnika u poslovnom partnerstvu, praćenje realizacije poslovnih procesa i projekata, a pre svega kroz rano otkrivanje poslovnih problema i umanjivanje njihovih eventualnih štetnih uticaja na ekonomske interese ili poslovnu reputaciju kompanije.[199]

Prevencija gubitaka

Suštinski posmatrano, svi poslovi korporativne bezbednosti, odnosno sve mere, radnje i kontrole koje su u nadležnosti te funkcije, imaju zadatak da spreče nastajanje gubitaka po zaposlene i druga lica (kupce, korisnike i druga zainteresovana lica), imovinu i poslovanje organizacije. Osim preventivnog delovanja korporativna bezbednost u svom delokrugu ima i preduzimanje svih potrebnih proaktivnih i reaktivnih radnji kojima bi se umanjili gubici u slučaju ostvarivanja pretnji ili nastanka posledica opasnosti, kao i omogućio dalji rad organizacije nakon prekida poslovanja uzrokovanog incidentom, katastrofom ili drugim bezbednosnim događajem.

U tom smislu, prevencija gubitaka (eng. *loss prevention*) ima posebnu ulogu u pojmu bezbednosti koji je naveden u *Evropskom priručniku za osnovnu stručnu obuku službenika obezbeđenja*[200], gde se definiše kao

> *„čuvanje života, zaštita imovine od svih vrsta gubitka u slučaju nesreće, krađe, prevare, požara, eksplozije, oštećenja ili otpada i uključuje sve aspekte prevencije gubitaka*".

198 Ibid, str. 225.

199 Ibid, str. 16.

200 Spaninks Louis, Quinn Larry, Byrne John, *European Vocational Training Manual For Basic Guarding*, Leonardo NL/96/2/1136/PI/II.1.1.b/FPC, Brussels, 1999.

Zato je implementacija različitih programa korporativne bezbednosti (protiv internih i eksternih krađa, prevara i drugih zloupotreba, namernih i nenamernih grešaka zaposlenih, odavanja tajni, prevencije povreda na radu itd.) od ključne važnosti za prevenciju gubitaka kao neophodne platforme uspešnog poslovanja bilo koje organizacije, a posebno ukoliko njena delatnost pripada visoko rizičnim sektorima kao što su bankarstvo, osiguranje/reosiguranje, logistika, proizvodnja, kao i različiti vidovi maloprodaje.

Jedan od osnovnih delatnosti bezbednosnog menadžmenta na prevenciji gubitaka u kompaniji je preventivni sistem bezbednosnih provera koji treba da obezbedi pravovremeno otkrivanje, izbegavanje, umanjivanje i otklanjanje rizika ekonomske bezbednosti. Kao što je ranije navedeno, ti zadaci se realizuju proverom privrednih društava, preduzetnika i drugih pravnih lica, proverom fizičkih lica, učesnika u poslovnim procesima, proverom ugovornih dokumenata, praćenjem realizacije ugovora u skladu sa utvrđenom dinamikom, upravljanjem procesima za otklanjanje poslovnih problema, smetnji i poteškoća, suzbijanjem koruptivnog i drugog neetičkog ponašanja zaposlenih i organizovanim merama za naplatu dospelih potraživanja[201].

Sa stanovišta opštih potreba top menadžmenta i poslovanja kreditnih institucija i investicionih kompanija, kao i korporacija koja se bave osiguranjem i reosiguranjem, prevencija gubitaka se može posmatrati i kroz prizmu upravljanja operativnim rizikom, a koji je prema propisima *EU (Regulation (EU) No 575/2013* i *Directive 2009/138/EC)* definisan kao rizik od gubitka po osnovu neadekvatnih ili neuspelih internih procesa, kadrova ili sistema ili usled eksternih događaja. Ističu se četiri glavna uzroka za definisanje operativnog rizika, a koji mogu poticati od različitih izvora i nosioca ugrožavanja: ljudski uzrok (neadekvatni resursi, ponašanje zaposlenih, interne krađe i prevare, nemotivisanost, zloba itd.); interna organizacija i procesi (sukob interesa, ljudske greške, nerazumevanje procesne šeme i dr.); informacioni sistemi (odliv informacija, prekid usluga, gubitak podataka, sajber bezbednost i sl.); spoljni uzroci (požar, terorizam, katastrofe, prevare, krađe i drugo). Ovi uzroci omogućavaju operativne (namerne i nenamerne) propuste, uključujući greške ili kašnjenja u obradi, zloupotrebe i druge nezakonite aktivnosti, ispade sistema, nedovoljne kapacitete, prevare, gubitak sredstava i podataka, odavanje informacija, pogrešno i ekonomski štetno ugovaranje poslova i druge pretnje, opasnosti i ranjivosti, koji, pored bezbednosnog, stvaraju i finansijski rizik, a mogu da naruše ugled i spreče organizaciju u dostizanju zacrtanih ciljeva. S obzirom da celoviti tretman operativnih rizika obuhvata i mere fizičke bezbednosti, upravljanje kontinuitetom poslovanja,

201 Stojanović Milan, Pavlović Dejan, op. cit., str. 119.

kontrole bezbednosti informacija i upravljanje incidentima, a shodno potrebama unutrašnje organizacije i drugim okolnostima, funkcija korporativne bezbednosti, pored uobičajenog delokruga, može biti nadležna i za poslove menadžmenta ukupnim operativnim rizicima kao merom prevencije gubitaka.

Poseban izazov predstavlja izgradnja optimalnog sistema prevencije gubitaka u maloprodaji, a imajući u vidu i visinu novčanih gubitaka koji se u evropskim okvirima kreće oko 1 – 1,5% od ukupnog prometa maloprodaja. Bez obzira na nedostatak preciznih podataka o obimu gubitaka u sektoru maloprodaje u RS, kao i zbog postojanja čitavog niz faktora koji negativno utiču na gubitke, svaka organizacija mora da bude svesna potrebe ulaganja u prevenciju, koju svakako ne sme posmatrati kao trošak. Ukoliko izuzmemo prirodne i tehničko-tehnološke izvore ugrožavanja (koji neophodno moraju biti tretirani), gubici u maloprodaji mogu nastati delovanjem svih nosilaca društvenog izvora ugrožavanja (unutrašnjih, spoljašnjih, kombinovanih), a oblici ugrožavanja su raznovrsni, uz porast broja sajber pretnji zbog sve zastupljenije e-trgovine. Pored kontrole gubitaka koji ne potiču od kriminalnih aktivnosti, odnosno koji nastaju usled grešaka zaposlenih, otpisom robe i prilikom realizacije drugih poslovnih procesa maloprodaje (pogrešne porudžbine vrste i količine robe, oštećenja robe, loša organizacija, kalo itd.), predmet angažovanja korporativne bezbednosti mora biti usmeren ka prevenciji inkriminisanih radnji - krađa, utaja, prevara, vandalizma i drugog. Radnje prevencije moraju biti holistički zastupljene, a za borbu protiv svakog od oblika ugrožavanja moraju da budu primenjene i specifične mere. Edukovani i visoko motivisani zaposleni u maloprodaji predstavljaju jedan od ključnih faktora bezbednosti, koji posebno mogu biti od koristi u prevenciji dela sitne krađe, kao specifične pretnje nad kojom je neophodno primeniti adekvatne zaštitne mere[202].

U izgradnji programa prevencije gubitaka od koristi mogu biti i podaci iz izveštaja o strategiji za otkrivanje i sprečavanje nedozvoljenih radnji na radnom mestu, koji naglašavajući veliki uticaj zaposlenih po gubitke organizacije, ukazuju i na elemente koje je potrebno da sadrži program kontrole gubitaka, a koji svakako zahteva angažovanje svih organizacionih celina korporacije, kao i aktivnu podršku top menadžmenta i drugih najviših organa u čijoj nadležnosti su upravljanje i donošenje strateških odluka[203].

202 Mandić J. Goran, *Osnovi sistema obezbeđenja pravnih lica*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd,, 2012., str. 445 – 472.

203 Videti više: *Strategies to Detect and Prevent Workplace Dishonesty*, Research Council CRISP Report, ASIS International Foundation, Alexandria VA, 2008.

Poslovno obaveštajno delovanje (Business Intelligence)

Izraz „*business intelligence*" potiče od Hauarda Dresnera, stručnjaka američke kompanije Gartner Group, koji ga je skovao 1989. godine u nameri da izvrši kategorizaciju metodoloških koncepata, kompjutertskih modela i tehnika koje mogu biti od koristi top menadžmentu kompanija u procesu odlučivanja. Taj termin se često pogrešno poistovećuje sa nelegalnom i tajnom poslovnom špijunažom, kao i sa pojmom *Competitive Intelligence*, koji se pojavio u Sjedinjenim Američkim Državama krajem 50-ih godina XX veka (smislio ga je Džerald Albaum koji je, istražujući američke elektroenergetske kompanije, zaključio da njihovi menadžeri raspolažu malim brojem informacija o klijentima, te je predložio uspostavljanje mehanizama kako bi donosioci odluka na osnovu pribavljenih informacija dobili odgovarajuća znanja o tome).[204] U teoriji postoji saglasnost u pogledu osnovnih ciljeva *Competitive Intelligence*, koji obuhvataju: otkrivanje pretnji koje poslovnom subjektu dolaze od konkurencije, eliminisanje ili ublažavanje uticaja mogućih iznenađenja, povećanje sopstvene konkurentske prednosti skraćivanjem vremena potrebnog za reakciju na pretnje i pronalaženje novih poslovnih prilika za korporaciju. Preovlađujući je stav da je *Competitive Intelligence* uži pojam, odnosno sastavni deo *Business Intelligence*.[205]

Izvan engleskog govornog područja postoji neusaglašenost oko prevođenja pojma *Business Intelligence (BI)*, zbog čega se isti uglavnom koristi u izvornom obliku. U domaćoj literaturi, medijima, oglasima koji nude te vrste usluga i stručnoj javnosti se često mogu čuti i izrazi kao što su "poslovno obaveštajno delovanje", "poslovna inteligencija",[206] "poslovno obaveštavanje", „poslovno istraživanje", „upravljanje poslovnim informacijama" i slično.

U odsustvu opšteprihvaćene definicije, može se oceniti da klasično poslovno obaveštajno delovanje ima sledeće odlike:

- to je proces legalnog i etičnog prikupljanja podataka i informacija koji nakon odgovarajuće obrade postaju znanje;

204 Albaum Gerald, *Competitive Intelligence*, C.I. Associates, Watertown MA 1959., pp. 16-19.

205 Fehringer Dale, Hohhof Bonnie (eds.), *Competitive Intelligence Ethics: Navigating the Gray Zone*, Competitive Intelligence Foundation, Alexandria VA 2006., p. 115.

206 U nekim jezicima se koristi više reči za određivanje sadržaja engleskog pojma „*intelligence*", koji inače može označavati i inteligenciju i obaveštajnu delatnost. Tako se u francuskom jeziku *intelligence* odnosi isključivo na ljudsku inteligenciju, dok se za obaveštajnu funkciju koriste druge reči, poput *renseignement*. Slično je i u nemačkom jeziku (*Nacrichten*).

- reč je o cikličnom procesu koji je usmeren na podatke i informacije pomoću kojih se mogu anticipirati procesi, događaji, akcije ili kretanja;
- u pitanju je instrument koji ima važnu ulogu u procesu donošenja odluka na nivou poslovnog subjekta.

S tim u vezi, osnovnim ciljem *Business Intelligence* smatra se uočavanje povoljnih poslovnih prilika, odnosno rano otkrivanje izvora ugrožavanja iz poslovnog i šireg okruženja kako bi menadžment kompanije imao dovoljno vremena za primerene protivakcije i otklanjanje opasnosti. Poslovno-obaveštajno delovanje obuhvata i analizu brojnih drugih činilaca, kao što su kretanja i trendovi na tržištu, ponašanje i navike kupaca, potencijalni procesi pripajanja i integracije, procena rizika ulaganja u određena područja i drugo.[207]

Uz ofanzivnu komponentu *Business Intelligence*, postoji i defanzivni, kontraobaveštajni aspekt (*Business Counterintelligence*), koji podrazumeva protivobaveštajno delovanje u poslovnom svetu, usmereno na ostvarenje bezbednosti kompanije i uspostavljanje mehanizama njene zaštite. U pitanju su aktivnosti iz domena korporativne bezbednosti kojima se teži eliminaciji ili smanjenju potencijalnih štetnih učinaka poslovno obaveštajnog delovanja konkurenata, kao i mere na zaštiti informacija poslovnog subjekta u odnosu na industrijsku špijunažu.[208] U tom smislu, osnovni ciljevi *Business Counterintelligence* su očuvanje pozicije korporacije u poslovnom okruženju, zaštita informacija poslovnog subjekta od industrijske špijunaže, procena mogućih opasnosti i pretnji i zaštita od nezakonitih i neetičkih nasrtaja drugih poslovnih subjekata. Sam izraz „kontraobaveštajno delovanje" može dovoditi do negativnih asocijacija jer implicira da se prema zaposlenima uspostavljaju izvesna ograničenja i nameću određena pravila ponašanja, što nije sasvim u skladu sa koncepcijom otvorenosti i slobode tržišta. Zbog toga ima sugestija da se umesto izraza "*counterintelligence*" upotrebljava termin "obezbeđenje sposobnosti kompeticije" (*competitive assurance*), kao neutralniji i podobniji.

U pogledu tradicionalnih tehnika i metoda poslovno obaveštajnog delovanja u procesu pribavljanja podataka i informacija, odnosno zona u okviru kojih se vrši njihovo prikupljanje, može se govoriti o tri različita područja: „bela zona", koju karakteriše primena legalnih i etički dopuštenih metoda i tehnika u postupku pribavljanja informacija; „siva zona", u okviru koje mogu biti primenjivane metode koje nisu u

207 Radun Viktor, *Konkurencija na nišanu – Teorijski i praktični aspekti istraživanja konkurencije*, HESPERIAedu, Beograd 2008., str. 95.

208 Prunckun Hank, *Counterintelligence Theory and Practice*, Rowman & Littlefield Publishers Inc., Lanham MD 2012., p. 29.

saglasnosti sa etičkim principima, ali koje nisu protivne zakonu, i „crna zona", koju odlikuje primena protivzakonitih i etici suprotnih sredstava i metoda. *Business Intelligence* se primarno vezuje za takozvanu „belu zonu", premda dosadašnja praksa svedoči da se pribavljanje podataka na ovaj način često odvija i unutar „sive zone". „Crna zona" je van okvira «poslovne inteligencije» i pripada području špijunaže.[209]

U načelu, postoje dva osnovna načina pribavljanja javno dostupnih podataka u klasičnom procesu poslovno obaveštajnog delovanja – primarni i sekundarni. U primarne izvore spadaju napredne internet pretrage, te javno dostupne publikacije poslovnih subjekata, finansijski izveštaji i drugi materijali vezani za poslovanje kompanija, izlaganja, intervjui, učešća na poslovnim događajima i manifestacijama i slično. U sekundarne izvore se mogu ubrojati različite elektronske baze podataka, stručna literatura, medijski sadržaji, analitički izveštaji i drugi dokumenti. Ovako prikupljeni podaci imaju relativno ograničene domete i značaj, jer se pre svega odnose na nešto što se već dogodilo, ili eventualno na stanje u sadašnjosti. Naime, da bi se došlo do kvalitetne poslovne odluke menadžmenta kompanije, potrebni su im podaci koji se neće odnositi samo na prošlo ili sadašnje vreme. To znači da su im neophodne i informacije koje sadrže namere, planove, procene i predviđanja stanja u budućnosti, zbog čega je u pribavljanju takvih podataka nezaobilazna uloga takozvanog „ljudskog izvora", a pre svega savremenih softverskih platformi, metodologija, alata i aplikacija koje teže prediktivnom analiziranju prikupljenih podataka.[210]

Business Intelligence se može koristiti za podršku širokom spektru operativnih i strateških poslovnih odluka. U tom kontekstu, osnovne operativne odluke uključuju pozicioniranje proizvoda i usluga ili određivanje njihovih cena. Strateške poslovne odluke uključuju prioritete, ciljeve i pravce delovanja poslovnog subjekta na najširem nivou. U svim slučajevima, poslovno obaveštajno delovanje je najefikasnije kada kombinuje podatke izvedene sa tržišta na kome kompanija posluje (spoljni podaci) sa podacima iz unutrašnjih izvora, kao što su interni finansijski i operativni podaci. Njihovo upoređivanje i nadgradnja mogu da pruže potpuniju sliku koja se ne može izvesti iz pojedinačnih skupova podataka.[211]

209 Klasan Vilko, „Poslovne izvjesnice i vojno-gospodarska diplomacija", *Polemos*, Vol. 14, No. 27, Hrvatsko sociološko društvo & Naklada Jesenski i Turk, Zagreb 2011., str. 83.

210 Sherman Rick, *Business Intelligence Guidebook – From Data Integration to Analytics*, Elsevier Inc., Waltham MA 2015., p. 376.

211 Coker Frank, *Pulse - Understanding the Vital Signs of Your Business*, Ambient Light Publishing, Bellevue WA, 2014, pp. 41–42.

Koncept *Business Intelligence* koji je sprovođen u proteklih nekoliko decenija ukazuje na cikličnu obaveštajnu aktivnost, koja uključuje nekoliko faza:

- planiranje i usmeravanje ukupnog ciklusa (*planning and direction*);
- proces prikupljanja podataka i saznanja (*collection*);
- selekciju i analiziranje prikupljenih podataka i informacija, te sačinjavanje finalnih analitičkih dokumenata (*processing and analysis*);
- dostavljanje sačinjenih obaveštajnih materijala i njihovo korišćenje od strane naručioca (*dissemination*).

Sve faze su uzajamno povezane i odvijaju se paralelno, pri čemu se sa okončanjem čitavog procesa ciklus ponavo odvija. Smatrano je da ovako koncipirano poslovno obaveštajno delovanje na pravi i efikasan način funkcioniše ako su ispunjeni sledeći kriterijumi:

- top menadžeri raspolažu osnovnim znanjima o procesu *Business Intelligence* i koriste dobijene rezultate u procesu donošenja i realizacije poslovnih odluka;
- na čelu organizacione jedinice za *Business Intelligence* se nalazi vrhunski stručnjak za to područje, koji uz to uživa poverenje top menadžera;
- organizaciona jedinica za poslovno obaveštajno delovanje kontinuirano deluje najmanje pet godina i čine je profesionalci odani svojoj kompaniji;
- *Business Intelligence* je deo poslovne kulture svih zaposlenih u korporaciji;
- operacije u procesu poslovno obaveštajnog delovanja se profesionalno planiraju i izvršavaju u skladu sa zakonskim i etičkim normama, poslovnom politikom, strategijom i planovima kompanije;
- organizaciona jedinica za poslovno obaveštajno delovanje na profesionalan način prikuplja podatke iz raspoloživih unutrašnjih i spoljnih izvora;
- analiza podataka daje odgovore na pitanja gde se korporacija nalazi u odnosu na poslovno okruženje i kakva joj je pozicija prema konkurentima i predviđa razvoj budućih događaja;
- kontinuirano se sprovode *Business Counterintelligence* operacije, s ciljem sprečavanja obaveštajnih operacija konkurentskih poslovnih subjekata, te zaštite intelektualne svojine i poslovnih informacija korporacije;

- u postupku prikupljanja, analiziranja, arhiviranja, pretraživanja i distribucije pribavljenih podataka i informacija koriste se savremene metodologije, IT aplikacije i plaforme.[212]

U današnje vreme, uporedo sa ekspanzivnim razvojem informacionih tehnologija, preovlađuju znatno restriktivnije definicije pojma *Business Intelligence*, po kojima je tu reč prvenstveno o upotrebi naprednih programa i metodologija za obradu podataka, kojima se na bazi relevantnih uzoraka otkrivaju uzroci problema i daju predviđanja poslovnih odluka. Iz toga proističe da težište više nije na prikupljanju podataka već na analitičkoj obradi velike količine informacija. Istovremeno se klasične definicije poslovno obaveštajnog delovanja kvalifikuju kao "Džems Bond *Business Intelligence*" i poistovećuju sa aktivnostima *Competitive Intelligence*, čiji je cilj dolaženje do informacija koje bi kompaniju učinile uspešnijom u odnosu na konkurenciju. Novije definicije i prakse koje iz njih proističu pod *Business Intelligence* podrazumevaju stratešku usmerenost modernih korporacija na razvoj i sintetizaciju softverskih alata i aplikacija namenjenih pribavljanju, selekciji, analiziranju i distribuciji informacija o poslovnom i širem okruženju i konkurenciji, radi unapređenja postupka donošenja odluka od strane top menadžmenta, a u cilju efikasnijeg poslovanja kompanije.[213] Primer ovakvog pristupa je definicija istraživačko-konsultantske firme *Forrester Research*, prema kojoj je poslovno obaveštajno delovanje

> *„skup metodologija, procesa, arhitektura i tehnologija koje transformišu sirove podatke u smislene i korisne informacije koje se koriste da bi se omogućio efikasniji strateški, taktički i operativni uvid i donošenje odluka."*[214]

U tom smislu, *Business Intelligence* obuhvata upravljanje informacijama (integraciju podataka, kvalitet podataka, skladištenje podataka, upravljanje glavnim podacima, analitiku teksta i sadržaja itd.). Samim tim, poslovno obaveštajno delovanje je krovni termin koji pokriva procese i metode prikupljanja, skladištenja i analize podataka iz poslovnih operacija ili aktivnosti radi optimizacije učinka.

Osavremenjeni pristup *Business Intelligence* se zasniva na strategijama, metodologijama i tehnologijama koje kompanije koriste za analizu podataka i upravljanje

212 Herring P. Jan, „World-Class Intelligence Programs", in: *Competitive Intelligence Magazine*, Vol. 10, No. 2, Issue 3, Alexandria VA, May-June 2006., pp. 20-24.

213 Stipanović Christian, „Izazovi poslovne inteligencije u turizmu", *UTM Revija*, Vol. 58, No. 5, UTM Revija, UT Ugostiteljstvo i turizam, Zagreb 2010., str. 32.

214 http://www.forrester.com/report/topic-overview-business-intelligence/RES39218

poslovnim informacijama.[215] U tom smislu, uobičajene funkcije BI tehnologija danas uključuju:

- Data Mining (korišćenje baza podataka, statistike i mašinskog učenja za otkrivanje trendova u velikim skupovima podataka);
- Data Warehouse (skladištenje podataka):
- Online Analytical Processing – OLAR (online analitička obrada),
- Benchmarking (uporedne procene),
- izveštavanje (deljenje analize podataka sa zainteresovanim stranama kako bi mogli da usvajaju zaključke i donose odluke),
- dolaženje do pokazatelja učinka i merenje poslovnih performansi (upoređivanje trenutnih podataka o učinku sa istorijskim podacima radi praćenja učinka u odnosu na ciljeve, obično koristeći prilagođene komandne table[216]);
- deskriptivnu analitiku (korišćenje preliminarne analize podataka da bi se saznalo šta se dogodilo);
- prediktivnu analitiku (preuzimanje istorijskih i aktuelnih podataka u realnom vremenu i modeliranje budućih ishoda u svrhe planiranja);
- preskriptivnu analitiku (obrada svih relevantnih podataka da bi se odgovorilo na pitanje: „Šta kompanija treba da čini?“)
- postavljanje upita vezanih za podatke i izvlačenje odgovore iz skupova podataka;
- statističku analizu (preuzimanje rezultata deskriptivne analitike i dalje istraživanje podataka pomoću statistike kao što je kako se određeni trend desio i zašto);
- vizuelizaciju podataka (pretvaranje analize podataka u vizuelne reprezentacije kao što su grafikoni, tabele i histogrami radi lakšeg korišćenja podataka);

215 Dedić Nedim, Stanier Clare, „Measuring the Success of Changes to Existing Business Intelligence Solutions to Improve Business Intelligence Reporting”, *10th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS)*, Vienna 2016, pp. 225–236.

216 Komandna tabla (*dashboard*) omogućava da se složeni podaci agregiraju i pregledaju na jednom mestu. Ključne karakteristike komandne table su: interaktivnost, podaci u realnom vremenu, prilagodljiv interfejs, standardni šabloni i sposobnost deljenja.

- vizuelnu analizu (istraživanje podataka kroz vizuelno pripovedanje kako bi se komunicirali uvidi u hodu i ostali u toku analize);
- pripremu podataka (objedinjavanje više izvora podataka, identifikovanje dimenzija i merenja i pripremanje za analizu podataka).

Alati i aplikacije *Business Intelligence* koriste podatke prikupljene iz skladišta podataka (*Data Warehouse - DW*) ili iz baza podataka, pri čemu se koncepti *BI* i *DW* kombinuju kao „*BI/DW*" ili kao „*BIDW*".[217] Skladišta podataka sadrže kopije analitičkih podataka koji olakšavaju podršku odlučivanju.

Prilikom odabira alata Business Intelligence, treba voditi računa o njihovim ključnim karakteristikama koje će biti od najveće pomoći poslovanju, uključujući: intuitivnost za upotrebu, raznovrsne opcije komandne table i vizuelizacije, pametne uvide, ugrađenu veštačku inteligenciju (AI), fleksibilnost primene, integraciju sa drugim platformama i aplikacijama, povezivanje podataka i ugradnju u poslovne aplikacije.

Savremenim softverskim rešenjima se kompanijama omogućava kreiranje korisnih informacija iz mnoštva podataka koji su disperzirani na različitim transakcijskim sistemima ili dolaze iz raznih internih i eksternih izvora.[218] S tim u vezi, najvažnije odlike poslovno obaveštajnog delovanja su vezane za sledeće:[219]

- osnovni cilj Business *Intelligence* je pružanje podrške i doprinos unapređenju procedura donošenja odluka top menadžmenta kompanije;
- donosiocima odluka se prezentuju samo informacije koje su im zaista neophodne, koje su blagovremene i koje su date u formi koja je najprikladnija za poslovno rukovodstvo;
- kroz proces selekcije obaveštajno interesantnih podataka, doprinosi se smanjenju kvantiteta informacija sa kojima se menadžeri poslovnog subjekta suočavaju, podižući istovremeno njihov kvalitet;
- poslovno obaveštajno delovanje predstavlja rezultat pažljivo usmeravanog i osmišljenog procesa kriranja novih ili otkrivanja prikrivenih znanja na osno-

217 Golden Bernard, *Amazon Web Services For Dummies*, John Wiley & Sons, Hoboken NJ, 2013., pp. 234-235.

218 Loshin David, *Business Intelligence: The Savvy Manager`s Guide*, Elsevier Inc., Waltham MA 2013., pp. 117-118.

219 Brijs Bert, *Business Analysis for Business Intelligence*, CRC Press, Boca Raton FL, 2016. pp. 125-127.

vu podataka koji se u poslovnom procesu kompanija kontinuirano generišu, eksploatišu, memorišu i upotrebljavaju;

- produkti *Business Intelligence* se prvenstveno izvode iz operativnih podataka korišćenjem adekvatnih logičko-analitičkih metoda;
- sprovođenje poslovno-obaveštajnog delovanja nameće kao neophodnost razvoj specijalizovanih informatičkih softverskih programa i hardverskih alata;
- *Business Intelligence* zahteva uspostavljanje koherentnog pristupa menadžmentu informacija i izgradnju jedinstvenog stava u pogledu njihovog značaja u poslovanju kompanije;
- za poslovno-obaveštajno delovanje je karakteristično globalno delovanje, kao i neopohodnost funkcionisanja u realnom vremenu.[220]

Danas postoje i brojni samouslužni softverski alati i platforme *Business Intelligence* koji pojednostavljuju proces analize. Ovo olakšava menadžerima i zaposlenima da vide i razumeju relevantne podatke i bez tehničkog znanja potrebnog za rudarenje podacima. Takođe, dostupne su i razne *BI* platforme za *ad hoc* izveštavanje, vizuelizaciju podataka i kreiranje prilagođenih komandnih tabli za više nivoa korisnika.

Kada je reč o problemima sa kojima se poslovno obaveštajno delovanje suočava, treba imati u vidu činjenicu da same poslovne operacije generišu veliku količinu različitih podataka u obliku email-ova, beležaka, vesti, komunikacije na društvenim mrežama i platformama, izveštaja, veb-stranica, prezentacija, foto i video datoteka, marketinških materijala i drugog. Prema *Merrill Lynch*-u, više od 85% svih poslovnih informacija egzistira u ovim oblicima, pri čemu kompanija može koristiti takav dokument samo jednom.[221] Zbog načina na koji se proizvode i čuvaju, ovakve informacije su ili nestrukturirane ili polustrukturirane. Upravljanje takvim podacima je još uvek nerešen problem u području informacionih tehnologija s obzirom na procenu da se 30–40% radnog vremena troši u traženju, pronalaženju i procenjivanju nestrukturiranih podataka.

220 Burns Larry, *Growing Business Intelligence – An Agile Approach to Leveraging Data and Analytics for Maximum Business Value*, Technics Publications, Basking Ridge NJ 2016., pp 103-105.

221 Rao Ramana, "From unstructured data to actionable intelligence", *IT Professional*, Vol. 5, Issue 6, IEEE Computer Society, Washington DC 2003, pp. 29–35.

Business Intelligence se koristi i strukturiranim i nestrukturiranim podacima. Prve je lako pretraživati, a drugi sadrže veliku količinu informacija potrebnih za analizu i donošenje odluka. Zbog poteškoća pravilnog pretraživanja, pronalaženja i procene nestrukturiranih ili polustrukturiranih podataka, u praksi se može desiti da ogromne baze informacija ne budu iskorišćene iako bi mogle uticati na određenu odluku, zadatak ili projekat, što na na kraju može dovesti do odluke zasnovane na lošoj ili nedovoljnoj informisanosti.

Izazovi vezani za korišćenje polustrukturiranih i nestrukturiranih podataka u poslovno obaveštajnom delovanju se tiču fizičkog pristupa nestrukturiranim tekstualnim podacima (čuvaju se u velikom broju formata), terminologije (postoji potreba za razvojem standardizovane terminologije), obima (otežana mogućnost analize od reči do reči i semantičke analize), te ograničene mogućnosti pretraživanja nestrukturiranih tekstualnih podataka.[222] Takođe, postoje i ograničenja u aktuelnoj fazi razvoja *Natural language processing (NLP)* i primene veštačke inteligencije.[223]

Na tragu razrešenja ovih problema su najnoviji *BI* alati, dizajnirani da omoguće lako tumačenje *Big Data*,[224] koji su u stanju su da efikasno obrađuju velike količine strukturiranih i nestrukturiranih podataka.

Za rešavanje problema povezanih sa pretraživošću i procenom podataka potrebno je nešto znati i o njihovom sadržaju. Ovo se može rešiti dodavanjem konteksta kroz korišćenje metapodataka. Mnogi poslovni sistemi već snimaju neke metapodatke (npr. ime datoteke, autor, veličina, itd.), ali bi korisniji bili metapodaci o stvarnom sadržaju, na primer sažeci, teme, lica ili kompanije koji se pominju. Najpoznatije savremene tehnologije dizajnirane za generisanje metapodataka o sadržaju su automatska kategorizacija i ekstrakcija informacija.

Alati *Business Intelligence* su donedavno bili zasnovani na tradicionalnom modelu poslovne inteligencije. To je bio pristup odozgo nadole, gde je čvorišna tačka poslovno obaveštajnog delovanja bila organizaciona jedinica za IT, i gde je na većinu, ako ne i na sva analitička pitanja odgovarano putem statičnih izveštaja. U praksi,

222 Feldman David, Himmelstein Jason, *Developing Business Intelligence Apps for SharePoint*, O'Reilly Media, Inc., Sebastopol CA 2013, pp. 140–143.

223 Blumberg Robert, Atre Shaku, "The Problem with Unstructured Data", *DM Review*, Daman Consulting, Austin TX 2003, pp. 42–46.

224 Big Data je pojam koji označava velike i kompleksne setove podataka, kod kojih tradicionalne aplikacije za obradu podataka nisu primenljive. Te skupove podataka karakterišu raznovrsnost formata, velike brzine obrade i pristupa i veliki obim informacija. Konkretno, obim je ono na šta ljudi obično ukazuju kao glavni faktor koji određuje, pošto se količina podataka stalno povećava i relativno je lako pohraniti u dugim vremenskim periodima.

ako bi neko imao naknadno pitanje u vezi sa dobijenim izveštajem, taj zahtev bi otišao na dno reda za prijavljivanje i proces bi morao da se započne iznova. To je dovodilo do sporih, frustrirajućih ciklusa izveštavanja, a korisnici često nisu bili u mogućnosti da iskoriste trenutne podatke za donošenje odluka.

Tradicionalni *Business Intelligence* je i dalje uobičajeni pristup za redovno izveštavanje i odgovaranje na statične upite. Međutim, savremeno poslovno obaveštajno delovanje je interaktivno i pristupačno. Iako su IT odeljenja i dalje važan deo upravljanja pristupom podacima, više nivoa korisnika je sada u stanju da prilagodi kontrolne table i da kreira izveštaje bez najave. Uz odgovarajući softver, korisnici su ovlašćeni da sami vizualizuju podatke i dobiju odgovore na svoja pitanja.

Po svojoj suštini, *Business Intelligence* ne treba da bude linearan proces jer će odgovor na jedno pitanje neizostavno dovesti do naknadnih pitanja i ponavljanja. Umesto toga, u pitanju je proces kao ciklus pristupa podacima, otkrivanja, istraživanja i deljenja informacija (analitički ciklus). Međutim, treba imati u vidu da nijedan napredni softver ne može sam po sebi dati odgovore na pitanja zbog čega treba prikupljati podatke, analitički ih obrađivati i korisnicima dostavljati finalni proizvod, kakvog to ima smisla za kompaniju, te kako tako stečeno znanje pretvoriti u akciju top menadžmenta.

Ključni zahtevi krajnjih korisnika na koje poslovno-obaveštajno delovanje u današnjem i budućem vremenu mora da ima spreman odgovor su:

- raspoloživost u realnom vremenu, odnosno spremnost da se krajnji korisnik snabde relevantnim informacijama koje treba da služe kao osnov za pravilno odlučivanje menadžmenta, a s ciljem obezbeđenja konkurentnosti kompanije na tržištu;
- prilagodljivost i fleksibilnost, što znači posedovanje kapaciteta za analitičku obradu prikupljenih podataka radi uspešnog postavljanja poslovnog subjekta u odnosu na izazove dinamičnog tržišta;
- sposobnost *Business Intelligence* i sistema skladištenja podataka da iznađe adekvatne odgovore na brojčanu multiplikaciju podataka i na rastući broj krajnjih korisnika na ovaj način dobijenih poslovnih informacija;
- usmerenost ka postizanju sve viših nivoa dostignutog znanja i veština pripadnika tima koji realizuje proces poslovno-obaveštajnog delovanja, odnosno ka iznalaženju sve manje komplikovanih softverskih rešenja kako bi se što olakšala njihova primena u praksi;

- bezbednost, to jest sposobnost da se efikasno zaštite uspostavljene baze podataka od neovlašćenog korišćenja, pristupa, kopiranja i krađa;
- trajna orijentacija prema stručnom osposobljavanju, obuci, permanentnom obrazovanju zaposlenih i afirmisanju unutrašnjeg intelektualnog kapitala, kao ključnih resursa poslovnog subjekta.
- kontinuirani razvoj *Business Intelligence* kako bi se održao korak sa poslovnim potrebama i tehnologijom, što se posebno odnosi na veštačku inteligenciju čije će uvide kompanije moći da integrišu u širu *BI* strategiju.[225]

Iako je proces *Business Intelligence* vezan za poslovni subjekt u okviru koga se sprovodi, poslovno obaveštajno delovanje ima određene implikacije i u domenu nacionalne bezbednosti. Taj uticaj postoji prvenstveno u sferi javnih, odnosno opštih interesa vezanih za postizanje unutrašnjeg privrednog blagostanja, visokog stepena ekonomskog razvoja, zaposlenosti i standarda u državi, s obzirom da uspešno poslovanje pojedinačne kompanije doprinosi povećanju nacionalnog bruto proizvoda, te ukupnom rastu nacionalne ekonomije.

Unutrašnje kontrole i istrage

Unutrašnje kontrole

Sve politike, procesi, mere i drugi elementi sistema korporativne bezbednosti moraju da budu izloženi stalnoj kontroli, nadzoru i reviziji. Zbog nekonzistentnog korišćenja pojmova u literaturi i zakonskoj regulativi, kao i usled neujednačenog prevođenja sa nekog od stranih jezika (najčešće engleskog), a kako u praksi ne bi stvaralo zabunu, smatramo da je poželjno razgraničiti značenje i ulogu pojmova unutrašnje (interne) kontrole/provere, nadzora i revizije u funkciji korporativne bezbednosti.

Pre svega, potrebno je imati u vidu da se pojam kontrola (eng. *control*) u bezbednosnoj literaturi, standardima i praksi odnosi na meru kojom se modifikuje rizik[226]. U tom smislu kontrola može uključivati proces, politiku, uređaj, praksu ili drugu radnju kojom se utiče na rizik. Zato se i u ovom Priručniku pojam „kontrola“ upo-

225 Brijs Bert, *Business Analysis for Business Intelligence*, op. cit. pp. 252-253.

226 Pogledati u delu termina i definicija standarde *ISO Guide 73*, *ISO/IEC 27000*, *ISO 22300* i dr.

trebljava u kontekstu navođenja administrativnih, operativnih, tehničkih, fizičkih, pravnih i drugih mera i radnji za upravljanje bezbednosnim rizikom.

Za razliku od prethodno navedenog pojma kontrole, izraz koji se obično koristi i prevodi kao „unutrašnja kontrola/provera" (eng. *internal control/audit*) predstavlja vid provere i „kontrole" nad nekim sistemom, procesom ili radnjom. U tom smislu se unutrašnja kontrola/provera u okviru funkcije korporativne bezbednosti može posmatrati kao zakonska obaveza, formalni zahtev bezbednosnih standarda ili kao vid dobre prakse. Naglašavamo da neusaglašen ili nefunkcionalan sistem unutrašnjih kontrola predstavlja povoljan ambijent za sprovođenje prevara i drugih zloupotreba i štetnih radnji.

Zakonska obaveza upućuje na neophodnost organizovanja, pa i određivanja organizacionih celina ili pojedinaca u funkciji sprovođenja unutrašnje kontrole. Primera radi, *Zakon o tajnosti podataka* obavezuje ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za poslove odbrane i Bezbednosno-informativnu agenciju, a po potrebi i drugi organ javne vlasti, da za unutrašnju kontrolu i druge stručne poslove u vezi sa određivanjem i zaštitom tajnih podataka sistematizuje posebno radno mesto, ili da za obavljanje ovih zadataka i poslova posebno zaduži postojeću organizacionu jedinicu. Rukovodilac organa javne vlasti odgovoran je za izgradnju adekvatnog sistema unutrašnje kontrole nad sprovođenjem ovog zakona i propisa donetog na osnovu ovog zakona, a shodno *Uredbi o posebnim merama nadzora nad postupanjem sa tajnim podacima*[227] unutrašnja kontrola prema načinu vršenja može biti najavljena ili nenajavljena, a prema obimu, potpuna ili delimična. I ostala podzakonska akta zahtevaju sprovođenje provera sa ciljem utvrđivanja efikasnosti preduzetih mera zaštite i potrebnog nivoa bezbednosti tajnih podataka. Iako neprecizira način na koji se sprovodi, i *Zakon o privatnom obezbeđenju* određuje da pravno lice kome pripadaju objekti od posebnog značaja za odbranu zemlje, samozaštitnu delatnost uredi na način da, pored planske i organizacione, ima organizovanu i kontrolnu funkciju. I *Zakon o informacionoj bezbednosti* ukazuje na neophodnost vršenja provere, i to provere[228] usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema za operatore IKT sistema od posebnog značaja, kao i na obavezu određivanja posebnog lica, odnosno organizacione jedinice za internu kontrolu za samostalne operatore IKT sistema. Uostalom, sva privredna

227 „Službeni glasnik RS", br. 90/2011.

228 Način provere uređen je *Uredbom o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja*, „Službeni glasnik RS", br. 94/2016.

društva i drugi oblici organizovanja imaju obavezu shodno *Zakonu o privrednim društvima* da sprovode kontrolu usklađenosti poslovanja društva sa zakonom, drugim propisima i aktima društva, proveru sprovođenja politika upravljanja rizicima i vrednovanje politika i procesa u društvu, kao i predlaganje njihovog unapređenja. Uzimajući u obzir i *Principe 23, 24 i 25 Kodeksa korporativnog upravljanja*, funkcija korporativne bezbednosti je dužna da u okviru sistema internih kontrola na nivou cele organizacije uspostavi i razvija „podsistem" internih kontrola iz svog delokruga, kao i da ih neprestano, redovno, u utvrđenim periodima, ispituje, ocenjuje i unapređuje u funkciji održavanja bezbednosnih rizika u nivou opredeljene prihvatljivosti i uz što manje ukupne troškove, obezbeđujući top menadžmentu i drugim organima sigurnost u ostvarivanju bezbednosnih ciljeva.

U smislu zahteva bezbednosnih standarda unutrašnja kontrola/provera predstavlja sistematičan, nezavisan i dokumentovan proces za pribavljanje dokaza provere i njegovu objektivnu procenu kako bi se utvrdilo u kojoj meri su kriterijumi provere ispunjeni, a koju organizacija sama sprovodi (ili eksterna strana u njeno ime) za potrebe rukovodstva i druge interne svrhe, i može predstavljati osnovu za samodeklarisanje organizacije o usklađenosti sa zahtevima standarda[229]. Internu proveru politika, procesa, procedura i drugih elemenata sistema menadžmenta bezbednošću treba nezavisno preispitivati u planiranim intervalima, ili kada nastupe značajne izmene u implementaciji bezbednosnih mera i radnji. Po pravilu, preispitivanje treba da sprovode pojedinci koji su nezavisni od oblasti koja se preispituje, a potrebno je da imaju odgovarajuće znanje i iskustvo, kao i da su obučeni za internog proveravača.Vodeći računa da se neupadne u zamku preteranog formalizma, pomoć u načinu sprovođenja interne provere može da pruži *Uputstvo za proveravanje sistema menadžmenta*[230], dok za sprovođenje provera određenih poslova iz funkcije korporativne bezbednosti postoje i zasebne smernice, kao u slučaju sistema upravljanja bezbednošću informacija gde su nam na usluzi smernice za proveru sistema *ISO/IEC 27007*[231] i za procenu kontrola bezbednosti informacija *ISO/IEC TS 27008*[232].

Ovako shvaćen pojam unutrašnje kontrole/provere ne sme se poistovećivati sa nadzorom (eng. *monitoring*) koji šire posmatrano predstavlja način ukupnog spro-

229 O pojmu unutrašnje kontrole/provere pogledati u delu termina i definicija standarda *ISO 28000*, *ISO 22300* i dr.

230 *ISO 19011:2018, Guidelines for auditing management systems.*

231 *ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.*

232 *ISO/IEC TS 27008:2019, Information technology — Security techniques — Guidelines for the assessment of information security controls.*

vođenja i organizaciju rada unutrašnjeg nadzora poslovanja korporacije, uključujući unutrašnje kontrole/provere i internu reviziju. U užem smislu nadzor predstavlja određivanje statusa sistema, procesa ili aktivnosti, a može uključivati kritičko posmatranje i superviziju. Predstavlja stalnu, svakodnevnu aktivnost na proveri, nadgledanju, posmatranju ili utvrđivanju statusa kako bi se identifikovala promena u odnosu na nivo učinka koji je potreban ili očekivan, a primenjuje se na svaki poslovni okvir, proces, proceduru rada, rizik ili kontrolu.

Ko kontroliše kontrolore? - je šaljivo pitanje kojim se želi ukazati na značaj izgradnje slojevitog, unakrsnog i nezavisnog sistema unutrašnje kontrole i nadzora. U okviru korporacije još jedan vid kontrole procesa i poslovanja jeste interna revizija (eng. *internal audit*) koja ima za cilj da sagleda da li su način upravljanja rizicima i način kontrole procesa, kao i rukovođenja tim procesima, adekvatni, odnosno da li se sistem uspostavljenih unutrašnjih kontrola stalno unapređuje i da li funkcioniše na odgovarajući način. Sagledavajući kroz prizmu prihvaćenog modela upravljanja rizicima (tzv. „model tri linije odbrane"), interna revizija predstavlja treću liniju procene aktivnosti upravljanja rizikom, zadužena za nezavisno razmatranje i prve i druge linije odbrane i objektivan prikaz efektivnosti uspostavljenih internih kontrola (u našem slučaju bezbednosnih).

Unutrašnje istrage

Zbog sličnosti se često u praksi ne pravi dovoljna razlika između prethodno navođenih termina - unutrašnja kontrola, nadzor i revizija – procesa prevashodno proaktivnog karaktera, sa pojmom unutrašnje istrage, kao funkcijom pretežno reaktivne prirode. Posebno se poistovećuje interna revizija sa istragom, koje iako slične po izgledu, različite su po prirodi, imaju drugačiju strukturu i standarde. Interna revizija je dizajnirana da proaktivno otkrije indikacije kršenja normi i zahteva u procesima i radnjama gde analiza ukazuje da je rizik od prestupa značajan. Istraga se sastoji od prikupljanja dovoljno informacija o specifičnim detaljima i sprovođenja onih procedura koje su neophodne da bi se utvrdilo da li je došlo do prestupa, gubitka ili izloženosti u vezi sa prestupom, ko je bio umešan i kako se dogodilo. Osnovni zadatak unutrašnje istrage je otkrivanje, utvrđivanje okolnosti i prikupljanje dokaza vezanih za bezbednosne incidente, događaje i srodna pitanja, prilikom čega može da se koriste i nalazi sprovedenih unutrašnjih kontrola, nadzora i revizija.

Preduzimanje mera na utvrđivanju okolnosti je i zakonska obaveza organizacija iz reda organa javne vlasti, kao, primera radi, u slučaju saznanja da je došlo do gubit-

ka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnih podataka i stranih tajnih podataka. Tom prilikom je, shodno *Zakonu o tajnosti podataka*, neophodno preduzeti sve potrebne mere za utvrđivanje okolnosti zbog kojih je došlo do gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka, izvršiti procenu prouzrokovane štete, kao i preduzeti potrebne mere u cilju otklanjanja štete i sprečavanja ponovnog gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja. Istraga treba da ide u pravcu preduzimanja aktivnosti radi utvrđivanja činjenica koje su uzrokovale povredu tajnosti, kao i aktivnosti na njihovom otklanjanju. Slično je i u slučaju povrede podataka o ličnosti, poslovne tajne ili narušavanja bezbednosti ostalih podataka i informacija, pa i prilikom saznanja o kršenju propisa, opasnosti po život, javno zdravlje, bezbednost, životnu sredinu i drugih štetnih radnji shodno *Zakonu o zaštiti uzbunjivača*. Način prijave, preduzimanje određenih radnji u cilju provere informacije i druga pitanja od značaja za unutrašnje uzbunjivanje uređeno je *Pravilnikom o načinu unutrašnjeg uzbunjivanja, načinu određivanja ovlašćenog lica kod poslodavca, kao i drugim pitanjima od značaja za unutrašnje uzbunjivanje kod poslodavca koji ima više od deset zaposlenih*[233]. Kako bi što efikasnije došla do saznanja o ovim i drugim kršenjima normi i nastaloj šteti, kao inicijalnoj fazi procesa unutrašnje istrage, neophodno je da organizacija, kao što smo i ranije naveli, izgradi različite vidove linija komunikacije i dojave kako bi prijavljivanje bilo moguće ne samo od strane zaposlenih, već i od kupaca, odnosno korisnika usluga, dobavljača, ali i anonimnih lica[234].

Pored zaštite sopstvenih resursa unutrašnje strukture korporativne bezbednosti u pojedinim kompanijama planiraju, organizuju i u formi privatno-javnog partnerstva realizuju relativno složene bezbednosne operacije koje podrazumevaju prikupljanje informacija, utvrđivanje činjenica, ali i pribavljanje dokaza o izvršenim proneverama, krađama, koruptivnim aktivnostima kao i drugim vidovima zloupotreba, ne samo od strane zaposlenih, već i od aktivnosti nelojalne konkurencije, kao i u cilju sprečavanja crnog tržišta i nelegalnog prometa dobara[235]. U tom smislu neophodno je uspostavljanje saradnje sa inspekcijskim organima, MUP-om

233 "Službeni glasnik RS", br. 49/2015 i 44/2018 - dr. zakon.

234 Kao primer smernica za način organizacije, planiranje, sprovođenje i druge aspekte unutrašnjih istraga pogledati publikaciju nemačkog saveznog udruženja za bezbednost poslovanja: *Leitplanken – Interne Ermittlungen*, ASW Bundesverband, Berlin DE 2021.

235 U sprečavanju crnog tržišta, nelegalnog prometa, aktivnosti nelojalne konkurencije, onemogućavanju nesavesne realizacije zaključenih ugovora i istraga drugih zloupotreba, poznati su iz medija i prakse primeri aktivnosti službi korporativne bezbednosti organizacija duvanske industrije, kompanija za promet nafte i dugih energenata, rudarskih i drugih kompanija.

i drugim relevantnim državnim organima i resornim institucijama, zasnovane na sadržajnim protokolima i implementiranim u svakodnevnoj operativnoj praksi. Na taj način relaksira se rad javnih službi nadležnih za sprovođenje zakona i olakšava rad pravosudnih organa, a kompanija je u dobitku jer ovakvim akcijama doprinosi sprovođenju zakona, suzbijanju korupcije i kriminala i uspostavljanju etičkih pravila ponašanja. Najneposrednije se štiti interes građana, potrošača jer se obezbeđuje da za uloženi novac dobiju robu i usluge potrebnog kvaliteta i kvantiteta.

Međutim, u okviru privatno-javnog partnerstva procesi su složeniji zbog logičnog pitanja eventualnog neovlašćenog posedovanja ili zadržavanja pojedinih informacija koje imaju širi ili javni značaj. Poslovna praksa rada uspešnih službi korporativne bezbednosti izdiferencirala je pojedine granične situacije kada bezbednosni problem nije više isključivo deo poslovnog života kompanije i kada je nužno inicirati poluge privatno-javnog partnerstva. To su pre svega situacije: kada se na ekspertskom nivou usaglasi sumnja u određene elemente krivičnog dela; kada se kao učesnik bezbednosno negativnih pojava ili procesa u kompaniji pojavi lice van kompanije, a posebno ako je pripadnik javnog sektora; kada se u radu na ostvarivanju bezbednosti kompanije dođe do informacija koje nemaju značaj za poslovanje, ali postoji zakonska obaveza prijavljivanja ili drugi javni interes.

Za razliku od državnih istražnih organa koji za primarni cilj imaju zaštitu društva, unutrašnja istraga prioritetno štiti organizaciju, uz nepostojanje jasnog zakonskog okvira i načina sprovođenja. I zato što je potrebna znatna količina kreativne mašte, mnogi istragu poistovećuju sa umetnošću, ali je svakako potrebno pridržavati se i pravila kriminalistike, psihologije, informacione tehnologije, logike i drugih znanja i veština potrebnih za valjano prikupljanje podataka i informacija, koje ukoliko je potrebno, mogu da posluže kao dokaz radi pokretanja disciplinskog, prekršajnog ili drugog postupka. Da bi dobili odgovore na osnovna pitanja istrage: šta, ko, gde, kada, kako, zašto – vezanim za stanja, incidente, događaje ili delovanja koja su protivpravna ili se smatraju neprihvatljivim, suprotna organizacijskim ciljevima i štetna (od istrage lažnih bolovanja, seksualnog uznemiravanja, korišćenja psihoaktivnih supstanci i drugih povreda radne discipline, do razotkrivanja raznih vidova prevara, korupcije, krađe, proizvodne štete, uticaja nelojalne konkurencije i dr.), bitno je dobro poznavanje organizacije i sistematizacije poslova, procesa i procedura, a neophodno je fazno obavljati raznorodne radnje koje obično uključuju sprovođenje intervjua (sa potencijalnim svedocima, mogućim saučesnicima, osumnjičenima i dr.), prikupljanje dokaza (iz internih dokumenata, eksternih javnih evidencija, siste-

ma video obezbeđenja, IKT sistema i dr.), analize dokaza, razvoja i testiranja hipoteza, do sačinjavanja konačnog izveštaja sa predlogom preporuka i mera.

S obzirom da se poslovanje mnogih organizacija sve više bazira i zavisi od informaciono-komunikacionih tehnologija, a po uzoru na obaveze operatore IKT sistema od posebnog značaja (može se poistovetiti sa kritičnom infrastrukturom) shodno Zakonu o informacionoj bezbednosti i podzakonskim aktima, potrebno je definisati i primenjivati procedure koje trebaju da obezbede procese za identifikaciju, prikupljanje i čuvanje informacija koje mogu da posluže kao dokaz radi pokretanja disciplinskog, prekršajnog ili krivičnog postupka. Kako bi se obezbedila prihvatljivost dokaza (da se mogu koristiti) i da bi imali težinu (kvalitet i kompletnost dokaza) potrebno je da organizacija osigura da su njeni informacioni sistemi u skladu s nekim od objavljenih standarda ili s pravilima prakse. Bez obzira da li se kompjuterska ili digitalna forenzika obavlja interno ili eksterno, neophodno je pridržavati se principa, standarda, kriterijuma i procedura za skupljanje, kopiranje (istraživanja treba raditi samo na kopijama dokaznog materijala), čuvanje (treba zaštititi integritet dokaznog materijala), transport i analizu digitalnih dokaza, a u nedostatku nacionalnih, poželjno je koristiti međunarodno prihvaćene standarde kao što su one objavljene od strane *SWGDE*[236] i *IOCE*[237]. Zbog prirode napada, kontinuirane latentne pretnje i specifične ranjivosti informacija i IKT sistema korporativna istraga u oblasti kompjuterskog kriminala ima poseban značaj[238].

Kao pomoć u istragama, naročito u slučaju kompjuterskih i finansijskih prevara i forenzici, mnoge korporacije i druge organizacije koriste usluge specijalizovanih firmi, a za istražne i detektivske usluge organizacija može da ugovorno angažuje pravna lica i preduzetnike licencirane za detektivsku delatnost u skladu sa *Zakonom o detektivskoj delatnosti*. Takve usluge se realizuju u cilju prikupljanja, obrade podataka i prenosa informacija koji se obično odnose na: lica koja su korisniku usluge prouzrokovala štetu (ako su ispunjeni zakonom utvrđeni uslovi odgovornosti za štetu); lica koja anonimno i protivpravno postupaju prema korisniku usluge, sa ili bez izazivanja štetnih posledica; predmete koji su izgubljeni ili ukradeni; uspešnost poslovanja pravnih lica i preduzetnika; zaštitu intelektualne i industrijske svojine; povrede radnih obaveza ili radne discipline.

236 *Scientific Working Group on Digital Evidence.*

237 *International Organization on Computer Evidence.*

238 Videti šire: Milutinović Miroslav, *Korporativna bezbednost*, Visoka škola strukovnih studija za kriminalistiku i bezbednost, Niš, 2011.

Naglašavamo da je, bez obzira da li se istraga sprovodi samostalno ili angažovanjem pružaoca usluga, bitno da se informacije i dokazi pribavljaju i kreiraju na zakonit i etički korektan način, a jedan od osnovnih principa je princip zakonitosti koji, pored ostalog, podrazumeva da zakonito postupanje i opšti javni interes imaju prednost nad partikularnim kompanijskim interesom, koji u pojedinim situacijama može biti neopravdano favorizovan. Princip direktivnosti, karakterističan za veće kompanije, koje inače i organizuju funkciju korporativne bezbednosti kao sastavnog dela top menadžmenta, podrazumeva striktno poštovanje standarda, pravilnika i svih drugih normativno-metodoloških dokumenata koji su odgovarajućim šablonima integrisani u oficijelni poslovni informacioni sistem i nezavisno od volje učesnika i vlasnika procesa onemogućavaju bilo kakvu proizvoljnost u postupanju. I konačno, na nivou funkcije korporativne bezbednosti se ne donose nikakve odluke koje imaju izvršnu snagu. Krajnji domet rada ove funkcije u kompaniji je informisanje top menadžmenta ili nadležnih državnih organa.

Treće poglavlje

Holistički princip menadžmenta korporativnom bezbednošću

Sadržaj poglavlja

Sistem menadžmenta korporativnom bezbednošću

Postojanje adekvatne organizacije poslova i izgradnja valjanog upravljačkog sistema jedni su od ključnih faktora uspešnog poslovanja svakog pravnog lica. Zbog toga što od organizacionog i upravljačkog aspekta značajno zavise svi ostali elementi i ukupno poslovanje kompanije, posebno je bitno voditi računa o načinu organizacije poslova, uključujući i onih iz delokruga korporativne bezbednosti, kao i o metodi izgradnje, održavanja i razvoja sistema upravljanja/menadžmenta[1], čiji je neizostavni deo i sistem menadžmenta bezbednošću. Stoga je i osnovi zadatak menadžera korporativne bezbednosti rad na izgradnji i upravljanje sistemom bezbednosti, kao i staranje o njegovoj poziciji i efikasnosti u okviru celovitog sistema upravljanja korporacijom.

1 Prema standardu osnova i rečnika sistema menadžmenta kvalitetom (*ISO 9000:2015, Quality management systems - Fundamentals and vocabulary*), sistem menadžmenta (eng. *management system*) predstavlja skup međusobno povezanih ili zavisnih elemenata organizacije za uspostavljanje politika i ciljeva, i procesa za postizanje tih ciljeva.

Definiciju sistema menadžmenta bezbednošću (eng. security management system) možemo preuzeti iz standarda kojim se specificiraju zahtevi za taj sistem - *ISO 28000*[2] - prema kome on predstavlja

> *„sistem koordinisanih politika, procesa i praksi kroz koje organizacija upravlja svojim bezbednosnim ciljevima".*

Naglašavamo da nepostoji jedinstven, univerzalni način izgradnje sistema menadžmenta bezbednošću, ali složićemo se da rešavanje bezbednosnih pitanja, uzrokovanih neizvesnosnim i nestabilnim okruženjem, iziskuje sistematski pristup, a koji se najtransparentnije razvija primenom priznatih standarda (za koje smo i ranije naveli da predstavljaju sublimiranu najbolju praksu). Funkcija korporativne bezbednosti trebala bi da primenjuje i objedinjeno upravlja sistemima koji su uređeni srodnim standardima menadžmenta, tj. Onim najviše strukture iz njenog delokruga (npr. menadžment sistemom kontinuiteta poslovanja - *ISO 22301*, bezbednošću informacija - *ISO/IEC 27001*, protiv mita - *ISO 37001* itd.), uključujući sektorske, granske i druge standarde (bez obzira da li se odnose na sistem menadžmenta sveukupnom ili parcijalnom bezbednošću), a tangiraju delatnost organizacije (npr. sistem menadžmenta uslugama privatnog obezbeđenja - *ISO 18788*[3], upravljanje procesima bezbednosne štampe - *ISO 14298*[4], bezbednost usluga transporta - *TAPA TSR*[5] i sl.).

Korporativna bezbednost ostvaruje prednost i uštedu organizaciji jedinstvenim upravljanjem, između ostalog i putem konvergencije i integracije bezbednosnih poslova. Takav pristup je potreban, pre svega, zbog veće sposobnosti ublažavanja multi rizika, a posebno prilikom reagovanja na različite bezbednosne incidente i događaje, kada preklapanje funkcija može usporiti odgovor, kao i otežati i poskupeti oporavak. Ako ni zbog čega drugog, benefiti konvergencije se ogledaju u olakšanom izveštavanju i uvidu u stanje ukupne bezbednosti od strane top menadžmenta, koji pomno prati efikasnost procesa i izuzetno vodi računa o budžetu i (nepotrebnim) troškovima[6]. Podrazumeva se da je sistem menadžmenta bezbednošću sastavni deo (podsistem) integrisanog sistema menadžmenta - *IMS* (eng. *Integrated Management System*), ko-

2 *ISO 28000:2022, Security and resilience - Security management systems – Requirements.*

3 *ISO 18788:2015, Management system for private security operations - Requirements with guidance for use.*

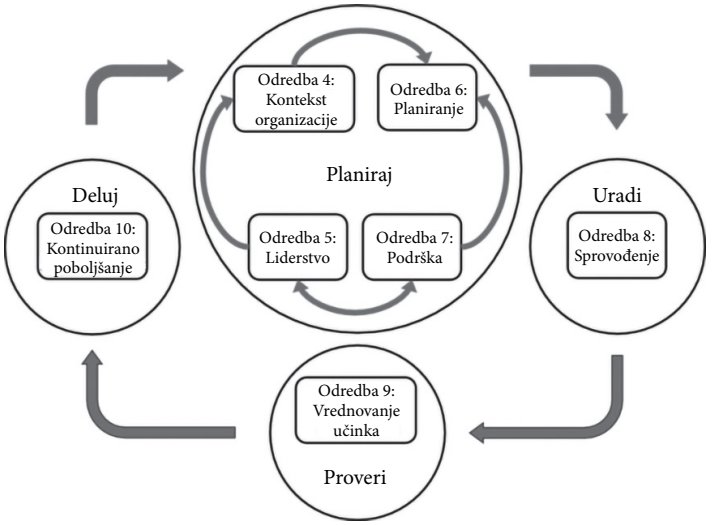
4 *ISO 14298:2021, Graphic technology, Management of security printing processes.*

5 *Trucking Security Requirements(TSR) 2017*, TAPA Standards, Boca Raton FL 2017.

6 O benefitima konvergencije poslova bezbednosti pogledati više: *The State of Security Convergence in the United States, Europe, and India*, ASIS International, Alexandria VA 2019.

jeg mnoge organizacije koriste kao način za efektivno i efikasno upravljanje. Takođe, prilikom izgradnje, održavanja i unapređenja sistema menadžmenta bezbednošću potrebno je pridržavati se univerzalnih osnovnih funkcija menadžmenta:

- planiranje,
- organizovanje,
- ruko(vođenje),
- koordinacija i
- kontrola[7].



Slika 3.1. *PDCA* model primenjen na sistem menadžmenta bezbednošću
Izvor: Slika preuzeta iz standarda za zahteve sistema menadžmenta bezbednošću *ISO 28000*

Kao što je i ranije navedeno, svaki sistem upravljanja, pa i sistem upravljanja bezbednošću, zasniva se na procesnom pristupu po modelu *Plan-Do-Check-Act (PDCA)*. Prema standardu *ISO 28000* ovaj model se primenjuje na planiranje, uspostavljanje, implementaciju, rad, praćenje, preispitivanje, održavanje i stalno poboljšanje efikasnosti sistema menadžmenta bezbednošću organizacije.

7 O funkcijama bezbednosnog menadžmenta pogledati: Dragišić Zoran, Radojević Kristina, *Bezbednosni menadžment*, Fakultet bezbednosti Univerziteta u Beogradu, Beograd, 2014., str. 49 - 195.

U skladu sa razumevanjem konteksta organizacije, početni korak u izgradnji sistema menadžmenta bezbednošću ogleda se u izradi krovne bezbednosne politike, odnosno formalno izražene namere i pravca delovanja organizacije u bezbednosnom smislu, a usklađene sa opštom politikom i ciljevima organizacije, i verifikovane od strane top menadžmenta. Takođe, određivanje, izrada i uspostavljanje bezbednosnih strategija[8], ciljeva, procesa, procedura, planova, pravilnika, ostalih normativnih akata, pripada osnovnim elementima izgradnje sistema, uključujući određivanje odgovornosti i resursa za implementaciju potrebnih mera i kontrola, sa naglaskom na one koje se odnose na bezbednost lanca snabdevanja, u današnje vreme veoma dinamične i kritične kategorije. Iako bezbednost ne predstavlja egzaktnu disciplinu, i praksa ukazuje da se bezbednost u krajnjoj liniji nemože u potpunosti izmeriti, u novije vreme putem sprovođenja procene rizika, određivanja bezbednosnih ciljeva kao rezultata koje treba postići (strateških, taktičkih ili operativnih), kao i praćenjem i evaluacijom performansi, uvodi se određena metrika u segment bezbednosti[9].

Rezultati analize pretnji, procene rizika od pretnji i opasnosti, kao i iz procene ranjivosti trebalo bi da ukažu na pravac odbrane i potreban nivo zaštite, dok će spro-

8 Primer izgradnje strategije i upravljanja procesima korporativne bezbednosti videti u : Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, *Korporativna sigurnost*, Udruga hrvatskih menadžera sigurnosti, Zagreb, 2011., str. 21 - 88.

9 Misao koja se pripisuje Albertu Ajnštajnu - "Ne računa se baš sve što se može izmeriti, kao što se ne može izmeriti baš sve što se računa" – ukazuje da su mnoge stvari teško merljive, ali sa druge strane ako su naša saznanja o komleksnom sistemu kojim upravljamo (kakav je sistem korporativne bezbednosti) nekompletna, tada će i rezultat voditi ka nepredvidivim posledicama. Ima puno dobrih razloga da se uloži napor i uspostavi kvalitativna i kvantitativna metrika indikatora bezbednosti, a pre svega kako bi mogli da pratimo stanje bezbednosti, da određujemo mere za unapređenje, kao i da redefinišemo ciljeve. Najprisutnija metrika je ona zastupljena u procesu procene rizika kojom se izračunava nivo rizika i koja, ako uzmemo za primer standard *SRPS A.L2.003*, može da bude u granicama od minimalno 1 do maksimalno 25, pa se može reći da je rizik vrlo mali, zanemarljiv ako je nivo 1 i 2, odnosno da je izrazito veliki ako je nivo 20 i 25. Slična metrika je predviđena pri izračunavanju nivoa rizika od katastrofa, za merenje performansi bezbednosti informacija (prilikom čega se mogu koristiti međunarodne smernice *ISO/IEC 27004:2016, Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*) itd., a merenje bi trebalo da bude primenjeno u svim drugim poslovima i procesima korporativne bezbednosti. Neophodno je da menadžment korporativnom bezbednošću vrednuje performanse bezbednosti i efektivnost sistema, odnosno da utvrdi šta je potrebno da se prati i meri, metode merenja i vrednovanja, i to na način koji je za to primenljiv i koji obezbeđuju validne rezultate. Ali ponavljamo nešto što je potvrđeno i u praksi, da iako vlasnik ili top menadžment najlakše razumeju brojke, ne smemo dozvoliti da se bezbednost i planiranje mera i kontrola bazira isključivo na rezultatima koji su proizašli iz merenja. U prilog tome navodimo, ilustracije radi, činjenicu da se procena rizika, kao početna radnja u određivanju bezbednosnih mera i kontrola, delom zasniva na subjektivnoj oceni, bez obzira na postojanje određene metodologije i metrike.

vođenje tzv. analize praznine (eng. *gap analysis*) ukazati na jaz između onog stanja bezbednosti gde smo trenutno u odnosu na potrebe i stanje gde bi želeli da bude, ostvarujući ujedno i otpornost organizacije. Definisanje i praćenje ključnih indikatora učinka (bilo kvalitativnih ili kvantitativnih) ukazaće na određivanje potrebnih korektivnih radnji kako bi se otklonile neusaglašenosti (sa internim propisima i zahtevima, kao i sa zakonskom regulativom i primenjenim bezbednosnim standardima) i sprovelo stalno unapređenje kao redovna, ponavljajuća aktivnost za poboljšanje performansi. Nezavisni proces interne, eksterne ili kombinovane provere daje objektivnu procenu kako bi se utvrdilo u kojoj meri su kriterijumi provere ispunjeni. Inspekcijski nadzor i rezultati interne revizije upotpunjuju sliku trenutnog stanja, a da bi mogli da se planiraju unapređenja, neophodno je da bezbednosni menadžment razvije programe nadzora i preispitivanja učinka u odnosu na bezbednosnu politiku i ciljeve, i odredi sredstva, nosioce i radnje za sanaciju i poboljšanje. O rezultatima provere se izveštava top menadžment, a odobrene aktivnosti za poboljšanje performansi i otklanjanje uzroka neusaglašenosti predstavljaju ključne elemente za održavanje i unapređenje sistem menadžmenta bezbednošću, kao stalne, neprekidne aktivnosti.

Bez obzira da li se sistem menadžmenta bezbednošću uspostavlja od starta ili je u pitanju zatečeno stanje, izgradnja treba da se izvodi postepeno i shodno finansijskoj mogućnosti organizacije, uzimajući u obzir sve njene specifičnosti. Odlučujuću ulogu mora da zauzme top menadžment[10], bez čije podrške u fazi iniciranja i tokom preispitivanjanije moguće adekvatno održavati i razvijati sistem menadžmenta bezbednošću. U zavisnosti od određenih potreba ili veličine organizacije navedena odgovornost top menadžmenta obično se formalizuje kroz rad grupe za koordinaciju strateškog bezbednosnog okvira – odbor za bezbednost. Da bi mogao da odgovori zadacima (kao što je razmatranje trenutnog bezbednosnog statusa, pravac potrebnih strateških promena, predstojeći izazovi i projekti i sl.) sastav odbora mora da čini rukovodstvo kompanije, tj. menadžer korporativne bezbednosti i drugi ključni rukovodioci najvišeg nivoa. Takođe, pored adekvatne organizacije bezbednosnih poslova, jedan od bitnih preduslova izgradnje uspešnog sistema menadžmenta jeste pozicioniranost lica odgovornog za sveukupnu bezbednost – menadžera korporativne bezbednosti (*CCSO*) – kome je povereno organizaciono rukovođenje i koji je neophodno da bude odgovaran direktno najvišem rukovodstvu, bez obzira na organizacionu strukturu kompanije.

10 O uticaju top menadžmenta na funkciju korporativne bezbednosti pogledati: Briggs Rachel, Edwards Charlie, *The Business of Resilience: Corporate security for the 21st century*, Demos, London UK, 2006., pp. 58 – 64.

Benefiti koje kompanija ima od ovakvog sistemskog pristupa menadžmenta bezbednošću ogledaju se u sveobuhvatnijoj proceni bezbednosnog okruženja u kojem posluje, boljem utvrđivanju adekvatnosti uspostavljenih mera i kontrola, većom usaglašenošću sa statutarnim, regulatornim i ostalim obavezama koje organizacija treba da ispunjava, što zajedno povećava otpornost organizacije, omogućava ostvarivanje kontinuiteta poslovanja i ispunjenje organizacijskih ciljeva, uz smanjenje/kontrolu troškova. Formalni pristup upravljanju bezbednošću može direktno doprineti poslovnoj sposobnosti i kredibilitetu organizacije, vodeći računa da se ne upadne u zamku (što se u praksi neretko dešava) preteranog formalizma, kada sistem menadžmenta postaje sam sebi svrha, braneći isključivo sopstveno postojanje i predstavljajući breme poslovanju, a zaboravljajući osnovnu ulogu koja se ogleda u izgradnji, održavanju i unapređenju bezbednih uslova za funkcionisanje organizacije i ostvarivanje njenih ciljeva. Sistem menadžmenta bezbednošću je potrebno posmatrati i kao sredstvo kojim top menadžment prati i kontroliše bezbednost organizacije, umanjuje rezidualne rizike i obezbeđuje da ukupna bezbednost i otpornost nastavi da zadovoljava korporativne, zakonske i zahteve korisnika i drugih zainteresovanih strana.

Menadžment bezbednosnim rizicima

Organizacije pri poslovanju sve više vode računa o rizicima, upravljaju njima na adekvatniji način, usklađujući se sa pozitivnim propisima i zahtevima važećih standarda koji se odnose na proces procene rizika, ali moramo priznati da menadžment ukupnim bezbednosnim rizicima u mnogim organizacijama još uvek nije zastupljen na odgovarajućem, sistemskom nivou. Mnogobrojni su razlozi za takvo stanje, a jedan od ciljeva ovog Priručnika je ukazivanje na ogroman značaj upravljanja bezbednosnim rizicima kao suštinskim procesom menadžmenta bezbednošću i podskupom šireg sistema upravljanja rizikom organizacije, utičući na svest kako menadžera korporativne bezbednosti, tako i na svest vlasnika kapitala, top menadžmenta, ali i na shvatanje njegovog pozitivnog uticaja kod svih zaposlenih u organizaciji.

Kao primer organizacija koje se susreću sa novijim izazovima u upravljanju bezbednosnim rizicima navodimo privredna društava koja pružaju usluge povezane s digitalnom imovinom, odnosno virtuelnom imovinom, a koja su shodno *Zakonu o digitalnoj imovini* dužna da, pored ostalog, sprovode odgovarajuće mere i radnje za prepoznavanje svih značajnih rizika po svoje poslovanje i donose delotvorne mere u cilju umanjenja tih rizika. U tom smislu, a značajno sa aspekta identifikacije ra-

njivosti, kontinuiteta poslovanja i drugih rizika iz delokruga poslova korporativne bezbednosti, neophodno je da takva privredna društva izgrade procedure za uspostavljanje delotvornih sistema u slučaju nepredviđenih okolnosti kako bi savladali rizike od prekida rada sistema, sa akcentom na rizike od pranja novca i finansiranja terorizma. Pored potrebnog postojanja sistema unutrašnje kontrole, ocena spremnosti i sposobnosti ovih privrednih društava da identifikuju, mere, prate, procenjuju i upravljaju rizicima je i u nadležnosti nadzornog organa (u ovom slučaju to su Narodna banka Srbije i Komisija za hartije od vrednosti).

Sama reč „rizik" potiče od italijanske reči *riscare*, što u prevodu znači usuditi se. Iako se o pojmu upravljanja rizikom može govoriti i u ranijem istorijskom periodu, metode koje se i danas koriste u upravljanju rizicima razvile su se krajem 17. i početkom 18. veka, dok je ozbiljniji razvoj nauke o riziku ipak prisutan od postindustrijskog, informacionog društva, kojeg je nemački ekspert U. Bek okarakterisao kao prelazak iz industrijskog u društvo rizika.[11]

Iako ne postoji jedinstvena definicija možemo reći da upravljanje bezbednosnim rizicima (eng. *security risks management*) organizacije predstavlja

> *„proces upravljanja koji se koristi za efikasno upravljanje bezbednosnim rizicima čitave organizacije, u proaktivnom i reaktivnom pogledu. Upravljanje bezbednosnim rizicima organizacije kontinuirano procenjuje pun obim rizika vezanih za bezbednost organizacije, i unutar kompletnog portfolija imovine preduzeća. Proces upravljanja kvantifikuje pretnje, uspostavlja planove za ublažavanje, identifikuje pravila prihvatanja rizika, upravlja incidentima, i usmerava vlasnike rizika u razvoju napora na sanaciji."*[12]

Kao i u slučaju definicije, ne postoji ni opšte prihvaćena metodologija procene ukupnog bezbednosnog rizika, te fokus bezbednosnog menadžmenta treba da ide u pravcu fleksibilnog i prilagodljivog pogleda na organizacione i upravljačke aspekte upravljanja rizikom, uključujući integraciju bezbednosti u upravljanju rizicima preduzeća, ulažući napore na povećanju standardizacije i uporedivosti među različitim metodologijama.[13]

11 Keković Zoran, Savić Suzana, Komazec Nenad, Milošević Mladen, Jovanović Dragiša, *Procena rizika u zaštiti lica, imovine i poslovanja*, Centar za analizu rizika i upravljanje krizama, Beograd, 2011, str. 24-25.

12 Pogledati: *Enterprise Security Risk Management: Overview and Case Studies,* ASIS International, CSO Roundtable, Alexandria VA, 2015.

13 Talbot Julian, Jakeman Miles, *Security Risk Management Body of Knowledge*, John Wiley and

Shodno navedenom, ukazujemo da je menadžment rizikom najcelishodnije sprovoditi u skladu sa međunarodno priznatim i univerzalnim standardima i smernicama, a bazni je svakako *ISO 31000*[14]. Elementarni okvir za proces procene rizika bilo koje organizacije dat je i standardom *ISO 9001*[15], na koga se može nadovezati *Enterprise Risk Management*[16], a svi zajednički ukazuju na značaj i benefite upravljanja procesom procene rizika kao neprekidnog procesa neophodnog za adekvatno upravljanje i kontinuitet poslovanja organizacije.

Na prethodno navedene elementarne standarde nadovezuju se standardi za menadžment bezbednosnim rizicima, a za potrebe ovog Priručnika izdvajamo proces menadžmenta bezbednosnim rizikom koji je grafički prikazan u standardu[17] publikovanim od strane nacionalne organizacije za standardizaciju Australije i Novog Zelanda, Slika 3.2.

Neophodno je da menadžment korporativne bezbednosti opredeljenu metodologiju prilagodi i u nju inkorporira procese procene rizika zahtevane pozitivnim propisima, kao i bezbednosnim standardima koji se odnose na poslove korporativne bezbednosti, odnosno na određenu delatnost. Tako na primer, za potrebe procene rizika od katastrofa neophodno je primenjivati metodologiju datu *Uputstvom o Metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja*,[18] a procenu rizika u zaštiti lica, imovine i poslovanja vršiti po zahtevima i na način propisan važećim srpskim standardom u oblasti privatnog obezbeđenja (*SRPS A.L2.003*). Znajući da je procena rizika ključ prevencije, i oni pozitivni propisi koji neodređuju precizno metodologiju zahtevaju njeno sprovođenje i ukazuju na značaj procene rizika. Takav je npr. *Zakon o informacionoj bezbednosti*[19] koji određuje da je prilikom planiranja i primene mera zaštite IKT sistema potrebno rukovoditi se načelom upravljanja rizikom, tj. da se izbor i nivo primene mera zasniva na proceni rizika. Slično je i sa *Zakonom o kritičnoj infrastrukturi*[20] čija načela delovanja ukazu-

Sons, Hoboken NJ, 2009., str. 14.

14 *ISO 31000:2018, Risk management — Guidelines.*

15 *ISO 9001:2015, Quality management systems — Requirements.*

16 *Enterprise Risk Management - Integrating with Strategy and Performance*, COSO, Englewood Cliffs NJ 2017.

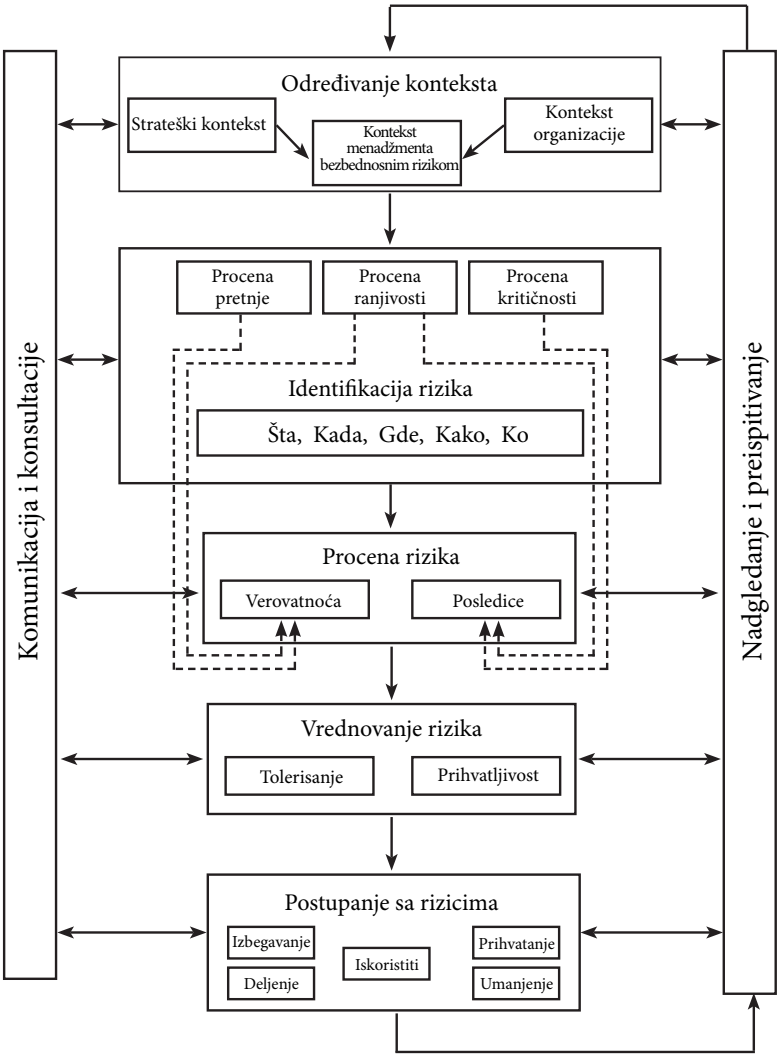
17 *Handbook - Security risk management, HB 167:2006,* Standards Australia & Standards New Zealand, Sydney AU-Wellington NZ, 2006.

18 „Službeni glasnik RS", br. 80/2019.

19 Član 3. tačka 1. *Zakona o informacionoj bezbednosti* ("Službeni glasnik RS", br. 6/2016, 94/2017 i 77/2019).

20 Član 3. *Zakona o kritičnoj infrastrukturi* („Službeni glasnik RS", br. 87/2018).

ju na stalni proces analize rizika po funkcionisanje kritične infrastrukture i procene adekvatnosti mera zaštite, a taksativno zahteva postojanje bezbednosnog plana operatora za upravljanje rizikom.



Slika 3.2. Proces menadžmenta bezbednosnim rizikom, prema Handbook - Security risk management, HB 167

Procena rizika je bazni proces i polazna tačka svih međunarodnih, nacionalnih, granskih, kao i bezbednosnih standarda izrađenih od strane strukovnih udruženja,

a koji naglašavaju potrebu za identifikacijom, kvantifikacijom i određivanjem prioritetnih rizika prema kriterijumima za prihvatanje rizika i ciljevima koje su relevantne za organizaciju. Jedni od najzastupljenijih u praksi su standardi upravljanja sistemom bezbednosti informacija serije *ISO/IEC 27000*, koji naglašavaju potrebu periodičnog vršenja procesa procene rizika, a čija efikasnost zavisi i od izgrađene veze sa procenama rizika u drugim oblastima. Smernice za upravljanje rizikom bezbednosti informacija konkretno su date standardom *ISO/IEC 27005* koji je dizajniran da pomogne adekvatnoj implementaciji bezbednosti informacija zasnovane na pristupu upravljanja rizikom. Na proces procene rizika slično gledaju i drugi univerzalni bezbednosni standardi koji se odnose na sisteme menadžmenta (serije standarda *ISO 22300, ISO 28000, ISO 45000* itd.), ali i granski standardi koji daju preporuke i smernice za upravljanjem sistemom bezbednosti u određenoj delatnosti (npr. *ISO 20858*[21], *ISO 14298*, *TAPA FSR 2017*[22] itd.).

Neophodnost integrisanog pristupa u proceni bezbednosnih rizika naznačena je i u međunarodnim, nacionalnim i standardima različitih strukovnih udruženja profesionalaca bezbednosti, koji prepoznaju kompleksnu paletu rizika sa kojim se suočavaju organizacije i njihovi lanci snabdeva, zahtevajući sveobuhvatan i sistematski pristup upravljanju rizicima. Za primer možemo navesti standarde američkog nacionalnog instituta za standardizaciju *ANSI (American National Standards Institute)*, u kojima se naglašava značaj proaktivnog upravljanja rizikom i poslovanjemu cilju podrške procesa prevencije, zaštite, pripravnosti, spremnosti, ublažavanja, odgovora, kontinuiteta i oporavka od neželjenih i štetnih događaja. Njihov standard za *Bezbednost i otpornost organizacije i lanca snabdevanja*[23] upravo ukazuje na neophodnost jedinstvenog sistema integrisanog upravljanja eliminacijom i ublažavanjem raznorodnih rizika u vezi sa poslovima korporativne bezbednosti, a standard za *Procenu rizika*[24] daje smernice za razvoj i održavanje koherentnog i efikasnog programa za procenu spektra rizika, uključujući principe, upravljanje ukupnim programom za procenu rizika i obavljanje pojedinačnih procene rizika.

Kao što upravljanje ukupnim sistemom bezbednosti zahteva strateške i operativne dokumente, tako je i za upravljanje bezbednosnim rizicima neophodna izgrad-

21 *ISO 20858:2007, Ships and marine technology — Maritime port facility security assessments and security plan development.*

22 *Facility Security Requirements (FSR) 2017*, TAPA Standards, Boca Raton FL, 2017.

23 Videti više: *Security and Resilience in Organizations and Their Supply Chains*, ORM.1-2017, ANSI & ASIS, Washington DC-Alexandria VA, 2017.

24 *Risk Assessment,* RA.1-2015, ANSI/ASIS/RIMS, Washington DC-Alexandria VA-New York NY 2015.

nja politike, programa, strategije i procedura, kao i adekvatnog sistema unutrašnjih kontrola i odgovarajućeg načina izveštavanja i drugih elemenata komunikacije u vezi sa rizicima.

Iz razloga što se jedan sistem smatra bezbednim ako je zaštićen od uticaja faktora rizika, zato upravljanje procesom procene rizika podrazumeva postojanje liste faktora rizika, koju je potrebno periodično ili po potrebi nadopunjavati. Kako bi se smanjio uticaj subjektivnosti procenitelja pojedini standardi izrađuju predefinisane liste faktora rizika, koje svakako treba da budu dopunjene u slučaju postojanja specifičnih faktora za određenu organizaciju.

Svrha holističkog pristupa u proceni rizika je stvaranje uslova za donošenje efikasnih i efektivnih odluka u funkciji unapređenja ukupne bezbednosti i otpornosti korporacije. Takođe, procena bezbednosnih rizika doprinosi efikasnijem postizanju vizije, misije i ciljeva organizacije, uz omogućavanje i podsticanje stalnog unapređenja svih procesa i postupaka, uključujući i sam proces procene rizika. Proces procene rizika bi trebao da rezultira određivanjem odgovarajućih mera i kontrola za postupanje sa rizikom, a koje bi trebale da budu srazmerne riziku uz postojanje niskog nivoa preostalog rizika. Odluka o ublažavanju rizika bi trebalo da sadrži i podatke o vlasnicima rizika, potrebnim resursima za realizaciju, rokovima za implementaciju, opcije zaizvodljivost i analizu cena–benefit.

Konačno, mere i kontrole za tretman svih bezbednosnih rizika moraju biti objedinjeno implementirane i nadgledane, jer jedino na takav način možemo efikasno kontrolisati primenjene proaktivne i reaktivne mere zaštite, uz postizanje najboljeg odnosa cene i koristi, koji je za top menadžment često od presudnog značaja.

Poželjan alat koji može da kombinuje alate za procenu rizika, da izrađuje objedinjene mape bezbednosnih rizika, grafički i na drugi način da izrađuje potrebne evidencije i izveštaje, prikazuje primenjene mere, kontrole i bezbednosne incidente, jeste aplikativno rešenje, tj. softver prilagođen bezbednosnim potrebama organizacije, omogućavajući lakše i brže odlučivanja u sve složenijem okruženju, uz transparentnost troškova upravljanja bezbednosnim rizicima.

Nezaobilazna aktivnost u procesu uvođenja i razvoja sistema menadžmenta bezbednosnim rizicima je rad na izgradnji svesti i postepenom menjanju bezbednosne kulture zaposlenih, i to u pravcu spoznaje i prihvatanja činjenice da upravljanje rizikom nije u isključivoj nadležnosti top menadžmenta, funkcije korporativne bezbednosti ili neke druge organizacione celine, već da odgovornost leži u svakom pojedincu.

Menadžment bezbednosnim incidentima i događajima

I pored svih preduzetih preventivnih i proaktivnih radnji, analiza i procene rizika od opasnosti, pretnji i ranjivosti, bez obzira na sve propisane i implementirane mere i kontrole za postupanje sa tim rizicima, moramo očekivati i biti spremni na incidente i događaje u vezi sa narušavanjem bezbednosti, odnosno na neželjene i štetne događaje. Način na koji organizacija upravlja bezbednosnim incidentima i događajima ukazuje na nivo njene otpornosti i značajno pospešuje uslove na izgradnji adekvatnog sistema kontinuiteta operacija i poslovanja, čiji je obavezni element i plan odgovora na incidente.

S obzirom da ne postoji jedinstvena definicija bezbednosnog incidenta, za potrebe ovog Priručnika možemo se poslužiti definicijom datom u dokumentu koji definiše termine koji se koriste u standardima bezbednosti i otpornosti - *ISO 22300*,[25] prema kome bezbednosni incident predstavlja

> *„svaki čin ili okolnost koja proizvodi posledicu"*

i to u vidu gubitka, prekida/poremećaja, hitne situacije ili krize. Za razliku od incidenta, čija je karakteristika da uvek prouzrokuje određenu (manju ili veću, materijalnu ili nematerijanu) štetnu posledicu, bezbednosni događaj je pojava ili promena određenog spleta okolnosti i može biti izvor rizika, ali u trenutku dešavanja bez posledica (takvo dešavanje nije dovelo do incidenta, odnosno akcidenta[26]). Za takav događaj bez posledica takođe se mogu upotrebiti izrazi kao što su „jedva izbegnut", „samo što se nije desio" i „umalo da se desi", ali mogu biti i pojave i okolnosti koje se nakon provere odbacuju kao neosnovane, odnosno ne bi prouzrokovale štetnu posledicu (npr. neosnovana prijava vršenja krivičnog dela, sumnja u kršenje internog propisa ili procedure, neopravdana prijava kompromitacije, prevare ili nekog oblika napada, lažna dojava o postavljenom opasnom predmetu ili minsko-eksplozivnom sredstvu itd.).

25 *ISO 22300:2018, Security and Resilience – Vocabulary, 3.111.*

26 Akcident je termin koji se koristi za događaj sa posledicom koja prevashodno ima uticaj na bezbednost i zdravlje na radu zaposlenih i drugih lica, kao i na životnu sredinu. Obično je u pitanju neželjeni ili nesrećni događaj koji se dešava nenamerno, ali rezultira štetom, povredom, uništenjem ili gubitkom (obično potiče od katastrofa, odnosno od elementarnih nepogoda ili tehničko-tehnoloških nesreća).

Bez obzira da li se pojava, okolnost ili događaj završio sa ili bez štetne posledice, neophodno je da organizacija razvije funkcionalni sistem koji definiše uloge i odgovornosti osoblja i operativne procedure koje će se koristiti u upravljanju bezbednosnim incidentima i događajima. Stepen pripremljenosti na incidente i događaje ukazuje na nivo zrelosti organizacije i spremnosti na odgovor, odnosno na razvijenost radnji koje se preduzimaju u cilju zaustavljanja uzroka neposredne opasnosti i pretnje, i/ili ublažavanja posledica, omogućavajući vraćanje stanja u normalu i nastavak operacija, procesa i poslovanja.

Dokumentovana politika upravljanja incidentima i događajima trebala bi da iskaže značaj i način njihovog prijavljivanja, uz naglašavanje razlike između hitnih incidenta i događaja, od onih koji to nisu. Postupak prijavljivanja (lično, telefonski, aplikacijski itd.) bi trebao da bude jasno uređen, a poslovna atmosfera na nivou u kojem zaposleni i druga zainteresovana lica (stranke, kupci, korisnici, pružaoci usluga itd.) imaju slobodu, bez zadrške i nedoumica, da prijave svaku sumnju, događaj, promenu ili slabosti domena poslova korporativne bezbednosti (korupciju, kompromitaciju podataka, povrede privatnosti, nasilje na radnom mestu, krađu, prevaru, vandalizam, sajber napad, opasnost i povredu, požar i druge vanredne situacije, slabost sredstava tehničke i IKT zaštite, slučajne štete itd.). Politika i procedure upravljanja bezbednosnim incidentima i događajima bi trebale da sadrže i institut anonimne dojave, a svaka opravdana prijava od strane zaposlenog ne bi smela da povlači nikakav vid odgovornosti, odnosno ne može biti osnov za korišćenje administrativne ili druge sankcije protiv zaposlenog.

Korporacije koje se bave određenim delatnostima, htele - ne htele, moraju razvijati sistem upravljanja bezbednosnim incidentima jer imaju zakonsku obavezu evidentiranja i obaveštavanja onih događaja i pojava zbog kojih mogu nastati ili su nastali gubici. Primera radi, takvu obavezu imaju poslovne banke koje su shodno *Odluci o upravljanju rizicima banke*[27] dužne da obaveste Narodnu banku Srbije o prirodnim katastrofama i sličnim događajima, kao i pokušajima izvršenja ili izvršenje dela koje je zakonom predviđeno kao krivično delo (npr. krađe, teške krađe, razbojničke krađe, prevare i sl.). Ako ni zbog čega drugog ono zbog navedenog potrebnog obaveštavanja, poslovne banke moraju da poseduju interni sistem upravljanja incidentima koji minimalno mora da sadrži evidenciju događaja (naziv i opis događaja, datum početka događaja, datum završetka događaja, datum saznanja za

27 "Službeni glasnik RS", br. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 - dr. odluka, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016, 119/2017, 76/2018, 57/2019, 88/2019, 27/2020, 67/2020 - dr. odluka, 89/2022 i 77/2023.

događaj i dr.), procenjeni iznos gubitka, kao i preduzete, odnosno planirane aktivnosti povodom događaja. Takođe, banke i druge finansijske institucije su dužne

> *„da uspostave proces upravljanja incidentima koji će omogućiti blagovremen i efikasan odgovor u slučaju narušavanja bezbednosti ili funkcionalnosti resursa informacionog sistema"*[28],

kao i da definišu upravljanje incidentima u slučajevima uspostavljanja ugovornog odnosa sa pružaocima usluga za određene aktivnost, uključujući i one vezane za korišćenje klaud usluga[29]. Slično je i sa operatorima kritične infrastrukture koji su po *Zakonu o kritičnoj infrastrukturi*[30] dužni da izveštavaju Ministarstvo unutrašnjih poslova u slučaju svakog vanrednog događaja, sa detaljnim opisom događaja, uzrocima, posledicama i predlogom mera i aktivnosti na poboljšanju bezbednosti kritične infrastrukture kojom upravljaju.

Pored zakonske obaveze, organizacije mogu primenjivati određene sektorske standarde koji se odnose na upravljanje incidentima. Takav je slučaj sa kompanijama iz sektora logistike, koji za izveštavanje o incidentima mogu koristiti specifikacije date standardom *EN 16352*[31], koji utvrđuje model za prijavljivanje kriminalnih dela (napad na vozača/posadu; otmica, odnosno upotreba sile, pretnja ili zastrašivanje vozača/posade; krađa vozila, tereta itd.) u vezi sa transportnim uslugama.

Kao što je, primera radi, operatorima IKT sistema od posebnog značaja uređen postupak obaveštavanja o incidentima shodno *Uredbi o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja*[32], svaka organizacija bi trebala da utvrdi svoju listu incidenata i događaja prema vrsti i značaju shodno nivou opasnosti. Upravljanje incidentima bi trebalo da uzme u obzir kombinaciju svih vrednosti organizacije kao što su objekti, oprema, osoblje, organizacione strukture, procedure i komunikacije, a praksa je ukazala na značaj i potrebu za dokumentovanjem svih postupaka i struktura upravljanja.

---

28 Videti tačku 29. *Odluke o minimalnim standardima upravljanja informacionim sistemom finansijske institucije* ("Službeni glasnik RS", br. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 i 100/2023 – odluka).

29 Pogledati: *Odluka o uslovima i načinu poveravanja aktivnosti u vezi sa informacionim sistemom finansijske institucije trećim licima* („Službeni glasnik RS", br. 100/2023).

30 Član 9, *Zakona o kritičnoj infrastrukturi* ("Službeni glasnik RS", br. 87/2018)..

31 *EN 16352:2013 - Logistics - Specifications for reporting crime incidents*, Brussels 2013.

32 "Službeni glasnik RS", br. 11/2020.

Kompleksnost poslova korporativne bezbednosti i postojanja multi rizika u vezi sa njima, iziskuje pažnju organizacije prilikom izgradnje holističkog sistema upravljanja bezbednosnim incidentima i događajima, uzimajući u obzir specifičnosti koje se odnose na njenu veličinu, strukturu, delatnost itd. Zbog sve većeg značaja koje informacije i IKT sistemi imaju za poslovanje većine organizacija, naglašavamo potrebu izgradnje adekvatnog sistema upravljanja incidentima vezanim za bezbednost informacija, koji prema osnovnom dokumentu serije standarda *ISO/IEC 27035*[33] predstavlja

> *„saradničke aktivnosti za rukovanje incidentima bezbednosti informacija na dosledan i efikasan način"*.

I u ovom slučaju incidenti stvaraju posledice i predstavljaju

> *„povezane i identifikovane događaje koji mogu naneti štetu imovini organizacije ili ugroziti njene operacije"*,

a događaji u vezi sa bezbednošću informacija su pojave bez (trenutne) posledice i

> *„koji ukazuju na moguće kršenje bezbednosti informacija ili neuspeh kontrola"*.

S obzirom da je upravljanje incidentima vezanim za bezbednost informacija umnogome ustrojeno priznatim standardima i principima, za potrebe ovog priručnika možemo izdvojiti one iz serije internacionalnog standarda *ISO/IEC 27035* (Delovi 1-3)[34], koji se odnose na upravljanje događajima, incidentima, ali i ranjivostima u oblasti bezbednosti informacija, i koji promovišu program sažeto strukturiran od sledećih pet faza procesa:

1. planiranje i priprema (organizacione mere, plan, tehnička podrška, obuka itd.);

2. detekcija, izveštavanje i procena incidenata i ranjivosti povezanih sa tim incidentom;

33 *ISO/IEC 27035-1:2023, Information technology - Information security incident management - Part 1: Principles and process.*

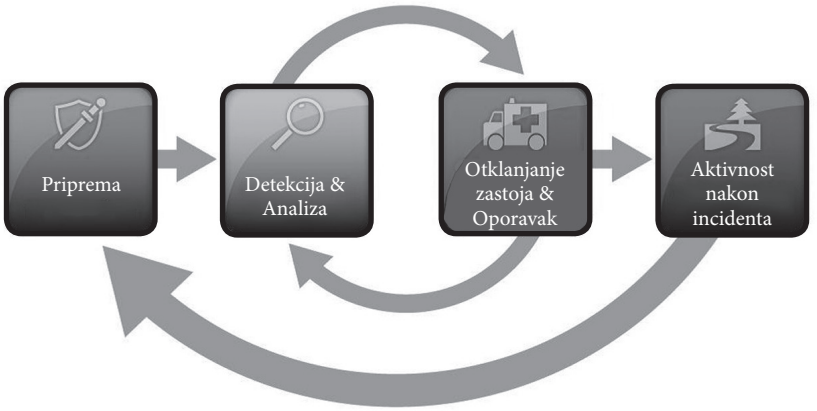
34 Serija standarda obuhvata sledeće: *ISO/IEC 27035-1; ISO/IEC 27035-2:2023, Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response; ISO/IEC 27035-3:2020, Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations.*

3. reakcija na incidente (uključujući aktiviranje odgovarajućih kontrola za sprečavanje, smanjenje i oporavak od uticaja);

4. aktivnosti na tretmanu prijavljenih ranjivosti koje su povezane sa incidentom;

5. učenje iz incidenata i ranjivosti, kao i implementacija i verifikacija preventivnih kontrola i mera poboljšanja sveukupnog pristupa upravljanju incidentima u oblasti bezbednosti informacija.

Slično je iskazano i u jednim od u praksi najčešće primenjenim smernicama za upravljanje incidentima vezanim za bezbednost računarskih/kompjuterskih sistema - *NIST Special Publication 800-61*[35], a u kojima je, između ostalog, i slikovito prikazan i razrađen životni ciklus odgovora na incidente:



Slika 3.3. Životni ciklus odgovora na incidente

Deljenjem potrebnih informacija o incidentima i dostavljanjem izveštaja zainteresovanim subjektima (top menadžmentu, internoj reviziji, nadležnim odborima, MUP-u i dr.) zaokružio bi se ciklus menadžmenta incidentima na dosledan i efikasan način. Sumirajući značaj sistema menadžmenta incidentima iz delokruga korporativne bezbednosti može se zaključiti da se, pored bolje reakcije i bržeg oporavka operacija i poslovanja, benefit ogleda i u sprovođenju analize incidenata (utvrđivanje strukture, trendova, efikasnost primenjenih mera itd.), kao i u iznalaženju potrebnih korektivnih mera i kontrola za poboljšanje bezbednosti, što kumulativno može imati uticaja na povećanje otpornosti, ali i smanjenje troškova kompaniji.

35 *Computer Security Incident Handling Guide,* NIST Special Publication 800-61, Revision 2, NIST, Gaithersburg MD, 2008.

Obuka i izgradnja bezbednosne svesti

Složićemo se da je ljudski faktor presudan za poslovanje i razvoj svake organizacije, i zato je potrebno pridavati značaj svakom zaposlenom koji dnevno na operativnom nivou preduzima različite mere i radnje, uključujući i one koje se odnose na bezbednost i utiču na otpornost organizacije. Samo kvalifikovani i senzibilni zaposleni prepoznaju i rade na očuvanju vrednosti i realizaciji ciljeva organizacije, svesni potencijalnih rizika i razumevajući ih na odgovarajući način. Zahtevani nivo bezbednosti se stoga uspešno sprovodi u okviru organizacije samo ako su zaposleni adekvatno obučeni i svesni, i koji u tom slučaju pomažu da se uspešno sprovode bezbednosne mere i kontrole na svim nivoima.

Bezbednosna kultura je deo korporativne ili organizacione kulture, koja prema standardu rečnika *ISO 22300*[36] predstavlja kolektivno uverenje, vrednosti, stavove i ponašanje organizacije koji doprinose jedinstvenom društvenom i psihološkom okruženju u kojem ona deluje. Dostignuti nivo bezbednosne kulture značajno utiče na ostale procese u kompaniji, a na kulturu najviše utiče svest zaposlenih, odnosno znanje i stav koji imaju u pogledu bezbednosnih rizika i zaštite vrednosti organizacije.

Posedovanje i unapređenje znanja, kao i izgradnja pozitivnog stava prevashodno se postiže izgradnjom i realizacijom različitih programa obuke, kao i sprovođenjem vežbi i testiranja. U vezi s tim, potrebno je imati na umu da pojedinci na različite načine opažaju, analiziraju i donose odluke u vezi sa bezbednosnim rizicima. Pored transparentnih, što jednostavnijih i razumljivijih za korišćenje bezbednosnih pravila i mera, redovne obuke, vežbe i testiranja, pre svega, omogućavaju zajednički cilj u vidu ublažavanja individualne razlike u percepciji rizika. Takođe, takav način oblikovanja svesti utiče i na reakciju pojedinca, grupe ili celog kolektiva u slučaju opasnosti ili nastupanja bezbednosnog incidenta ili događaja.

Odlučujuću ulogu može odigrati stav najvišeg rukovodstva i drugih menadžerskih linija koji svojim ponašanjem i poštovanjem usvojenih politika i procedura daju motivišući primer ostalim zaposlenima, a koji moraju da usvoje i aktivno primenjuju činjenicu da ostvarivanje bezbednog i otpornog ambijenta predstavlja zadatak i odgovornost svakog pojedinca koji je angažovan u njoj. Pozitivna uloga top menadžmenta ogleda se i u aktivnoj podršci programima obuke i unapređenja znanja i veština svih zaposlenih, a posebno onih direktno uključenih u bezbednosne procese. Na nivou EU dobar primer podsticaja radu na podizanju svesti možemo videti u

36 *ISO 22300:2018, Security and Resilience – Vocabulary, 3.225.*

tzv. *NIS 2* direktivi (*Directive (EU) 2022/2555*[37]) kojom se uređuju mere za visoki zajednički nivo sajber bezbednosti, gde se neposredno i direktno ističe obaveza subjekata da, radi adekvatnog upravljanja ranjivostima i rizicima sajber bezbednosti, usvajaju širok spektar osnovnih praksi sajber higijene, što pored ostalog, podrazumeva angažovanje na podizanju svesti korisnika IKT sistema, organizujući obuku za svoje osoblje i podižući svest o sajber pretnjama, fišingu ili tehnikama socijalnog inženjeringa. I domaća zakonska regulativa daje sve značajniju podršku, ali i obavezu organizacijama da sprovode različite vidove obuka. Primere možemo naći od *Zakona o bezbednosti i zdravlju na radu*[38] (obavezuje poslodavca da, prilikom organizovanja rada i radnog procesa obezbedi različite vidove obuka zaposlenih), preko *Zakona o zaštiti od požara*[39] (uređuje obaveznu obuku zaposlenih putem programa osnovne obuke, kao i posebnu obuku za lica koja rade na poslovima zaštite od požara), do *Zakona o tajnosti podataka*[40] (kao jednu od opštih mera zaštite propisuje utvrđivanje posebnih programa obuke za potrebe obavljanja poslova zaštite tajnih podataka)[41], *Zakona o sprečavanju pranja novca i finansiranja terorizma*[42] (propisuje dužnost obveznika za donošenje programa o godišnjem stručnom obrazovanju, osposobljavanju i usavršavanju zaposlenih koji obavljaju poslove sprečavanja i otkrivanja pranja novca i finansiranja terorizma) i drugih propisa koji se odnose na poslove korporativne bezbednosti.

Pored sprovođenje radnji obuke koje se vrše u skladu sa zakonskim obavezama, kampanje podizanja svesti je potrebno preduzimati i na osnovu zahteva primenjenih bezbednosnih standarda i smernica, kompanijskih potreba, ali i shodno nedostacima konstatovanih sprovedenom unutrašnjom i/ili spoljnom kontrolom i revizijom, uzimajući u obzir poslovne aktivnosti i imajući u vidu postojeću organizacijsku kulturu i resurse. Prilikom planiranja programa obuke korisno je imati u vidu i nalaze istraživanja o sajber kulturi u RS koje je sproveo *RATEL* (koji obavlja poslove Nacionalnog CERT-a), prema kome

37 *OJ L 333*, 27.12.2022, p. 80.

38 Član 15. tačka 4. *Zakona o bezbednosti i zdravlju na radu*, „Službeni glasnik RS", br. 35/2023.

39 Članovi 53-55. *Zakona o zaštiti od požara,* „Službeni glasnik RS", br. 111/2009, 20/2015, 87/2018 i 87/2018 - dr. zakoni.

40 Član 32. tačka 12. *Zakona o tajnosti podataka*, „Službeni glasnik RS", br. 104/2009.

41 Primera radi navodimo da *Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka* sprovodi osnovnu obuku o bezbednosnoj kulturi, kao i druge vidove edukacije i obuke namenjene rukovodiocima, menadžerima i ostalim zaposlenima iz oblasti rada sa tajnim podacima (pogledati: http://www.nsa.gov.rs/tekst/80/obuke.php, 26.4.2024).

42 Član 5. tačka 4. *Zakona o sprečavanju pranja novca i finansiranja terorizma*, "Službeni glasnik RS", br. 113/2017, 91/2019, 153/2020 i 92/2023.

> *„čak 18% stalno zaposlenih ne zna da li krši interna pravila informacione bezbednosti svog poslodavca, iako znaju da pravila postoje, postavlja se pitanje o tome da li su pravila formulisana na razumljiv način? Dalje, 13% njih svesno krši ova pravila. Ovim istraživanjem nije ispitivana priroda kršenja ovih pravila – moguće je i da su ona za zaposlene na neki način sputavajuća, što bi ponovo dovelo u pitanje sam sadržaj ovih pravila."*[43]

Osim realizacije raznovrsnih obuka kao procesa poboljšanja učinka, bezbednosne veštine i svest zaposlenih se naročito razvijaju sprovođenjem različitih oblika vežbi i testiranja. Možemo napomenuti neke vidove vežbi koje se sprovode u praksi, a čije izvođenje je zahtev i mnogobrojnih propisa i standarda koji se odnose na poslove korporativne bezbednosti:

- evakuacije u slučaju nastupanja opasnosti ili udesa;
- vežbe postupaka u slučaju terorističke pretnje ili drugog oblika napada;
- vežbe sajber otpornosti;
- simulacija nastupanja krizne situacije;
- vežbovno gađanje vatrenim oružjem itd.

Redovnim sprovođenjem testova (proba) nad planovima kontinuiteta poslovanja, obezbeđenja, zaštite od požara, mobilizacije i drugim planovima, kao i probom bezbednosnih tehničkih sistema i opreme (tehničke zaštite, IKT i drugih tehničkih sistema), takođe se pozitivno utiče na povećanje svesti o značaju zaštitnih mera i kontrola.

Rad na ličnom razvoju menadžera korporativne bezbednosti, drugih menadžera i ostalih zaposlenih je neophodan faktor za podizanje opšte bezbednosne svesti i kulture. Unapređenje ličnih znanja i veština postiže se i putem posete sajmovima, prezentacijama i konferencijama, kakva je i jedna od vodećih u zemlji iz domena korporativne bezbednosti koju, sada već tradicionalno, organizuje *Srpska asocijacija menadžera korporativne bezbednosti (SAMKB)*[44]. Ovakve konferencije predstavljaju godišnje okupljanje struke menadžera korporativne bezbednosti sa međunarodnim učešćem menadžera iz javnog i privatnog sektora iz RS, zemalja u regionu i šire, sa

43 Istraživanje „*Sajber kultura u Srbiji*", Nacionalni CERT Republike Srbije, decembar 2020., str. 45 (http://www.cert.rs/files/shares/Sajber%20Kultura%20Ratel%20web%20V0.5.6.pdf, 2.2.2024.)

44 Više o asocijaciji *SAMKB* i konferenciji pogledati: http://www.korporativnabezbednost.rs/, 26.3.2024.

ciljem razmene iskustava i primera dobre prakse, kao i ukazivanjem na značaj uspostavljanja sistema korporativne bezbednosti u procesima upravljanja organizacijama, bez obzira da li pripadaju javnom ili privatnom sektoru, odnosno nezavisno od veličine ili delatnosti. Slične konferencije organizuju i strukovna udruženja zemalja u okruženju koja deluju i u okviru regionalne asocijacije za korporativnu bezbednost – *South-East Europe Corporate Security Association (SEECSA)*[45].

Možemo zaključiti da se uloga menadžmenta korporativnom bezbednošću ogleda u kreiranju koncepta obuke i programa podizanja svesti, u saradnji sa sektorom ljudskih resursa i drugim relevantnim internim i eksternim subjektima, a uz neizostavnu saglasnost i podršku top menadžmenta. Bitno je imati na umu da izgradnja bezbednosne kulture i svesti nije proizvod koji se može kupiti, već predstavlja neprekidni proces koji je potrebno permanentno planirati, sprovoditi i preispitivati kako bi se nivo kulture postepeno menjao u pravcu boljeg poimanja bezbednosnih rizika, kao i prihvatanja i primene propisanih mera i pravila od strane svih zaposlenih.

Bezbednosna agenda, ma koliko bila dobro zamišljena i velikodušno podržana, nije u stanju da se izdigne iznad loše bezbednosne prakse zaposlenih. Poput analogije sa slabom karikom u lancu, bezbednost organizacije ne može biti jača od najslabijeg svakodnevnog ponašanja njenih zaposlenih. Zato je jedan od najvažnijih zadataka bezbednosnog menadžmenta da utiče na ponašanje zaposlenih putem podizanja njihove svesti o postojanju i značaju bezbednosti. U tom smislu program podizanja svesti treba da ima za cilj da pomogne zaposlenima da razumeju svoje individualne bezbednosne odgovornosti, da ispune te odgovornosti i da se voljno angažuju na sprovođenju tih ciljeva.[46]

Ne postoji organizacija koja je potpuno imuna na raznovrsne ugrožavajuće faktore, niti je moguće sprovesti apsolutnu zaštitu. Međutim, praksa ukazuje da kada se problemi pojave, kada nastupe bezbednosni izazovi ili nastanu događaji sa štetnom posledicom po bezbednost ili otpornost, one organizacije koje su izabrale da uče iz njih kako bi smanjile verovatnoću da se incidenti ponove, ne tražeći primarno „žrtveno jagnje“ među zaposlenima, razvijaju pozitivnu bezbednosnu kulturu koja će afirmativno uticati na stav zaposlenih. Praksa je, takođe, ukazala da su razvijanje adekvatne komunikacije, doslednost u postupanju, kao i davanje odgovornosti zaposlenima nasuprot stigmatizacije, ključni za stvaranje pozitivne bezbednosne kulture.

45 Više o asocijaciji *SEECSA* pogledati: http://www.seecsa.org/, 26.3.2024.

46 Fay J. John, *Contemporary Security Management*, Third Edition, Butterworth-Heinemann, Burlington MA, 2011., str. 389 – 395.

Četvrto poglavlje

Digitalizacija korporativne bezbednosti

Sadržaj poglavlja

Inovacije u tehnološkim rešenjima - ključ za savremenu korporativnu bezbednost

Ubrzani razvoj tehnologije i sve složeniji bezbednosni izazovi zahtevaju od savremenih organizacija da neprestano unapređuju svoje sisteme zaštite. U ovakvom poslovnom okruženju, gde pretnje po korporativnu bezbednost evoluiraju brzinom kojom i tehnologija napreduje, inovacije u tehnološkim rešenjima postaju neizostavan deo strategije zaštite organizacija. Ova inovativna rešenja obuhvataju niz tehnologija i sistema koji ne samo da pomažu u identifikaciji i sprečavanju bezbednosnih

incidenata, već i obezbeđuju kontinuirani monitoring i unapređenje bezbednosnih procesa. Korporativna bezbednost više nije samo pitanje fizičke zaštite imovine i ljudskih resursa. Danas ona podrazumeva i zaštitu digitalnih podataka, intelektualne svojine i kritične infrastrukture koji su ključne za poslovanje. Sa porastom pretnji, kompanije su primorane da se oslanjaju na inovativna tehnološka rešenja koja su u stanju da reaguju na ove izazove na proaktivan i dinamičan način.

Inovacije kao što su primena veštačke inteligencije i Internet stvari (IoT) sada predstavljaju ključne elemente u izgradnji bezbednosnih sistema. Ovi napredni alati ne samo da omogućavaju bolju zaštitu korporativnih resursa, već i značajno doprinose efikasnosti i održivosti bezbednosnih procesa. U ovom kontekstu, kompanije koje integrišu inovacije u svoje bezbednosne strategije mogu očekivati da ostanu korak ispred pretnji i zadrže konkurentsku prednost u sve nepredvidljivijem poslovnom okruženju.[1]

U svetu koji se neprestano menja, gde tehnologija igra sve značajniju ulogu u svim aspektima poslovanja, održavanje visoke bezbednosti postaje sve veći izazov. Sve sofisticiranije pretnje i kompleksnije metode napada zahtevaju od organizacija da budu ne samo reaktivne već i proaktivne u zaštiti svojih resursa. U ovakvom okruženju, inovacije u tehnološkim rešenjima za korporativnu bezbednost postaju osnova na kojoj se grade efikasne strategije zaštite.Tradicionalne metode bezbednosti, koje su se ranije oslanjale na fizičke barijere i osnovne tehnike kontrole pristupa, više nisu dovoljne da zaštite savremene kompanije od novih tipova pretnji. Ove pretnje ne samo da mogu prouzrokovati direktnu materijalnu štetu, već i ozbiljno narušiti ugled i poverenje koje je kompanija izgradila kod svojih klijenata i partnera.

Upravo tu dolaze do izražaja inovacije u tehnološkim rešenjima. Tehnologije kao što su veštačka inteligencija i mašinsko učenje omogućavaju analizu ogromnih količina podataka u realnom vremenu, što znači da pretnje mogu biti otkrivene i neutralisane pre nego što izazovu ozbiljnu štetu. Napredna biometrijska autentikacija i dvofaktorska provera identiteta unose nove standarde u bezbednost pristupa, smanjujući mogućnosti za neovlašćen pristup osetljivim podacima. Internet stvari (IoT) i virtuelna realnost omogućavaju napredne metode monitoringa i obuke zaposlenih, što dodatno poboljšava operativnu efikasnost i brzinu odziva na potencijalne pretnje.

1 Matthews Taylor, „Taking action to safeguard IoT devices“, *Security Magazine*, 15.05.2024 (http://www.securitymagazine.com/keywords/5974-iot-security, 22.08.2024).

Uvodeći i integrišući ova inovativna rešenja, kompanije mogu ne samo da zaštite svoje resurse, već i da stvore bezbednosnu kulturu koja podstiče svest o bezbednosti među zaposlenima i gradi poverenje sa klijentima i partnerima. U takvom ambijentu, gde su bezbednosne pretnje neizbežne, inovacije u tehnološkim rešenjima za korporativnu bezbednost predstavljaju stratešku prednost koja kompanijama omogućava da ostanu korak ispred napadača i obezbede dugoročnu održivost svog poslovanja.[2]

Veštačka inteligencija u funkciji korporativne bezbednosti

Veštačka inteligencija (Artificial Intelligence - AI) sve više postaje ključni element savremenih bezbednosnih sistema, odnosno sistema tehničke zaštite sa posebnim akcentom na primenu kamera koje koriste AI tehnologiju. Ove kamere su daleko naprednije od tradicionalnih sistema video obezbeđenja, jer omogućavaju inteligentnu analizu video-sadržaja u realnom vremenu, identifikaciju potencijalnih pretnji i automatsko preduzimanje odgovarajućih mera. Prednosti primene kamera koje koriste AI u poslovima korporativne bezbednosti su brojne, počev od analize i prepoznavanja lica gde kamere sa tehnologijom veštačke inteligencije mogu automatski da prepoznaju i uporede lica u realnom vremenu sa bazama podataka, što omogućava brzu identifikaciju osoba.

Ova tehnologija se koristi u različitim scenarijima, od kontrole pristupa do sprečavanja kriminalnih aktivnosti u korporacijama. Primeri za to su otkrivanje anomalija i neobičnih ponašanja, gde AI kamere mogu da prepoznaju neuobičajene obrasce ponašanja, kao što su agresivni pokreti poput pokušaja upotrebe vatrenog oružja, ostavljanja predmeta u javnim prostorima ili kretanja u zabranjenim zonama.[3] Ove anomalije se automatski prijavljuju nadležnim službama kako bi se brzo reagovalo na potencijalne pretnje. Zahvaljujući veštačkoj inteligenciji, kamere mogu da prate kretanje specifičnih objekata ili osoba kroz više kamera u različitim zonama. Ova funkcija je posebno korisna u velikim infrastrukturama kao što su aerodromi, tržni centri i industrijski kompleksi.

2 Davenport H. Thomas, „Artificial Intelligence for the Real World, *Harvard Business Review*, 30.01.2018 (http://hbr.org/webinar/2018/02/artificial-intelligence-for-the-real-world, 18.08.2024).

3 „A first-of-its-kind AI solution to detect guns and gunshots“ (http://www.youtube.com/watch?v=_j94ErQD8Uo, 01.09.2024).

Kamere koje koriste AI tehnologiju se mogu integrisati sa drugim sistemima tehničke zaštite, kao što su alarmni sistemi i drugi sistemi detekcije, kako bi se stvorio sveobuhvatan bezbednosni okvir. Na primer, kada kamera prepozna sumnjivu aktivnost, ona može automatski da aktivira alarm ili obavesti nadležnu osobu. Kamere sa AI tehnologijom značajno redukuju potrebu za ljudskim nadzorom, čime se smanjuje mogućnost propusta i povećava brzina reakcije na potencijalne pretnje. U tom smislu veštačka inteligencija u sistemima tehničke zaštite, sa fokusom na kamere i druge elemente sistema video obezbeđenja, predstavlja revolucionarni korak ka unapređenju korporativne bezbednosti. Ove tehnologije ne samo da poboljšavaju efikasnost i tačnost bezbednosnih procesa, već omogućavaju kompanijama i da bolje zaštite svoju imovinu, informacije i osoblje. Sa nastavkom razvoja i primene AI u bezbednosti, očekuje se da će ove tehnologije postati standard u modernom poslovanju samom primenom strategije korišćenja vešatčke inteligencije u Republici Srbiji[4].

U velikim industrijskim kompleksima, gde su operativni procesi složeni i gde rade stotine ili hiljade zaposlenih, bezbednost i zdravlje na radu (BZR) predstavljaju jedan od najvažnijih aspekata korporativne bezbednosti. Sa napretkom tehnologije, posebno veštačke inteligencije, značajno su unapređeni mehanizmi za sprečavanje incidenata, otkrivanje opasnosti i povećanje ukupne bezbednosti u radnom okruženju. Kamere na bazi AI tehnologije mogu da prate radnike u realnom vremenu, identifikuju potencijalno opasne radnje i automatski obaveštavaju nadležne službe ili samog radnika o kršenju bezbednosnih procedura. AI kamere mogu automatski da detektuju da li zaposleni nose odgovarajuću zaštitnu opremu, kao što su šlemovi, rukavice i zaštitne naočare. Sistemi zasnovani na veštačkoj inteligenciji mogu da identifikuju opasna ponašanja, kao što su prebrzo kretanje u blizini mašina, rad na visini bez osiguranja ili rad u zabranjenim zonama.Ukoliko neki zaposleni ili radnik uslužnog preduzeća ne nosi neophodnu opremu, sistem može automatski da pokrene alarm ili obavesti nadležno lice, čime se značajno smanjuje rizik od povreda. Ovo je posebno korisno u visokorizičnim granama kao što su naftna i gasna industrija,

4 *Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godina*, Vlada Republike Srbije, Beograd, decembar 2019. godine ("Službeni glasnik RS", br. 96/2019). Strategija u tački 2. definiše veštačku inteligenciju na sledeći način: „Veštačka inteligencija (VI) odnosi se na sisteme koji pokazuju razumno, inteligentno, ponašanje na osnovu analize svog okruženja i donose odluke – sa određenim stepenom autonomije – da ostvare konkretne ciljeve. Sistemi zasnovani na veštačkoj inteligenciji mogu biti bazirani isključivo na softveru i delovati u virtuelnom svetu (na primer, virtuelni asistenti, softveri za analizu fotografija, internet pretraživači, sistemi za prepoznavanje govora i lica) ili mogu biti ugrađeni u uređaje – hardver (na primer, napredni roboti, autonomna vozila, dronovi i slično)".

hemijske fabrike i proizvodni pogoni, gde je prisustvo opasnih materija i mašina uobičajeno.[5]

Veštačka inteligencija može biti korišćena i u edukaciji i obuci zaposlenih za bezbedan rad. Virtuelna realnost (VR) i proširena realnost (AR) su tehnologije koje, uz pomoć AI, mogu da simuliraju stvarne situacije u kojima se zaposleni mogu naći i tako ih na bezbedan način obuče za reagovanje u slučaju opasnosti. AI sistemi mogu takođe da analiziraju radne aktivnosti i predlože dodatnu obuku za zaposlene koji pokazuju znakove nepoznavanja bezbednosnih procedura. Ovo osigurava da svi zaposleni uvek budu u toku sa najnovijim bezbednosnim standardima i procedurama. AI sistemi mogu biti integrisani sa sistemima za kontrolu pristupa kako bi se obezbedilo da samo ovlašćena lica imaju pristup visokorizičnim zonama. Ovo sprečava potencijalno opasne situacije, kao što su slučajni ulazi u zone sa opasnim materijalima. Bez obzira na način primene, razvoj i upotreba veštačke inteligencije traba da bude u skladu sa etičkim smernicama donetih od strane Vlade Republike Srbije.[6]

Kao što smo zaključili u ovom poglavlju priručnika, veštačka inteligencija igra sve značajniju ulogu u oblasti bezbednosti i zdravlja na radu u velikim industrijama, doprinoseći smanjenju rizika od povreda, unapređenju radnih procesa i osiguravanju ukupne korporativne bezbednosti. Kako se razvoj ove tehnologije nastavlja, njena primena će postati još šire rasprostranjena, omogućavajući poslovnim subjektima da stvore sigurnije i efikasnije radno okruženje.

Primena internet stvari (IoT) u korporativnoj bezbednosti

Primena Interneta stvari (Internet of things - IoT) u korporativnoj bezbednosti je širok i duboko integrisan proces koji obuhvata više oblasti tehnoloških inovacija. S obzirom na to da IoT podrazumeva umrežavanje fizičkih uređaja, senzora i softvera, svaki aspekt korporativne bezbednosti može se automatizovati i poboljšati preko inteligentnih sistema koji komuniciraju u realnom vremenu. S obzirom da „pametno" video nadgledanje zauzima sve veću upotrebu u poslovima korporativne bezbednosti, kamere koje podržavaju IoT tehnologiju omogućavaju nadgledanje u

5 „How to improve workplace safety with AI Monitoring" (http://www.youtube.com/watch?v=qN6nnJ8ncL0, 18.09.2024).

6 *Zaključak o usvajanju Etičkih smernica za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije*, „Službeni glasnik RS", br. 23/2023.

realnom vremenu i automatsko reagovanje na potencijalne incidente. Kamere koriste edge kompjuting kako bi procesirale podatke na samoj lokaciji, što znači da se slika i video materijal analiziraju lokalno pre slanja podataka na centralizovani server, omogućavajući bržu detekciju sumnjivih aktivnosti i automatske reakcije, kao što je pokretanje alarma ili zaključavanje vrata. Ugrađena veštačka inteligencija u IoT kamere omogućava analizu velikih količina video sadržaja bez potrebe za ljudskom intervencijom. Na primer, sistemi mogu identifikovati određene događaje kao što su pokušaji krađe, upad ili neovlašćeno kretanje po prostorijama nakon radnog vremena. Kamere mogu aktivirati alarme ili poslati upozorenje obezbeđenju ukoliko otkriju nepravilne ili sumnjive radnje. Pored toga, IoT video sistemi se mogu koristiti za učenje uobičajenih obrazaca kretanja zaposlenih i posetilaca, a zatim prepoznavati svaki odstupajući obrazac. Ova funkcionalnost je posebno korisna u objektima kao što su banke, gde je kontinuirano praćenje aktivnosti ključno za sigurnost. IoT uređaji koji upravljaju kontrolom pristupa obezbeđuju veoma fleksibilnu i bezbednu infrastrukturu za kompanije. Biometrijski sistemi kao što su skeneri za otiske prstiju, lice, iris ili glas mogu biti integrisani u IoT mrežu, omogućavajući personalizovanu kontrolu pristupa. Ovi sistemi osiguravaju da samo ovlašćene osobe mogu ući u određene prostore, a biometrijsku autentifikaciju je skoro nemoguće falsifikovati, što je čini mnogo sigurnijom od tradicionalnih metoda kao što su ključevi ili kartice. Ovi sistemi često koriste multifaktorsku autentifikaciju, odnosno kombinaciju više metoda, kao što su biometrijski identifikator i RFID kartica, što je posebno korisno u visokobezbednim objektima.[7]

Sistemi za kontrolu pristupa u funkciji IoT tehnologije takođe omogućavaju daljinsko upravljanje pristupom u realnom vremenu. Ovlašćena lica mogu dodeliti ili oduzeti pristup osobama preko mobilne aplikacije ili kompjutera, čak i ako nisu fizički prisutni na lokaciji. Svi događaji povezani sa kontrolom pristupa se beleže i mogu se analizirati radi identifikacije potencijalnih bezbednosnih propusta. Senzori iz segmenta IoT tehnologije koji prate fizičke uslove u objektima igraju važnu ulogu u zaštiti zaposlenih i infrastrukture od različitih opasnosti. Senzori za temperaturu i vlažnost u velikim zgradama, skladištima ili proizvodnim pogonima prate parametre poput temperature i vlažnosti vazduha. Ako ovi parametri pređu bezbednosne granice, sistem može automatski aktivirati mere zaštite kao što su aktiviranje ventilacije ili sistema za hlađenje. U hemijskoj industriji ili skladištima sa toksičnim supstancama, IoT senzori mogu otkriti curenje gasa ili pojavu opasnih materija i

7 „Biometrijska autentikacija kao siguran način zaštite identiteta“, *NetSet Global Solutions*, (http://www.netsetglobal.rs/biometrijska-autentikacija/, 21.09. 2024).

aktivirati alarme ili sisteme za uklanjanje takvih materija. Ovakav automatizovani sistem je ključan za sprečavanje incidenata kao što su eksplozije ili trovanja. „Pametni" detektori dima povezani su sa centralizovanim sistemom koji može automatski poslati signal vatrogasnim službama, aktivirati sisteme za gašenje požara i evakuaciju. Ovi sistemi koriste kombinaciju senzora za toplotu, detekciju dima i vizuelno praćenje kako bi se odmah reagovalo na izvor požara. Integracija različitih senzora i alarmnih uređaja u IoT ekosistem omogućava unapređene mere automatske zaštite. IoT platforma može upravljati višestrukim vrstama alarmnih sistema, kao što su detektori pokreta, senzori za otvaranje vrata i prozora, kao i senzori za lomljenje stakla. Kada se detektuje neki od ovih događaja, sistem može aktivirati određene akcije kao što su zaključavanje prostorija ili slanje upozorenja. IoT takođe omogućava alarmnim sistemima direktnu komunikaciju sa lokalnim bezbednosnim službama, omogućavajući trenutnu reakciju na incidente. Na primer, ako senzori detektuju provalu, alarm automatski šalje upozorenje nadležnim službama i može pokrenuti zaključavanje objekta. IoT generiše ogromnu količinu podataka koji se mogu obraditi i analizirati kako bi se poboljšala efikasnost sistema bezbednosti. Zahvaljujući Big Data pristupu, IoT sistemi mogu analizirati podatke iz prošlosti i identifikovati obrasce koji mogu ukazivati na potencijalne pretnje.[8]

Mašinsko učenje omogućava sistemima da postanu pametniji kako više podataka ulazi u sistem, što znači da vremenom mogu preciznije predviđati i sprečavati rizike. U velikim kompanijama, IoT senzori mogu analizirati kretanje ljudi unutar objekata i prilagoditi mere zaštite na osnovu prethodnih obrazaca. Ako sistem primeti neobično kretanje, kao što je pristup osetljivoj zoni van radnog vremena, može poslati upozorenje bezbednosnom timu ili automatski blokirati pristup.

IoT sistemi za bezbednost mogu se integrisati sa drugim korporativnim sistemima kao što su ERP sistemi ili sistemi za upravljanje rizicima, čime se omogućava bolja koordinacija i prevencija rizika na svim nivoima. Ova interoperabilnost omogućava kompanijama da postignu veću efikasnost i transparentnost u planiranju i upravljanju bezbednosnim merama, što je ključno za moderno upravljanje rizicima i bezbednošću. Treba imati u vidu i da je očuvanje bezbednosti samih IoT-a sistema izazovno, kao i zaštita povezanih uređaja od čestih bezbednosnih propusta. IoT-a prati proizvođače uređaja tokom celog životnog ciklusa proizvoda, na šta treba posebno obratiti pažnju.[9]

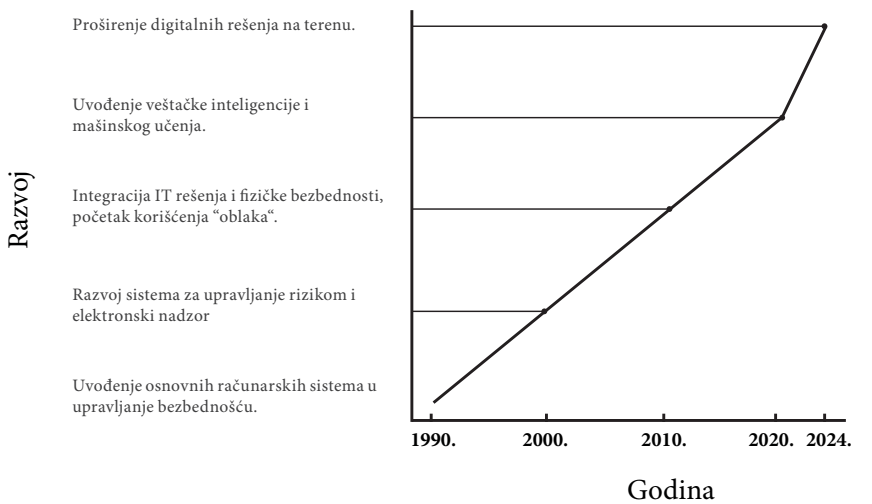
8 Kranz Maciej, *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry*, Wiley, Hoboken NJ, 2016, pp. 183-186..

9 „Industry-Leading Security for Evolving IoT Threats" (http://www.silabs.com/security,

Digitalizacija u funkciji korporativne bezbednosti

Digitalizacija u funkciji korporativne bezbednosti podrazumeva integraciju savremenih digitalnih tehnologija u sve aspekte bezbednosnih procesa unutar korporacije. Ovaj proces ne predstavlja samo tehnološku promenu, već i sveobuhvatnu transformaciju načina na koji kompanije pristupaju zaštiti svojih resursa, informacija i ljudi. U današnjem globalizovanom i sve više digitalnom okruženju, korporacije se suočavaju sa potrebom da digitalizuju svoje sektore, pa tako i segmente korporativne bezbednosti.

Dokumentovanje procesa u korporativnoj bezbedosti su evoluirali od ručnog beleženja podataka olovkom na papiru, preko digitalizacije pomoću softvera, do savremene primene veštačke inteligencije za automatizaciju i unapređenje analize podataka.



Slika 4.1. Hronološki razvoj digitalizacije korporativne bezbednosti

Kao što se može videti na Slici 4.1. u poslednjih nekoliko decenija je digitalizacija korporativne bezbednosti prošla kroz nekoliko ključnih faza razvoja kako bi odgovorila na rastuće potrebe za bezbednošću u dinamičnom poslovnom okruženju.[10]

03.09.2024).

10 „Security Info Watch, Emerging Security Technologies" (http://www.securityinfowatch.com/, 03.09.2024).

Sledeći grafikon prikazuje ove faze, počevši od uvođenja osnovnih računarskih sistema 1990-ih godina, pa sve do primene veštačke inteligencije i digitalnih rešenja na terenu do 2024. godine:

1990-e: Uvođenje osnovnih računarskih sistema u upravljanje bezbednošću.Tokom ovog perioda, kompanije su počele koristiti računare za upravljanje bezbednosnim sistemima, prelazeći sa manuelnih procedura na automatizovane sisteme. Ova digitalna transformacija je omogućila centralizaciju informacija i efikasnije upravljanje podacima o bezbednosti.

2000-e: Razvoj sistema za upravljanje rizikom i elektronski nadzor. Početkom 2000-ih dolazi do uvođenja naprednijih sistema za upravljanje rizicima. Elektronski sistemi za nadzor omogućili su prikupljanje podataka u realnom vremenu i njihovu analizu, što je unapredilo identifikaciju i odgovor na bezbednosne pretnje. Ova faza označava prelazak na sofisticiranije alate za nadgledanje i kontrolu.

2010-e: Integracija IT rešenja i fizičke bezbednosti, početak korišćenja" oblaka". U ovom periodu svedoci smo sve veće integracije IT sistema sa fizičkom bezbednošću. Korišćenje ovakvih rešenja olakšava obradu velikih količina podataka i omogućava udaljeni pristup informacijama, čime se povećava efikasnost bezbednosnih operacija.

2020-e: Uvođenje veštačke inteligencije i mašinskog učenja.Tehnološki napredak u oblasti veštačke inteligencije (AI) i mašinskog učenja (ML) dovodi do transformacije u analizi i prepoznavanju bezbednosnih pretnji. Ove tehnologije omogućavaju automatizovanu detekciju anomalija i prediktivnu analitiku, čime se značajno poboljšava sposobnost preduzeća da preventivno reaguje na potencijalne rizike.

2024: Proširenje digitalnih rešenja u praksi. Najnoviji trendovi u digitalizaciji bezbednosti fokusiraju se na primenu naprednih tehnologija direktno na terenu. Ovo uključuje implementaciju mrežnih senzora, autonomnih sistema i interaktivnih uređaja koji omogućavaju bržu reakciju i bolju povezanost svih segmenata bezbednosnih operacija u realnom vremenu. Ovaj hronološki razvoj nam pokazuje kako se tehnologija kontinuirano razvijala kroz evoluciju istorije digitalne transformacije, od pre-interneta do generativne veštačke inteligencije kako bi odgovorila na izazove korporativne bezbednosti. Takođe, to nam ukazuje na važnost stalne modernizacije i prilagođavanja novih tehnoloških rešenja kako bi se održala adekvatna bezbednost u poslovnom okruženju. Savremeni pristup korporativnoj bezbednosti se brzo razvija i zahteva da kompanije budu spremne da primene digitalna rešenja kako bi ostale korak ispred potencijalnih pretnji. Digitalizacija omogućava korporacijama

da poboljšaju svoju sposobnost da identifikuju, analiziraju i reaguju na rizike na način koji je daleko efikasniji i brži od tradicionalnih metoda.

Modeliranje digitalnih bezbednosnih procesa

Digitalizacija bezbednosnih procesa predstavlja produžetak sveopšte digitalne transformacije korporativnih struktura, koja donosi nove mogućnosti za poboljšanje efikasnosti, preciznosti i otpornosti bezbednosnih sistema. Za razliku od ranijih pristupa koji su se oslanjali na fragmentirane i često ručne procese, današnji digitalni modeli za zaštitu obuhvataju punu integraciju svih bezbednosnih aktivnosti i resursa u jedan koherentan, fleksibilan i automatizovan sistem.

Modeliranje ovih procesa za potrebe digitalizacije podrazumeva kreiranje strukturalnih i funkcionalnih okvira koji definišu kako različite komponente zaštite rade zajedno u digitalnom okruženju. Ovo omogućava organizacijama da vizualizuju, planiraju i optimizuju svoje bezbednosne aktivnosti koristeći savremene tehnologije. Modeliranje zauzima važnu ulogu u identifikaciji rizika, kreiranju strategija za odgovor na pretnje i implementaciji sistemskih rešenja za održavanje bezbednosti na potrebnom nivou.

Osnovni elementi u modeliranju digitalnih procesa

U početne korake modeliranja ulazi identifikacija i analiza pretnji, opasnosti i ranjivosti. Korišćenjem alata za prediktivnu analitiku, sistemi mogu automatski analizirati istorijske podatke i na osnovu toga predvideti moguće incidente.[11] Pored toga, modeliranje uključuje i definisanje metoda za brzo prepoznavanje anomalija u ponašanju ili u sistemu, što olakšava proaktivno reagovanje.[12]

Ne manje važan segment digitalizacije je automatizacija procesa reagovanja na pretnje i opasnosti. U modelu procedura i sistema fizičko-tehničke zaštite, automatizovani odgovori su zasnovani na unapred definisanim pravilima koja određuju način reagovanja na različite situacije (npr. automatsko zatvaranje vrata, aktiviranje alarma, obaveštavanje bezbednosnih timova).

11 „Digital Transformation: How to Scope and Eecute Strategy“ (http://www.gartner.com/en/information-technology/topics/digital-transformation, 14.09. 2024.

12 ARIS Express – Free Modeling Software (http://www.ariscommunity.com/aris-express, 10.09. 2024).

Modeliranje uključuje i simulacije koje omogućavaju testiranje različitih scenarija pretnji i opasnosti. Ovo pomaže da se otkriju slabe tačke u sistemu i poboljša strategija reagovanja. Simulacije mogu uključivati razne scenarije, poput sajber napada, fizičkog upada, ili incidenta u vezi sa internim pretnjama.

Faza planiranja u procesu modeliranja digitalnih sistema obezbeđenja

Modeliranje podrazumeva fazno izvođenje, pri čemu se u fazi planiranja identifikuju svi rizici i definišu bezbednosni ciljevi. Takođe se planiraju resursi potrebni za implementaciju digitalnih rešenja, kao što su ljudski potencijali, tehnička infrastruktura i softverska podrška. Dobro osmišljen plan omogućava bolju kontrolu rizika i obezbeđuje da sistem bude otporan na pretnje i u skladu sa regulatornim zahtevima.

Nakon identifikacije rizika, prelazi se na definisanje bezbednosnih ciljeva. Ovi ciljevi obuhvataju poverljivost, integritet i dostupnost podataka. Poverljivost se odnosi na zaštitu podataka od neovlašćenog pristupa, integritet obezbeđuje da podaci ne budu neovlašćeno izmenjeni, dok je dostupnost ključna za osiguranje da su podaci i sistemi dostupni onda kada su potrebni. Pored tehničkih ciljeva, važno je i da se sistem uskladi sa pravnim i regulatornim zahtevima, kao što su GDPR ili zahtevima standarda poput ISO 27001.

U ovom delu se odlučuje koje će tehnologije i alati biti korišćeni za zaštitu sistema, na primer poput softvera za enkripciju, kontrolu pristupa i sisteme za monitoring pretnji. Takođe se razvijaju planovi za reagovanje na incidente, koji uključuju procedure za otkrivanje, reagovanje i oporavak nakon potencijalnih sajber napada.[13]

Strategija takođe predviđa kontinuirano unapređenje sistema na osnovu novih pretnji i tehnoloških inovacija. Praksa je ukazala da je korisno da se sve aktivnosti i planovi detaljno dokumentuju u okviru sveobuhvatne dokumentacije, koja će služiti kao referentni dokument za sve učesnike u projektu. Ova dokumentacija obuhvata analizu rizika, definisane bezbednosne ciljeve, resurse i strategije, kao i planove za odgovor na incidente.

13 *Studija izvodljivosti uspostavljanja procedura nacionalnog CERT-a i upravljanja sistemom za prijavu incidenata*, RATEL, Beograd 2018.

Faza dizajna

Sledeća faza kreiranja digitalnog modela uključuje dizajn sistema koji je modularno fleksibilan i omogućava buduće nadogradnje. To podrazumeva definisanje protokola za kontrolu pristupa, integraciju IoT uređaja i korišćenje AI i mašinskog učenja za prediktivnu analitiku.

Prvi aspekt dizajna je modularnost sistema, što znači da je sistem podeljen na nezavisne, ali povezane delove. Ovaj pristup omogućava da svaki modul funkcioniše samostalno, što znači da u slučaju nadogradnje ili izmene jednog dela sistema, ostali delovi mogu nastaviti normalno da rade. Modularnost je važna jer omogućava lako prilagođavanje novim potrebama, uvođenje novih bezbednosnih mera i unapređenje postojećih komponenti bez značajnih izmena u celokupnoj strukturi sistema. Arhitektura sistema je sledeći ključni aspekt dizajna. Ona obuhvata način na koji različiti bezbednosni elementi (na primer kao što su fajervolovi, sistemi za otkrivanje upada, enkripcija i upravljanje rizicima) komuniciraju i sarađuju u cilju zaštite sistema. Ovde se definiše kako će sistem funkcionisati u celini, integrišući sve njegove delove u jednu koordinisanu celinu koja omogućava efikasnu zaštitu od pretnji, ujedno povećavajući otpornost. Skalabilnost je takođe važan aspekt dizajna. Digitalni sistem mora biti dizajniran tako da se lako može prilagoditi rastu organizacije ili promenama u tehnološkom okruženju. Ovo znači da sistem mora biti u mogućnosti da obradi veći broj korisnika, više podataka ili složenije pretnje, bez potrebe za potpunom rekonstrukcijom osnovne strukture. Skalabilnost omogućava da sistem ostane efikasan i otporan na nove izazove i pretnje kako se razvijaju sa vremenom.

Pored navedenog, važan aspekt je interoperabilnost. Budući da digitalni sistemi često moraju da funkcionišu u heterogenim okruženjima, sistem mora biti dizajniran tako da podržava komunikaciju i saradnju između različitih tehnologija i platformi. Ovo omogućava lako integrisanje sistema bezbednosti sa postojećim infrastrukturama unutar organizacije, kao i sa spoljnim sistemima i alatima, obezbeđujući efikasnu saradnju i razmenu podataka.U dizajnu se takođe postavljaju bezbednosne politike i kontrole, koje definišu kako će sistem upravljati pristupom, autentifikacijom i nadzorom. To uključuje mere poput dvofaktorske autentifikacije, enkripcije podataka i politika za kontrolu pristupa osetljivim informacijama. Važan deo ovog aspekta je i uvođenje mehanizama za automatsko reagovanje na bezbednosne incidente, kao i sistema za evidenciju i praćenje aktivnosti u cilju otkrivanja potencijalnih pretnji.

Na kraju, dizajn mora da prođe kroz proces testiranja i validacije, kako bi se osiguralo da sve komponente sistema funkcionišu u skladu sa planiranim ciljevima. Ovo uključuje simulaciju različitih bezbednosnih scenarija i testiranje kako sistem reaguje na različite tipove napada. Validacija podrazumeva proveru kompatibilnosti svih komponenti i usklađenost sa definisanim bezbednosnim standardima i regulativama.

Faza implementacije

Ova faza podrazumeva praktičnu primenu modela kroz instalaciju neophodne opreme i softvera. Potrebno je i uspostaviti standarde za bezbednost podataka i praćenje aktivnosti u realnom vremenu. Faza implementacije u procesu modeliranja predstavlja neophodan korak u kojem se teorijski model pretvara u praktičnu realnost. U ovoj fazi, vrši se instalacija neophodne opreme i softvera, kao i konfiguracija sistema u skladu sa prethodno definisanim arhitektonskim rešenjima i bezbednosnim politikama.

Prvi korak u implementaciji podrazumeva postavljanje hardvera, uključujući servere, mrežne uređaje i skladišta za podatke, koji se konfigurišu tako da osiguraju siguran i pouzdan rad sistema. Paralelno sa tim, instaliraju se i softverski alati poput fajervolova, antivirusa, sistema za otkrivanje i sprečavanje upada (IDS/IPS), kao i softver za enkripciju podataka. Ovi alati se konfigurišu tako da funkcionišu u skladu sa utvrđenim bezbednosnim standardima i politikama. Uspostavljanje bezbednosnih tehničkih standarda je sledeći važan korak. To obuhvata primenu pravila za kontrolu pristupa, autentifikaciju korisnika, zaštitu podataka i definisanje politika za obradu i skladištenje osetljivih informacija. Ove mere su ključne za sprečavanje neovlašćenog pristupa podacima i resursa, i osiguravaju da sistem radi u skladu sa najvišim standardima zaštite. Praćenje aktivnosti u realnom vremenu je jedan od ključnih elemenata implementacije. Uspostavljaju se sistemi za monitoring koji kontinuirano prate mrežni saobraćaj, aktivnosti korisnika i integritet sistema, detektujući potencijalne pretnje i reagujući na njih u stvarnom vremenu. Ovi sistemi omogućavaju brzu reakciju na primer na sajber-napade, dok ujedno evidentiraju i analiziraju sve sumnjive aktivnosti.Nakon instalacije i konfiguracije sistema, sprovodi se testiranje kako bi se osiguralo da sve komponente funkcionišu u skladu sa predviđenim parametrima. Testiranje uključuje simulaciju mogućih napada i stres-testove koji osiguravaju stabilnost i otpornost sistema na pretnje. Time se eliminišu sve potencijalne slabosti pre konačne operativne primene.Na kraju, neophodno je organizovati obuku korisnika

kako bi se upoznali sa novim bezbednosnim standardima, procedurama i pravilnim korišćenjem sistema. Edukacija smanjuje rizik od ljudskih grešaka i osigurava da svi korisnici rade u skladu sa dokumentovanim protokolima, što je presudno za održavanje stabilnosti i bezbednosti sistema.[14]

Faza monitoringa i optimizacije

Nakon implementacije, sistem mora biti kontinuirano praćen i optimizovan na osnovu stvarnih podataka. Redovno ažuriranje i prilagođavanje sistema omogućava dugoročnu efikasnost. Faza monitoringa i optimizacije predstavlja ključnu komponentu za održavanje i poboljšanje digitalnog sistema bezbednosti nakon njegove implementacije. U ovoj fazi, sistem se kontinuirano prati i analizira kako bi se osiguralo njegovo optimalno funkcionisanje i brzo reagovanje na potencijalne pretnje.

Faza podrazumeva kontinuirani monitoring sistema, koji omogućava praćenje svih aktivnosti u realnom vremenu, uključujući mrežni saobraćaj, pokušaje pristupa i druge aktivnosti korisnika. Ovaj proces omogućava blagovremeno otkrivanje sumnjivih radnji i preduzimanje neophodnih mera za sprečavanje potencijalnih incidenata. Nakon što se prikupe stvarni podaci o funkcionisanju sistema, vrši se optimizacija na osnovu tih informacija. Ovaj proces podrazumeva analizu podataka radi identifikovanja novih oblika pretnji ili mogućih slabosti u bezbednosnim merama. Takva analiza omogućava prilagođavanje i unapređenje sistema kako bi se osigurala njegova efikasnost i stabilnost. Jedan od ključnih aspekata ove faze je redovno ažuriranje sistema, što podrazumeva instaliranje novih softverskih zakrpa, poboljšanja hardvera i usklađivanje sa najnovijim bezbednosnim standardima. Ova ažuriranja su ključna za održavanje zaštite od novih vrsta sajber-pretnji, kao i za usklađivanje sa regulativama i bezbednosnim politikama. Pored reaktivnih mera, faza optimizacije uključuje i proaktivan pristup unapređenju sistema. Ovo znači da se redovno prate novi tehnološki trendovi i najbolje prakse kako bi sistem ostao ažuran i prilagođen budućim izazovima.

Proaktivna optimizacija osigurava da sistem bude spreman za sve vrste pretnji, pre nego što se one pojave. Veoma je važno sprovoditi periodične interne i eksterne revizije i provere sistema. Ovi pregledi omogućavaju detaljnu procenu rada sistema, identifikaciju slabih tačaka i daju preporuke za dalje unapređenje. Provere takođe pomažu u osiguravanju da sistem ostane u skladu sa propisima i najvišim standar-

14 Adams Malcolm, „Implementing NIST Cyber Security Framework: Step-by-Step Guide“, *BusinessTech Weekly*, 08.07.2023. (http://www.businesstechweekly.com/legal-and-compliance/nist/implementing-nist-cybersecurity-framework/, 29.08.2024).

dima bezbednosti. Modeliranje digitalnih procesa nastaviće da se razvija uz unapređenje tehnologija poput veštačke inteligencije, kvantnih računara i robotike. Ovaj razvoj će omogućiti stvaranje još naprednijih i bezbednijih sistema koji će moći da upravljaju sve složenijim pretnjama i rizicima. Kompanije koje budu uložile u razvoj modela digitalnih procesa biće bolje pripremljene za izazove budućnosti, omogućavajući im dugoročnu stabilnost i održivost u brzom i promenljivom poslovnom okruženju. Savremeni digitalni sistemi obezbeđenja omogućavaju veću prilagodljivost i skalabilnost u poređenju sa tradicionalnim modelima. Ovo je posebno važno za velike korporacije sa složenim bezbednosnim potrebama, kao što su multinacionalne kompanije koje posluju u više zemalja i okruženja. Digitalizacija omogućava da se bezbednosni procesi lako prilagođavaju specifičnim potrebama različitih lokacija ili delova objekata, uz istovremeno zadržavanje centralnog upravljanja i kontrole.

Proces upravljanja rizikom u digitalnom okruženju - Realno vreme i predikcija pretnji

Tradicionalno upravljanje rizikom obično se oslanjalo na periodičnu procenu koja je obuhvatala retrospektivnu analizu podataka. Digitalizovani sistemi prevazilaze ovu ograničenost time što neprekidno prate okolinu i prikupljaju podatke u realnom vremenu. Digitalizovani sistemi obezbeđenja pružaju sveobuhvatniji i dinamičniji pristup upravljanju rizicima, uz mogućnost realno-vremenskog praćenja, kategorizacije rizika, i predikcije budućih pretnji. Ovo uključuje podatke iz različitih izvora kao što su:

- sistemi video obezbeđenja, za kontrolu pristupa,
- sajber-bezbednosni alati,
- analiza anomalija u kretanju i ponašanju zaposlenih.

Ovi podaci se zatim obrađuju u realnom vremenu, omogućavajući brzu identifikaciju potencijalnih pretnji i opasnosti. Jedna od ključnih prednosti digitalnog sistema je mogućnost dinamičke procene rizika, koja omogućava da se rizici kontinuirano preispituju i procenjuju. Digitalizovani sistemi mogu integrisati različite metode procene rizika, od kojih poseban značaj imaju *metode scenarija*.[15]

15 *ISO/IEC 31010:2019, Risk management – Risk assessment techniques.*

Reč je o metodologiji koja se oslanja na stvaranje različitih scenarija (na primer, "šta ako" situacije) u cilju identifikacije potencijalnih rizika i njihovih posledica. Ovakav pristup omogućava organizacijama da razumeju potencijalne uticaje i planiraju odgovore. Algoritmi mašinskog učenja koji analiziraju velike količine podataka kako bi identifikovali ponavljajuće obrasce rizika od potencijalnih pretnji i opasnosti. Primena prediktivne analitike za utvrđivanje budućih rizika na osnovu trendova i ponašanja, čime se omogućava da se potencijalne pretnje i opasnosti identifikuju pre nego što postanu stvarni incidenti. Kontekstualizacija rizika na osnovu različitih faktora, kao što su vreme, lokacija i specifični profili pretnji.

Kategorizacija rizika u digitalizovanom sistemu ima značajnu ulogu u efikasnom upravljanju proaktivnim merama zaštite od pretnji i opasnosti. Ona omogućava da se resursi koriste optimalno, a odgovori na incidente prilagode ozbiljnosti situacije. Svaki nivo rizika zahteva drugačije mere, što omogućava kompanijama da reaguju brže i preciznije. Automatizacija malih rizika, pojačani nadzor srednjih i trenutna aktivacija bezbednosnih timova za visoke rizike čini sisteme efikasnijim i prilagodljivijim. Ovo ne samo da smanjuje troškove već i optimizuje ljudske i tehnološke resurse u zaštiti organizacije. Kako bi bolje razumeli razradićemo na primeru kako funkcioniše upravljanje malim, srednjim i visokim rizicima u ovom kontekstu.

a. Mali rizici u digitalnom sistemu

Mali rizici, kao što su neovlašćeni ulazi u manje važne zone, ne zahtevaju neposrednu ljudsku intervenciju, već se obrađuju kroz automatizaciju unutar sistema. Primer za ovo bi bio zaposleni koji greškom pokuša da uđe u zonu za koju nema odgovarajuće dozvole, npr „EX ZONE" u industiji. Automatsko praćenje i upozorenja, npr. sistemi za kontrolu pristupa mogu automatski evidentirati takav incident, poslati obaveštenje odgovornim osobama, ali ne zahtevaju hitno postupanje. To znači da će se slični incidenti pratiti kako bi se uočili potencijalni obrasci ili više puta ponavljani incidenti kako bi se pratila učestalost. Programi za samostalnu reakciju ili automatizacija omogućavaju da se mali rizici rešavaju bez uključivanja zaposlenih, korišćenjem protokola kao što su automatsko zaključavanje vrata ili upućivanje zaposlenog na verifikaciju propusnice pre ponovnog pokušaja ulaska. U nekim slučajevima, sistem može predložiti dodatnu obuku zaposlenih ako se isti tip greške ponavlja.Evidencija za dalju analizu je vrlo korisna gde se mali incidenti beleže i čuvaju u bazama podataka radi kasnije analize. Ako se neovlašćeni ulazi u istu zonu ponavljaju ili se incidenti nagomilavaju, sistem može podići nivo rizika na srednji ili visok.

b. Srednji rizici u digitalnom sistemu

Srednji rizici, kao što su sumnjivo ponašanje zaposlenih ili neobične aktivnosti na IKT mreži, zahtevaju brži odgovor, ali i dalje ne zahtevaju trenutnu reakciju službenika obezbeđenja. Ovakvi rizici se često tretiraju kroz kombinaciju automatizovanih i ljudskih reakcija.Pojačani nadzor i automatski protokoli pri pojavi srednjeg rizika, sistem može automatski uključiti dodatne mere nadzora, kao što su pojačana video-analitika ili aktivacija dodatnih senzora. Na primer, neobične aktivnosti na računarskoj mreži mogu pokrenuti protokol za privremenu blokadu pristupa ili verifikaciju identiteta.Obaveštenja srednjih rizika često aktiviraju alarme koji zahtevaju da bezbednosni timovi ili odgovorni zaposleni brzo reaguju.[16]

To može uključivati brzu proveru situacije, poput zahteva za dodatnim verifikacijama ili praćenje kretanja zaposlenih u određenoj zoni. U nekim slučajevima, sistem će poslati obaveštenje zaposlenima da ažuriraju svoje pristupne podatke ili ponovo prođu kroz proceduru verifikacije. Kao preventivna mera može da bude pokretanje istraga, u slučaju da se određeno ponašanje ponavlja, automatizovani sistemi mogu aktivirati dublju istragu od strane bezbednosnih timova. Ovo omogućava analizu ponašanja, prikupljanje dokaza i preduzimanje konkretnih mera kako bi se sprečio potencijalni veći rizik.

c. Visoki rizici u digitalnom sistemu

Visoki rizici, kao što su sajber-napadi ili fizički proboj zaštićenih objekata, zahtevaju trenutnu reakciju i uključivanje različitih nivoa bezbednosnog tima.

Automatska aktivacija hitnih mera predstavlja ključni mehanizam u digitalizovanim sistemima bezbednosti, koji momentalno reaguju pri detekciji visokog rizika. U ovakvim situacijama, sistemi automatski aktiviraju niz mera koje mogu uključivati trenutno zaključavanje prostorija, ograničavanje pristupa kritičnim podacima ili objektima, automatsko isključivanje određenih računarskih sistema ili pokretanje bek-ap sistema za zaštitu podataka. Ove mere su dizajnirane tako da obezbede brz i efikasan odgovor na potencijalne pretnje i spreče njihovo dalje širenje.Još jedan važan aspekt je integracija sa fizičkim obezbeđenjem, koja omogućava direktno uključivanje ljudskih resursa u slučaju visokog rizika. Digitalni sistemi u ovakvim situacijama momentalno alarmiraju timove fizičkog obezbeđenja. Ovo uključuje automatizovane mere poput alarma, ali i slanje bezbednosnih patrola ili angažovanje

16 „Levels of Risk Matrix“, Vector Solutions (http://www.vectorsolutions.com/resources/blogs/levels-of-a-risk-matrix/, 11.09.2024).

dodatnih timova koji su specijalizovani za rešavanje ovakvih incidenata. Ova integracija između digitalnih i fizičkih mera značajno povećava efikasnost odgovora na pretnje. Tokom kriznih situacija, realni monitoring i koordinacija između različitih bezbednosnih jedinica je od ključnog značaja. Sistemi za upravljanje incidentima pružaju praćenje svih aspekata incidenta u realnom vremenu, omogućavajući koordinaciju između digitalnih sistema i timova na terenu. Bezbednosni timovi mogu pratiti situaciju koristeći video-nadzor, podatke iz različitih senzora ili čak izveštaje zaposlenih koji su na licu mesta. Ovakav nivo koordinacije omogućava brzu i preciznu reakciju na sve vrste bezbednosnih pretnji. Posle završetka incidenta, neophodno je sprovesti detaljnu analitičku procenu kako bi se utvrdilo šta je dovelo do proboja i koje su mere bile najefikasnije.

Ovaj proces podrazumeva pregled svih dostupnih podataka, kao što su izveštaji, video-zapisi, aktivacije alarma i reakcije timova. Dubinska analiza pomaže u boljem razumevanju incidenta i identifikaciji mera koje je potrebno unaprediti kako bi se sprečili budući incidenti, čime se jača celokupni bezbednosni sistem.[17]

Digitalni alati za povećanje produktivnosti fizičkog obezebeđenja

Svet bezbednosti prolazi kroz brzu transformaciju zahvaljujući integraciji digitalnih alata i tehnologija. Tradicionalni pristupi fizičkoj zaštiti postaju manje efikasni, dok mobilne aplikacije povezane sa softverskim platformama pružaju mogućnost da se bezbednosni zadaci obavljaju brže, preciznije i sa manjom mogućnošću ljudskih grešaka.[18]

Ovo poglavlje ima za cilj da pojasni kako mobilna aplikacija za pripadnike fizičkog obezbeđenja može povećati produktivnost poslova fizičko-tehničke zaštite, kroz funkcije poput praćenja u realnom vremenu, automatskog generisanja izveštaja i analitike podataka. Sistem je dizajniran da olakša rad obezbeđenja, poboljša koordinaciju i obezbedi bržu reakciju u redovnim situacijama, a naročito u vanrednim i hitnim događajima.

Mobilna aplikacija za fizičko obezbeđenje

17 „Zaštita imovine na otvorenom prostoru bez infrastrukture“ (http://www.youtube.com/watch?v=r8NGNxtm9hI, 14.08.2024).

18 „Advanced Visitor Management System for Enterprises (http://www.youtube.com/watch?v=vx51DtgBEBQ, 09.08.2024).

Mobilna aplikacija predstavlja alat kojim se upravlja zadatkom svakog radnika obezbeđenja. Uz podršku softvera, ona omogućava brzo prikupljanje i analizu podataka o aktivnostima na terenu. Ključna prednost aplikacije je što omogućava punu mobilnost, omogućavajući radnicima da reaguju u realnom vremenu na promene u okruženju i bezbednosne incidente. Mobilna aplikacija za fizičko obezbeđenje predstavlja inovativni alat koji značajno unapređuje operativne sposobnosti radnika na terenu, poboljšavajući njihovu mobilnost i fleksibilnost. Mobilne aplikacije osiguravaju da svi službenici obezbeđenja budu neprestano povezani sa Kontrolnim centrom i dobijaju informacije u realnom vremenu, što im omogućava da reaguju na različite situacije na najbolji mogući način.

Pristup informacijama sa bilo koje lokacije predstavlja još jedan značajan aspekt mobilnosti. Radnici obezbeđenja mogu lako dobiti podatke o mapama objekta, procedurama reagovanja i upozorenjima o potencijalnim pretnjama. Dostupnost informacija im omogućava da donose informisane odluke u realnom vremenu, što je od velike važnosti u situacijama kada brzina reagovanja može odlučiti o ishodu incidenta. Mobilna aplikacija ne samo da čini radnike informisanim, već im takođe pruža alate potrebne za adekvatno upravljanje bezbednosnim zadacima. U situacijama kao što su alarmi, napadi ili bilo kakve sumnjive aktivnosti, radnici koji su u neposrednoj blizini lokacije incidenta mogu odmah dobiti obaveštenje o događaju. Ovo omogućava da se na incident odgovori odmah, čime se smanjuje rizik od eskalacije situacije.

Na primer, ako dođe do neovlašćenog ulaska u objekat, radnici sa štićenog objekta mogu odmah uputiti najbližu patrolu na tu lokaciju, a Kontrolni centar može biti obavešten u realnom vremenu. Fleksibilnost mobilne aplikacije omogućava menadžerima da brzo prilagođavaju patrolne rute u zavisnosti od aktuelnih informacija. Ako, na primer, dođe do promene u rasporedu ili uočenja novih rizika, menadžeri mogu odmah izmeniti zadatke bez potrebe za dugim procedurama. Ova mogućnost brze izmene zadataka i prilagođavanja na licu mesta značajno poboljšava operativnu fleksibilnost bezbednosnih timova, čineći ih sposobnijim da se nose s različitim izazovima. Smanjenjem zavisnosti od fiksnih sistema je još jedna prednost mobilne aplikacije.[19]

U tradicionalnim bezbednosnim sistemima, radnici često moraju da se vraćaju u centralu radi instrukcija, što usporava rad i povećava rizik od propusta. Mobilne aplikacije omogućavaju radnicima da ostanu na terenu, čime se minimizuje vreme

19 „The Future of Security Guard Operations", *Officer Reports* (http:/www./officerreports.com/blog/the-role-of-technology-in-security-guard-operations/, 02.09. 2024).

bez potrebe za kontaktom sa bazom. Ovo povećava njihovu produktivnost i osigurava da svi zadaci budu ispunjeni na vreme.

U praktičnom smislu, mobilne aplikacije imaju širok spektar primena. U hitnim intervencijama, kao što su požari, razbojništva ili druge krizne situacije, radnici mogu momentalno obavestiti druge članove tima i organizovati odgovor u kratkom vremenu. Takođe, tokom svakodnevnog rada, kada se jave nepredviđene situacije, radnici mogu prijaviti promene i dobiti nove instrukcije odmah, što ih čini značajno spremnijim za reagovanje. Ova inovacija ne samo da poboljšava operativne procese, već i značajno doprinosi većoj bezbednosti i ličnoj sigurnosti svih uključenih.

Softver za centralizovano upravljanje i analitika

Softverski deo sistema predstavlja centralni "hab "za praćenje i upravljanje svim aktivnostima. On integriše podatke iz mobilnih aplikacija, generiše izveštaje i omogućava naprednu analitiku. Podaci prikupljeni putem aplikacije uključuju sve događaje, patrole, incidente i druge aktivnosti, koji se zatim koriste za pravovremenu reakciju i strateško planiranje. Na taj način, sistem pruža sveobuhvatan uvid u bezbednosne aktivnosti, uključujući patrole, incidente i druge važne događaje.

Jedna od osnovnih funkcija softvera je generisanje detaljnih izveštaja koji obuhvataju sve prikupljene informacije. Ovi izveštaji su od suštinskog značaja za donošenje adekvatnih odluka, jer pružaju uvid u trendove, obrasce i potencijalne rizike. Na primer, analizom podataka o patrolama, mogu se identifikovati oblasti koje su više podložne incidentima ili gde je potrebno pojačano prisustvo osoblja. Ovakav uvid ne samo da pomaže u optimizaciji resursa, već i u poboljšanju bezbednosnih procedura. Kroz naprednu analitiku, softver omogućava prediktivno izveštavanje, što znači da može predvideti potencijalne incidente na osnovu istorijskih podataka. Na osnovu obrazaca u podacima, sistem može ukazati na verovatnoću pojave određenih događaja, kao što su upadi ili greške u bezbednosti. Ova prediktivna analiza igra važnu ulogu u strateškom planiranju, omogućavajući menadžerima da preduzmu proaktivne mere u cilju minimizovanja rizika.[20]

Softver omogućava upravljanje incidentima u realnom vremenu, što znači da se svi događaji mogu odmah beležiti i obrađivati. Kada se prijavi incident, sistem može automatski obavestiti odgovorne radnike i uputiti ih na lokaciju događaja, čime se ubrzava proces reagovanja. Ova funkcija značajno povećava efikasnost bezbedno-

20 „Bezbednosno procesno rešenje sa video sistemom" (http://www.youtube.com/watch?v=mIQHr1cevis, 19.08.2024).

snih timova i smanjuje vreme reagovanja, što može biti od presudnog značaja u kriznim situacijama. Dodatno, softver pruža mogućnosti za kontinuirano praćenje i evaluaciju bezbednosnih mera. Na osnovu prikupljenih podataka, menadžeri mogu analizirati efikasnost različitih strategija i procedura. Ovo podrazumeva upoređivanje različitih perioda, ocenu rezultata nakon implementacije novih mera i prilagođavanje strategija na osnovu stečenih iskustava.[21]

U suštini, softver za centralizovano upravljanje i analitiku ne samo da poboljšava operativnu efikasnost bezbednosnih timova, već doprinosi i sveobuhvatnom poboljšanju bezbednosnog okruženja. Softverom se podstiče strateško razmatranje bezbednosnih procedura, optimizuju se resursi i unapređuje se kvalitet usluga koje pružaju timovi fizičkog obezbeđenja. Softver predstavlja osnovu za moderno upravljanje bezbednošću, što omogućava organizacijama da budu bolje pripremljene za izazove u složenom i brzo promenljivom bezbednosnom okruženju.

Integracija inovacija u korporativnu strategiju bezbednosti

Uvođenje novih tehnologija u korporativnu bezbednost zahteva pažljivo planiranje i sistematski pristup, uključujući restrukturiranje organizacije, obuku kadrova, strateško planiranje i kontinuirano unapređenje. Uspešna implementacija novih tehnologija ne samo da poboljšava bezbednost, već može značajno povećati efikasnost i konkurentnost kompanije u savremenom poslovnom okruženju. Ovakav sistematski pristup obezbeđuje da inovacije ne samo da ispunjavaju trenutne potrebe, već i da su usmerene na buduće izazove i mogućnosti. Ovo poglavlje priručnika predstavlja primer za uspešnu implementaciju inovativnih rešenja u svakodnevne bezbednosne operacije.[22]

Prilagođavanje organizacionih struktura novim tehnologijama

Prilagođavanje organizacionih struktura u cilju integracije novih tehnologija podrazumeva stvaranje fleksibilnijih i dinamičnijih timova, optimizaciju postojećih procesa i uspostavljanje novih uloga. Ovo omogućava efikasnu saradnju između

21 http://www.youtube.com/watch?v=RBUBauFjCAU

22 Rogers L. David, *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*, Columbia Business School Publishing, New York NY 2016, pp. 273-280.

različitih sektora i osigurava da nove tehnologije budu integrisane na svim nivoima organizacije. U narednom delu teksta prikazaćemo osnovne korake primene.

Analiza trenutne organizacione strukture

Prvi korak u integraciji novih tehnologija u korporativnu bezbednost jeste procena postojeće organizacione strukture kako bi se identifikovale potencijalne prepreke. Neophodno je ispitati da li trenutna struktura podržava efikasnu saradnju između različitih sektora, uključujući sektore bezbednosti, IT-a i uprave, ili postoje oblasti koje mogu usporiti ili ometati integraciju novih rešenja.Upotreba analize procesa omogućava dublju procenu ovih interakcija i identifikaciju nedostataka u komunikaciji i koordinaciji. Na primer, ako sektor bezbednosti i IT nemaju redovnu i efikasnu saradnju, implementacija digitalnih bezbednosnih sistema može biti kompromitovana zbog loše integracije sa postojećim IT infrastrukturama. Takođe, ukoliko uprava nije aktivno uključena u proces ili nedovoljno podržava inicijative za tehnološke promene, može doći do kašnjenja u donošenju ključnih odluka. Analiza procesa otkriva te nedostatke i omogućava redefinisanje ključnih uloga i odgovornosti, kao i poboljšanje komunikacionih kanala, kako bi se omogućila brža i efikasnija integracija inovacija u postojeće sisteme.[23]

Uspostavljanje novih timova ili odeljenja

Praksa ukazuje, a način poslovanja uspešnih kompanija potvrđuje da za uspešnu implementaciju novih tehnologija, organizacije treba da formiraju posebne timove ili odeljenja koja će biti specijalizovana za upravljanje tehnološkim inovacijama. Ovi timovi treba da budu fokusirani na inovacije i prilagođavanje postojećih procesa, kao i na izgradnju novih kapaciteta unutar organizacije.Ovi timovi ne samo da objedinjuju tehničke eksperte i bezbednosne stručnjake, već uključuju i članove iz drugih odeljenja kao što su finansije, ljudski resursi i pravni sektor. Ovo omogućava multidimenzionalni pristup inovacijama i obezbeđuje da nove tehnologije budu implementirane u skladu sa finansijskim i pravnim zahtevima kompanije. Na primer, uvođenje tima koji bi se fokusirao na primenu veštačke inteligencije (AI) u sistemima tehničke zaštite i drugim nadzornim sistemima. Taj tim bi uključivao ne samo IT stručnjake, već i bezbednosne analitičare i pravne konsultante kako bi se osiguralo da su svi aspekti upotrebe AI usklađeni sa propisima i etičkim standardima. Ovaj

23 Laloux Frederic, *Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness*, Nelson Parker, Cambridge MA 2014.

pristup pomaže u pravovremenom rešavanju svih potencijalnih izazova, bilo da su tehnološki ili regulatorni, čime se poboljšava efikasnost i bezbednost.

Uvođenje novih uloga u kompaniji

Kako bi kompanije uspešno integrisale nove tehnologije i ostale konkurentne, praksa je ukazala na važnost kreiranja novih strateških i drugih potrebnih pozicija koje će voditi ovaj proces. Uloge kao što su direktor za inovacije ili službenik za digitalnu transformaciju postaju ključne u upravljanju tehnološkim promenama i osiguravanju da organizacija prati najnovije trendove. Upravljanje uvođenjem novih uloga u kompaniji podrazumeva niz važnih odgovornosti koje su usmerene na optimizaciju i integraciju novih tehnologija u poslovne procese. Praćenje tehnoloških inovacija predstavlja prvi korak u ovom procesu. Osobe na ovim pozicijama aktivno prate razvoj novih tehnologija i inovacija u bezbednosnoj industriji, kao i u drugim relevantnim sektorima. Njihov zadatak je da procene koje tehnologije mogu biti od koristi za kompaniju, kao i da analiziraju kako ih na najbolji način primeniti.

Sledeći aspekt je razvoj strategija za integraciju, i u tom smislu zaposleni koji su zaduženi za inovacije i digitalnu transformaciju formulišu i vode strategije za usvajanje novih tehnoloških rešenja. Ovo uključuje planiranje resursa, obuku zaposlenih i koordinaciju sa različitim odeljenjima. Kroz ovaj proces, stvara se čvrsta osnova za uspešnu implementaciju novih rešenja. Najvažaniji deo odgovornosti podrazumeva nadzor nad implementacijom. Njihova uloga uključuje stalno nadgledanje procesa integracije novih tehnologija u postojeće sisteme. Oni se staraju da tehnologije budu uspešno implementirane i da funkcionišu u skladu sa standardima, bez ometanja operativnih procesa. Ovim aktivnostima, osigurava se glatka tranzicija i maksimalna efikasnost u radu kompanije.[24]

Fleksibilnost i agilnost u organizaciji

Uspešna integracija novih tehnologija u kompaniji zahteva stvaranje fleksibilnih i agilnih timova koji su u stanju da brzo reaguju na izazove i prilagode se promenama. Ovi timovi, fokusirani na kratkoročne zadatke kao što su uvođenje inovacija ili rešavanje tehnoloških problema, omogućavaju organizaciji da brzo implementira nova rešenja, bez odugovlačenja izazvanog složenim procedurama odobravanja.Agilni timovi treba da imaju ovlašćenje da donose odluke u realnom vremenu,

24 Lencioni M. Patrick, *The Five Dysfunctions of a Team: A Workshop for Team Leaders*, Pfeiffer, San Francisco CA 2012, pp. 202-211

čime se izbegavaju nepotrebna odlaganja u primeni tehnologija. Ovaj način rada osigurava da kompanija ostane fleksibilna i prilagodljiva, jer se timovi mogu brzo reorganizovati i usmeriti na rešavanje novih problema koji se pojave tokom primene inovacija. Na primer, ako se pojavi potreba za brzom reakcijom u slučaju kiber napada, agilni tim će odmah pristupiti rešavanju problema, implementirajući neophodne mere zaštite i nova bezbednosna rešenja. Ovakva struktura omogućava organizaciji da reaguje efikasno i blagovremeno, čime povećava sigurnost i sposobnost prilagođavanja brzim promenama u tehnološkom okruženju.

Fleksibilnost i brzina prilagođavanja ovakvih timova ključni su faktori koji omogućavaju organizaciji da odgovori na savremene izazove i zadrži konkurentsku prednost u vremenu kada su inovacije neophodne za opstanak i razvoj.[25]

Interfunkcionalna komunikacija

Jačanje komunikacije između različitih sektora u kompaniji je od ključnog značaja za uspešnu integraciju novih tehnologija. Bez dobro organizovane saradnje, implementacija tehnoloških inovacija može biti otežana ili usporena zbog neusklađenosti i nedostatka koordinacije između sektora. Kako bi se izbegli ovi problemi, potrebno je uspostaviti redovnu komunikaciju između odeljenja kroz strukturisane sastanke i korišćenje modernih kolaborativnih alata koji omogućavaju razmenu informacija u realnom vremenu. Ovi alati i prakse omogućavaju da se zaposleni iz različitih sektora, poput bezbednosti, IT-a i uprave, lakše povezuju i sarađuju na zajedničkim projektima. Redovni sastanci omogućavaju bržu razmenu ideja i rešavanje potencijalnih problema koji se mogu javiti tokom primene novih tehnologija. Na taj način se osigurava da svi sektori rade u skladu sa zajedničkim ciljevima i da se nove tehnologije efikasno integrišu u postojeće sisteme. Ojačana komunikacija ne samo da ubrzava proces implementacije već i poboljšava ukupnu efikasnost organizacije, jer omogućava bolje razumevanje međusobnih potreba i izazova svakog sektora. Ovakav pristup olakšava prevazilaženje prepreka i omogućava kontinuiranu saradnju, što je ključno za uspešno usvajanje novih tehnologija u kompaniji.

25 „People & Organizational Performance, Mckinsey & Company (http://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/why-an-agile-transformation-office-is-your-ticket-to-real-and-lasting-impact, 22.08.2024).

Obuka kadrova za rad sa novim bezbednosnim tehnologijama

Obuka zaposlenih za rad sa novim tehnologijama je neophodna kako bi se obezbedila maksimalna efikasnost bezbednosnih sistema. Tehnologije mogu biti sofisticirane i zahtevaju specifična znanja i veštine, što znači da će zaposleni morati da se obuče ne samo kako bi se upoznali sa alatima, već i kako bi razvili kritičke sposobnosti za upravljanje rizicima.

Identifikacija potreba za obukom

Prvi korak u pripremi zaposlenih za rad sa novim tehnologijama je utvrđivanje koje veštine nedostaju u trenutnom kadru. Ovaj proces podrazumeva detaljnu analizu trenutnih sposobnosti zaposlenih i usklađivanje tih podataka sa zahtevima koje nove tehnologije donose. Pažljivo ispitivanje postojećih nivoa znanja i kompetencija omogućava identifikaciju konkretnih oblasti u kojima je potrebno dodatno usavršavanje. Nakon ove analize, kompanija može definisati specifične vidove obuka koji će omogućiti zaposlenima da se prilagode novim alatima i sistemima.

Na primer, ako organizacija planira da uvede sisteme za mašinsko učenje, zaposlenima će možda biti potrebna obuka iz oblasti analize podataka, kako bi razumeli osnove tehnologije, a ne samo njenu upotrebu. Na ovaj način, proces obuke ne samo da unapređuje tehničke veštine, već i podstiče dublje razumevanje novih rešenja, što doprinosi uspešnijoj i efikasnijoj integraciji tehnologija u radno okruženje. Ovakva identifikacija potreba za obukom je ključna za osiguranje da kompanija ima kvalifikovan kadar koji može maksimalno iskoristiti prednosti novih tehnologija, istovremeno smanjujući rizike od grešaka i neefikasnosti tokom primene.

Izrada kurikuluma obuke

Kreiranje efikasnog kurikuluma za obuku zaposlenih uvođenjem novih tehnologija zahteva pažljivo planiranje koje obuhvata i teorijske i praktične aspekte. Teorijski deo obuke treba da omogući zaposlenima upoznavanje sa principima funkcionisanja novih alata i programa u okviru bezbednosnih sistema i tehnologija, kako bi stekli osnovno razumevanje njihovih koncepata i primene. Ovaj deo programa obično uključuje predavanja, prezentacije i studije slučaja koji objašnjavaju kako tehnologija funkcioniše i zašto je bitna za organizaciju.S druge strane, praktični deo obuke fokusiran je na razvoj konkretnih veština kroz simulacije i rad na realnim

scenarijima. Na ovaj način, zaposleni mogu primeniti naučeno u kontrolisanom okruženju i steći sigurnost u korišćenju novih alata i sistema pre nego što ih primene u svakodnevnim radnim aktivnostima.

Dobra praksa ukazuje da program obuke treba biti podeljen u faze. Prva faza podrazumeva osnovnu obuku za sve zaposlene, u kojoj se svi upoznaju sa osnovnim konceptima novih tehnologija i dobijaju opšte veštine potrebne za njihovo korišćenje. U kasnijim fazama, napredni kursevi mogu biti ponuđeni specijalizovanim timovima koji će direktno raditi sa novim tehnologijama. Ovi napredni kursevi će obuhvatati dublje razumevanje i kompleksnije veštine, prilagođene potrebama stručnjaka iz različitih odeljenja. Ovakva podela u faze omogućava postepeno i temeljno usavršavanje veština, osiguravajući da svi zaposleni budu spremni za rad sa novim tehnologijama na različitim nivoima.[26]

Simulacije i praktične vežbe

Korišćenje simulacija realnih bezbednosnih incidenata predstavlja važan deo obuke zaposlenih pri uvođenju novih tehnologija. Simulacije omogućavaju zaposlenima da steknu praktično iskustvo u rešavanju različitih problema u kontrolisanom okruženju, što im pruža sigurnost u primeni novih alata i sistema u stvarnim situacijama. U okviru ovih vežbi mogu se simulirati scenariji poput sajber-napada, fizičkih pretnji ili kršenja bezbednosnih protokola, što zaposlenima daje priliku da reaguju na način koji će se od njih očekivati u realnim uslovima.

Na primer, ako kompanija uvodi sisteme zasnovane na veštačkoj inteligenciji, simulacije mogu pokazati kako sistem detektuje i reaguje na potencijalne pretnje i opasnosti u realnom vremenu. Ovo omogućava zaposlenima da nauče kako da efikasno koriste novi sistem, kako da tumače podatke koje dobijaju i kako da preduzmu odgovarajuće mere na osnovu automatskih upozorenja. Na ovaj način, simulacije ne samo da poboljšavaju razumevanje tehnologije, već i razvijaju veštine neophodne za brzo i adekvatno reagovanje u kritičnim situacijama. Praktične vežbe i simulacije omogućavaju organizaciji da unapredi spremnost svog osoblja za rešavanje incidenata, smanjujući rizik od ljudskih grešaka i povećavajući efikasnost bezbednosnih procedura u stvarnim uslovima.

26 Measom Kurt, „7 Ways to Educate Employees on New Security Technology and Foster Security Culture“, *Security Management* (http://www.asisonline.org/security-management-magazine/articles/2024/10/culture/new-technology-security-culture, 24.10.2024).

Kontinuirana obuka i usavršavanje

Obuka zaposlenih u vezi sa novim tehnologijama ne bi trebalo da bude ograničena na jednokratni trening, već predstavlja kontinuirani proces koji se prilagođava kako tehnologije napreduju. Tehnološke inovacije u oblastima poput bezbednosti brzo se razvijaju, što zahteva od kompanija da stalno unapređuju znanja i veštine svojih zaposlenih. Uspostavljanje redovnih radionica, seminara i programa sertifikacije omogućava zaposlenima da budu u toku sa najnovijim trendovima, kao i sa izmenama i novim funkcijama sistema koje kompanija koristi.

Primer kontinuirane obuke može uključivati redovne treninge u korišćenju bezbednosnih sistema zasnovanih na veštačkoj inteligenciji. Kako se ti sistemi nadograđuju i uvode nove aplikacije, kao što su poboljšani algoritmi za prepoznavanje pretnji ili brže obrade podataka, obuke bi omogućile zaposlenima da efikasno koriste nove funkcije i razumeju njihove prednosti u svakodnevnom radu. Pored toga, redovna obuka osigurava da zaposleni ne izgube korak sa tehnološkim promenama, čime se minimizira rizik od zastarelih znanja i veština. Ovakvi programi kontinuiranog usavršavanja predstavljaju osnovni deo strategije kompanije za obezbeđivanje konkurentnosti i održivog razvoja u dinamičnom tehnološkom okruženju.

E-učenje i onlajn platforme

Edukativne platforme za e-učenje pružaju značajnu fleksibilnost u načinu na koji zaposleni mogu sticati nova znanja i veštine, što je naročito korisno u velikim organizacijama sa različitim radnim rasporedom i obavezama. Onlajn kursevi omogućavaju zaposlenima da uče u svom ritmu, prilagođavajući tempo učenja svojim ličnim potrebama i obavezama, bez prekida u svakodnevnim radnim zadacima.[27]

Ovaj pristup omogućava kontinuirano usavršavanje i omogućava pojedinacima da napreduju u skladu sa svojim mogućnostima.Primer efikasne primene e-učenja je platforma koja nudi onlajn kurseve iz oblasti upotrebe veštačke inteligencije u upravljanju bezbednosnim rizicima. Ova vrsta kursa može biti od velike koristi za zaposlene koji nemaju prethodno iskustvo u ovoj oblasti, jer im omogućava da steknu nove veštine i produbе svoje razumevanje bezbednosnih tehnologija u digitalnom okruženju. Platforma bi mogla pružati modulisane kurseve koji pokrivaju sve od osnovnih pojmova veštačke inteligencije do njene primene u složenim bezbednosnim scenarijima, što omogućava personalizovano učenje za svakog korisni-

27 Jadrić Mario, Ćukušić Maja, Lenkić Marina, *E-učenje: Moodle u praksi*, Ekonomski fakultet, Split 2012, str. 14-16.

ka.E-učenje takođe smanjuje potrebu za fizičkim prisustvom na tradicionalnim treninzima, čime se omogućava veća efikasnost u upravljanju vremenom i resursima u organizaciji. Ovakvi programi ne samo da unapređuju veštine zaposlenih, već i doprinose rastu organizacije omogućavajući konstantno učenje i razvoj bez prekidanja redovnih poslovnih aktivnosti.

Strateško planiranje uvođenja inovativnih rešenja

Strateško planiranje je suština uspešne integracije novih tehnologija u bezbednosne sisteme. Ono uključuje detaljno definisanje ciljeva, analizu resursa, planiranje fazne implementacije i procenu mogućih rizika. Prvi korak u ovom procesu je analiza trenutnog stanja i procena potreba. Pre nego što se pristupi integraciji novih tehnologija, neophodno je detaljno analizirati postojeće bezbednosne sisteme i identifikovati slabosti koje nova rešenja mogu popraviti. Ovaj korak uključuje reviziju postojećih procesa, tehnologija i resursa, sa ciljem utvrđivanja šta je potrebno modernizovati i u kojoj meri, kako bi se obezbedila efikasna i bezbedna implementacija novih sistema.[28]

Detaljna analiza postojećih sistema

Proces modernizacije bezbednosne infrastrukture podrazumeva detaljnu analizu postojećih sistema kako bi se utvrdilo u kojoj meri su oni zastareli u odnosu na savremene tehnološke standarde. Ovaj proces uključuje sistematsko ispitivanje svih bezbednosnih tehnologija koje se trenutno koriste u kompaniji, s ciljem identifikacije oblasti koje zahtevaju unapređenje ili potpuno nova rešenja. Analiza se može fokusirati na procenu efikasnosti trenutnih sistema video obezbeđenja, provere koliko su oni sposobni da obrađuju i analiziraju slike u realnom vremenu uz pomoć novih tehnologija poput veštačke inteligencije. Takođe, sistemi za kontrolu pristupa mogu biti pregledani kako bi se utvrdilo da li koriste adekvatne mere identifikacije i zaštite od neovlašćenog ulaska. Sajber-bezbednosni alati koji štite mrežu i podatke moraju biti analizirani u odnosu na trenutne pretnje, kao što su fišing, kako bi se utvrdilo da li je potrebna njihova nadogradnja. Rezultati ove analize mogu poslužiti kao osnova za dalje strateško planiranje uvođenja novih tehnologija koje će poboljšati ukupnu bezbednost, omogućavajući efikasnije upravljanje rizicima i adaptaciju na nove bezbednosne izazove.

28 Gupta Sunil, *Driving Digital Strategy: A Guide to Reimagining Your Business*, Harvard Business Review Press, Brighton MA 2018, pp. 245-252.

Definisanje ciljeva integracije

Uspešna integracija inovacija u bezbednosne sisteme zahteva jasno definisanje kako kratkoročnih, tako i dugoročnih ciljeva. Kratkoročni ciljevi mogu uključivati poboljšanje vremena reakcije na incidente, unapređenje trenutnih operativnih procedura ili smanjenje identifikovanih rizika u okviru postojećih bezbednosnih sistema.

S druge strane, dugoročni ciljevi mogu se fokusirati na strateške aspekte, kao što su povećanje nivoa automatizacije, smanjenje operativnih troškova kroz efikasnije upravljanje resursima i postepena digitalizacija bezbednosnih procesa.

Na primer, ako je primarni cilj smanjenje vremena odziva na bezbednosne incidente, novo uvedeni sistemi moraju omogućiti bržu detekciju pretnji i automatizovane mehanizme za reagovanje. U tom kontekstu, tehnologije kao što su veštačka inteligencija i mašinsko učenje mogu igrati ključnu ulogu u identifikaciji rizika u realnom vremenu i preduzimanju mera pre nego što incident eskalira. Jasno definisanje ovih ciljeva osigurava da integracija novih tehnologija ne samo da unapređuje postojeće sisteme, već i stvara merljive rezultate koji doprinose dugoročnom razvoju bezbednosne infrastrukture.

Fazno uvođenje novih tehnologija

Uvođenje inovacija u bezbednosne sisteme najbolje je izvršiti u fazama kako bi se omogućila postepena integracija i minimalizovali potencijalni rizici. Ovaj pristup podrazumeva da se nove tehnologije prvo testiraju kroz pilot-projekte ili u ograničenim uslovima pre nego što se primene u celokupnom poslovnom okruženju. Fazna implementacija omogućava kompaniji da proceni funkcionalnost novih sistema, identifikuje sve potencijalne probleme ili nedostaci i preduzme korektivne mere pre šire primene.

Na primer, ako kompanija planira da uvede određen sistem za upravljanje bezbednosnim rizicima zasnovan na veštačkoj inteligenciji, početna faza implementacije može biti ograničena na jedan objekat ili manji deo infrastrukture. Ovo omogućava detaljno testiranje novog sistema u realnim uslovima, kao i procenu njegove efikasnosti u identifikaciji i reagovanju na potencijalne pretnje. Ako pilot faza pokaže pozitivne rezultate, tehnologija se može postepeno uvoditi u ostale delove kompanije, čime se osigurava uspešna implementacija bez značajnog ometanja poslovnih

procesa.Fazni pristup smanjuje rizik od neuspešnih implementacija i pruža fleksibilnost u prilagođavanju tehnologije specifičnim potrebama i zahtevima organizacije.

Uvođenje novih tehnologija u bezbednosne sisteme može doneti različite izazove i rizike, koji mogu obuhvatati tehnološke greške, ili potrebu za značajnim investicijama. S tim u vezi, kompanija mora razviti sveobuhvatne strategije za upravljanje rizicima koje uključuju detaljnu analizu potencijalnih rizika i kreiranje planova za njihovo minimizovanje. Proces počinje identifikacijom specifičnih rizika koji se mogu pojaviti u kontekstu novih tehnologija. Ovo uključuje, na primer, procenu rizika od sajber napada na nove sisteme nadzora. U tom slučaju, važno je uspostaviti mere za zaštitu podataka, kao i mehanizme za brzo reagovanje u slučaju incidenta.

Finansijsko planiranje i optimizacija budžeta

Implementacija inovativnih rešenja u bezbednosnim sistemima može zahteva značajna finansijska ulaganja, što čini finansijsko planiranje delikatnim aspektom ovog procesa. Kompanije moraju proceniti način na koji mogu optimizovati troškove, kako bi osigurale da će ulaganje biti održivo na dugoročnom planu. Prvi korak u ovom procesu uključuje detaljnu analizu odnosa troškova i koristi. Ova analiza podrazumeva procenu svih troškova povezanih sa novim tehnologijama, uključujući inicijalne investicije, troškove održavanja, obuke i potencijalne troškove povezane sa rizicima. Pored toga, važno je identifikovati i proceniti sve potencijalne koristi koje proizilaze iz implementacije novih rešenja, kao što su poboljšana efikasnost, smanjeni operativni troškovi ili povećana bezbednost. Drugi važan aspekt na koji praksa ukazuje je angažovanje izvođača koji nude rešenja "ključ u ruke". Ovi izvođači pružaju celokupno rešenje, uključujući projektovanje, instalaciju i integraciju sistema, što kompanijama omogućava da smanje rizike povezane sa implementacijom i postignu bolju kontrolu nad ukupnim troškovima. Izbor pouzdanih izvođača ovog tipa pomaže u pojednostavljivanju procesa implementacije i omogućava fokusiranje na osnovne poslovne operacije. Sledeći korak je planiranje resursa potrebnih za održavanje novih sistema. Ovo podrazumeva razmatranje budžetskih alokacija za redovno održavanje tehnologija, kao i za kontinuirane obuke zaposlenih. Kompanija bi trebalo da uspostavi jasne finansijske metrike i indikatore uspeha koji će se koristiti za praćenje povraćaja ulaganja (ROI) i efikasnosti ulaganja u nove tehnologije. Kroz sistematsko finansijsko planiranje, optimizaciju budžeta i uključivanje "ključ u ruke" izvođača, kompanije mogu obezbediti da ulaganja u inovacije ne samo da budu opravdana, već i da doprinose dugoročnom rastu i konkurentnosti.[29]

29 „Povrat ulaganja (ROI)", *Rečnik 2024*, Economy-pedia (http://www.sr.economy-pedia.

Ocena efikasnosti i kontinuirano unapređenje digitalizovanih bezbednosnih sistema

Nakon implementacije novih tehnologija, krucijalno je redovno praćenje i procena njihove efikasnosti kako bi se osiguralo da one doprinose postizanju poslovnih i bezbednosnih ciljeva. Kontinuirano unapređenje treba da bude sastavni deo strategije, sa ciljem poboljšanja performansi i adekvatne reakcije na nove rizike.

Redovna evaluacija sistema

Uspostavljanje mehanizama za redovnu evaluaciju efikasnosti bezbednosnih tehnologija je ključni aspekt održavanja i unapređenja novih sistema. Ovo podrazumeva konstantno praćenje specifičnih metrika koje ukazuju na performanse sistema, kao što su broj bezbednosnih incidenata, vreme odziva na pretnje i broj lažnih alarma. Ove metrike omogućavaju kompaniji da proceni da li novouvedene tehnologije postižu željene rezultate i da li funkcionišu u skladu sa postavljenim bezbednosnim ciljevima.

Na primer, nakon uvođenja novog sistema za detekciju pretnji, redovno merenje broja lažnih alarma i vremena potrebnog za odgovor na stvarne pretnje može pružiti jasan uvid u to koliko je sistem efikasan. Ako metrike pokažu značajno smanjenje lažnih alarma i poboljšanje vremena odziva na realne pretnje, to će potvrditi da je nova tehnologija uspešno implementirana i da opravdava ulaganje. U slučaju da rezultati nisu u skladu sa očekivanjima, evaluacija omogućava identifikaciju slabih tačaka i korektivne mere za unapređenje sistema. Redovna evaluacija pomaže organizaciji da kontinuirano poboljšava svoje bezbednosne sisteme, prilagođavajući ih novim izazovima i tehnologijama, čime se osigurava dugoročna efikasnost i održivost.

Kontinuirano prilagođavanje i ažuriranje sistema

S obzirom na brz razvoj tehnologija i konstantne promene u bezbednosnim izazovima, sistemi koji su jednom implementirani moraju biti redovno ažurirani i prilagođeni novim pretnjama. Ovo obuhvata instalaciju softverskih ažuriranja koja osiguravaju da bezbednosni sistemi ostaju u toku sa najnovijim tehnološkim razvojem i mogućim pretnjama. Pored toga, redovno testiranje novih funkcija i poboljša-

com/11040327-return-on-investment-roi#google_vignette, 21.09.2024).

nje postojećih mehanizama omogućavaju kompanijama da optimizuju svoje sisteme kako bi odgovorili na promene u okruženju.

Na primer, sistem za video obezbeđenje koji je inicijalno zasnovan na veštačkoj inteligenciji može početi sa osnovnom funkcijom nadgledanja, ali kako tehnologija napreduje, taj sistem može biti ažuriran na način da uključi nove mogućnosti kao što su automatsko upozoravanje na anomalije ili rano otkrivanje incidenata. Takva ažuriranja ne samo da poboljšavaju ukupnu efikasnost sistema, već omogućavaju kompaniji da blagovremeno odgovori na novonastale pretnje i izazove u oblasti bezbednosti.Ovakav pristup obezbeđuje da sistemi ostanu robusni i prilagodljivi.[30]

Povratna informacija od korisnika sistema

Uspešna integracija i primena novih tehnologija ne završava se samo tehničkom implementacijom. Važan deo evaluacije i poboljšanja sistema uključuje i prikupljanje povratnih informacija od zaposlenih koji te sisteme koriste na svakodnevnom nivou.

Njihovi utisci i iskustva mogu pružiti važne uvide o praktičnim izazovima i potencijalnim problemima koji možda nisu uočeni u početnim fazama planiranja i testiranja. Primer za ovo je situacija gde zaposleni koji rade sa novim sistemom za kontrolu pristupa primete da su određeni delovi korisničkog interfejsa složeni ili nepraktični za upotrebu u svakodnevnim operacijama. Takve povratne informacije mogu ukazati na potrebu za prilagođavanjem interfejsa ili poboljšanjem performansi, kako bi sistem postao intuitivniji i efikasniji za upotrebu. Ovo obezbeđuje da sistemi ne budu samo tehnološki napredni, već i korisnički prilagođeni, što povećava produktivnost i ukupno zadovoljstvo zaposlenih.[31]

Unapređenje performansi putem ekvilajzera analitika

Kompanije mogu značajno poboljšati performanse svojih bezbednosnih sistema korišćenjem naprednih analitičkih alata za dublju analizu podataka. Ovi alati omogućavaju identifikaciju trendova u bezbednosnim incidentima, često ponavljajućih problema, kao i područja koja zahtevaju dodatna poboljšanja. Analitika može pružiti uvid u operativnu efikasnost sistema, kao i otkriti skrivene rizike koji možda

30 „Bosch Security – Queuing notification with Video Analytics“ (http://www.youtube.com/watch?v=CLQD54CYt64, 03.09.2024).

31 http://www.youtube.com/watch?v=-rOdYR-OZfM&list=PLz97rFi-OzLfkBjxjtkICApnRKIzjjFtD&index=1

nisu očigledni u svakodnevnom praćenju. Primer ovakve primene može biti analiza podataka prikupljenih od sistema video obezbeđenja, koja može pokazati da se incidenti najčešće dešavaju u određenim vremenskim periodima, na primer, tokom noći ili za vreme smena sa manjim brojem zaposlenih. Na osnovu ovih uvida, kompanija može primeniti specifične preventivne mere tokom tih perioda, kao što je pojačan nadzor ili raspoređivanje dodatnog osoblja, čime se smanjuje rizik od budućih incidenata. Ovakav pristup ne samo da poboljšava operativnu bezbednost, već i omogućava organizaciji da preduzme proaktivne mere zasnovane na podacima, što dugoročno dovodi do većih ušteda i bolje zaštite resursa.

Revizije i provere sistema

Da bi osigurale da bezbednosni sistemi funkcionišu na najvišem nivou efikasnosti, kompanije mogu pored redovnih, ali i vanrednih internih revizija i provera organizovati i nezavisne eksterne kontrole. Angažovanje nezavisnih revizora omogućava objektivnu evaluaciju sistema i pruža neutralan pogled na njihovu efikasnost, kao i preporuke za dalja poboljšanja. Ovakav pristup minimizira rizik da interni timovi previde određene probleme zbog uobičajene prakse ili pristrasnosti. Primer efikasnosti nezavisne provere, odnosno revizije nalazimo u situacijama u kojima se kontrolni procesi obavljaju u određenim vremenskim intervalima (kvartalno, polugošnje, godišnje). Ovakve provere mogu otkriti neočekivane rizike, kao što su tehnološke ranjivosti ili nepravilnosti u korišćenju novih sistema koje interne provere možda nisu primetile. Revizori takođe mogu predložiti ažuriranja ili promene u procesima kako bi osigurali bolji odgovor na novonastale pretnje ili poboljšali trenutne prakse. Ovaj proces obezbeđuje kontinuirano poboljšanje bezbednosnih sistema i njihovu prilagođenost aktuelnim i budućim pretnjama, opasnostima i ranjivostima i sa njima povezanim rizicima.

Literatura

Monografije, udžbenici, zbornici, priručnici, izveštaji, uputstva

1. *A Business Framework for the Governance and Management of Enterprise IT*, ISACA, Schaumburg IL, 2012.

2. *A guide to integrated security management systems*, British Security Industry Association, Worcester UK, 2017.

3. *A guide for running an effective Penetration Testing programme*, CREST, Coventry UK, April 2017.

4. Albaum G., *Competitive Intelligence*, C.I. Associates, Watertown MA 1959.

5. *An Introduction to Information Security,* NIST Special Publication 800-12, Rev. 1, Gaithersburg MD, *2017.*

6. *Aufbau und Struktur Eines Reise-Risikomanagements*, ASW Bundesverband, Berlin DE, 2016.

7. *Bank Robberies – Executive Summary*, The European Banking Federation, Brussels, 2011.

8. *Bela knjiga: predlozi za poboljšanje poslovnog okruženja u Srbiji*, Savet stranih investitora, Beograd 2022.

9. *Boosting your Organisation's Cyber Resilience, Joint Publication*, CERT-EU and ENISA, Brussels, 2022.

10. Briggs R., Edwards C., *The Business of Resilience: Corporate security for the 21st century*, Demos, London UK, 2006.

11. Brijs B., *Business Analysis for Business Intelligence*, CRC Press, Boca Raton FL, 2016.

12. Burns L., *Growing Business Intelligence – An Agile Approach to Leveraging Data and Analytics for Maximum Business Value*, Technics Publications, Basking Ridge NJ 2016.

13. *Business Continuity Guideline - A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*, GDL BC 01, ASIS, Alexandria VA 2005.

14. *Buying quality private security services*, CoESS & UNI-Europa, Brussels, 2023.

15. Garner A. B. (ed.), *Black's Law Dictionary*, 8th Ed., West, Eagan MN, 2004.

16. Gelbstein E., *Information security for non-technical managers*, 1st edition, Bookboon.com, London, 2013.

17. Golden B., *Amazon Web Services For Dummies*, John Wiley & Sons, Hoboken NJ, 2013.

18. Goldstein P., Reese R. A., *Copyright, Patent, Trademark and Realated State Doctrines: Cases and Materials on the Law of Intellectual Property*, Foundation Press, New York NY 2008.

19. Grima S., Thalassinos E., Cristea M., Kadłubek M., Maditinos D., Peiseniece L. (Eds.), *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management*, Emerald Publishing Ltd., Leeds UK 2023.

20. *Guidance on cyber resilience for financial market infrastructures*, BIS and IOSCO, Basel CH, 2016.

21. *Guidelines 3/2019 on processing of personal data through video devices*, Version 2.0, European Data Protection Board, Brussels, January 2020.

22. *Guidelines on the security measures for operational and security risks ofpayment services under Directive (EU) 2015/2366 (PSD2),* European Banking Authority - EBA, Paris, 2018.

23. Gupta S., *Driving Digital Strategy: A Guide to Reimagining Your Business*, Harvard Business Review Press, Brighton MA 2018.

24. Guttmann R., *Eco-Capitalism: Carbon Money, Climate Finance, and Sustainable Development*, Palgrave Macmillan, London UK 2018

25. *Dictionary of Business Continuity Management Terms*, The Business Continuity Institute, Reading UK, 2011.

26. Dragišić Z., Radojević K., *Bezbednosni menadžment*, Fakultet bezbednosti Univerziteta u Beogradu, Beograd, 2014.

27. *ENISA Threat Landscape 2022*, The European Union Agency for Cybersecurity (ENISA), Athens, 2022.

28. *Enterprise Risk Management - Integrating with Strategy and Performance*, COSO, Englewood Cliffs NJ 2017.

29. *Enterprise Security Risk Management: A holistic approach to security*, ASIS International, Alexandria VA, 2015.

30. *Enterprise Security Risk Management: Overview and Case Studies,* ASIS International, CSO Roundtable, Alexandria VA, 2015.

31. *Zaštita podataka o ličnosti u oblasti radnih odnosa*, Publikacija br. 3, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Beograd, 2018.

32. Ivandić Vidović D., Karlović L., Ostojić A., *Korporativna sigurnost*, Udruga hrvatskih menadžera sigurnosti, Zagreb, 2011.

33. *Izveštaj o radu za 2023. godinu*, Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, Uprava za bezbednost i zdravlje na radu, Beograd, 2024.

34. *Internet organised crime threat assessment (IOCTA) 2018*, Europol, The Hague NL, 2019.

35. *INFORM REPORT 2022, Shared evidence for managing crises and disasters*, United Nations Office for the Coordination of Humanitarian Affairs, New York NY, 2022.

36. *IT-Grundschutz Catalogues*, Federal Office for Information Security (BSI), 13th version, Bonn DE, 2013.

37. Jadrić M., Ćukušić M., Lenkić M., *E-učenje: Moodle u praksi*, Ekonomski fakultet, Split 2012.

38. Keković Z., Dimitrijević R. I., Šekarić N., *Korporativna bezbednost – hrestomatija*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2018.

39. Keković Z., Kešetović Ž., *Krizni menadžment I, Prevencija krize*, Univerzitet u Beogradu, Fakultet bezbednosti, 2006.

40. Keković Z., Savić S., Komazec N., Milošević M., Jovanović D., *Procena rizika u zaštiti lica, imovine i poslovanja*, Centar za analizu rizika i upravljanje krizama, Beograd, 2011

41. *Korporativno upravljanje – Priručnik*, IFC, Beograd, 2011.

42. Kranz M., *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry*, Wiley, Hoboken NJ, 2016.

43. Laloux F., *Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness*, Nelson Parker, Cambridge MA 2014.

44. *Leitplanken – Interne Ermittlungen*, ASW Bundesverband, Berlin DE 2021.

45. Lencioni M. P., *The Five Dysfunctions of a Team: A Workshop for Team Leaders*, Pfeiffer, San Francisco CA 2012.

46. Loshin D., *Business Intelligence: The Savvy Manager`s Guide*, Elsevier Inc., Waltham MA 2013.

47. Mazurkiewicz P., *Corporate Environmental Responsibility: Is a common CSR framework possible?*, World Bank, Wachington DC 2004.

48. Mandić J. G., *Osnovi sistema obezbeđenja pravnih lica*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2012.

49. Mandić J. G., *Sistemi obezbeđenja i zaštite*, Fakultet civilne odbrane, Univerzitet u Beogradu, Beograd, 2004.

50. Mandić J. G., Stanojević P., *Korporativna bezbednost*, Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, 2019.

51. Milutinović M., *Korporativna bezbednost*, Visoka škola strukovnih studija za kriminalistiku i bezbednost, Niš, 2011.

52. *Minimum Security Requirements for Federal Information and Information Systems,* FIPS PUB 200, NIST, Gaithersburg MD, 2006.

53. Moberly D. M., *Safeguarding Intangible Assets*, Butterworth-Heinemann, Oxford UK 2014.

54. *Oblast bezbednosti i zdravlja na radu, Drugi deo*, Inspektorat za rad, Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, Beograd, 2018.

55. *Opinion 2/2017 on data processing at work – WP 249*, European advisory body on data protection and privacy, Brussels, June 2017.

56. *Payment threats and fraud*, EPC 214-17v1.0, European Payments Council, Brussels, 2017.

57. Pleskonjić D., Maček N., Đorđević B., Carić M., *Sigurnost računarskih mreža*, Viša elektrotehnička škola, Beograd, 2006.

58. *Primena Zakona o tajnosti podataka u Republici Srbiji*, *Nadzor i sudska praksa*, Fondacija za otvoreno društvo, Beograd, jun 2021.

59. *Principles for financial market infrastructures*, BIS and IOSCO, Basel CH-Madrid ES, 2012.

60. *Protective Security Requirements, Guide to personnel security for your organisation*, Department of the Prime Minister and Cabinet, Wellington NZ, 2019.

61. *Procena pretnje od teškog i organizovanog kriminala*, MUP Republike Srbije, Beograd 2015.

62. Prunckun H., *Counterintelligence Theory and Practice*, Rowman & Littlefield Publishers Inc., Lanham MD 2012.

63. Radun V., *Konkurencija na nišanu – Teorijski i praktični aspekti istraživanja konkurencije*, HESPERIAedu, Beograd 2008.

64. Ramcharan R., *International Intellectual Property Law and Human Security*, Asser Press, The Hague NL 2013

65. *Reducing the risk of wholesale payments fraud related to endpoint security*, BSI, London 2018.

66. *Report to the Nations - Global study on occupational fraud and abuse*, ACFE, Austin TX, 2018.

67. *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN (2017) 450 final, European Commisssion, Brussels, 13.9. 2017.

68. Rogers L. D., *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*, Columbia Business School Publishing, New York NY 2016

69. *Sendai Framework for Disaster Risk Reduction 2015-2030*, The Third UN World Conference, Sendai JP, 2015.

70. *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, NIST Special Publication 800-53, NIST, Gaithersburg MD, 2020.

71. *Security Industrial Policy – Action Plan for an innovative and competitive Security Industry,* EC COM(2012)417 final, European Commission, Brussels, 26.7.2012.

72. Spaninks L., Quinn L., Byrne J., *European Vocational Training Manual For Basic Guarding*, Leonardo NL/96/2/1136/PI/II.1.1.b/FPC, Brussels, 1999.

73. Stajić Lj., Mandić G., *Sistem zaštite imovine i poslovanja*, Pravni fakultet, Novi Sad, 2008.

74. Stojanović M., Pavlović D., *Ekonomska bezbednost poslovanja*, Srpska asocijacija menadžera korporativne bezbednosti i Škola plus, Beograd, 2014.

75. *Strategies to Detect and Prevent Workplace Dishonesty*, Research Council CRISP Report, ASIS International Foundation, Alexandria VA, 2008.

76. *Strateška procena javne bezbednosti*, MUP Republike Srbije - Direkcija policije, Beograd 2017.

77. *Strengthening digital society against cyber shocks, Key findings from The Global State of Information Security Survey 2018*, PwC, 2019.

78. *Studija izvodljivosti uspostavljanja procedura nacionalnog CERT-a i upravljanja sistemom za prijavu incidenata*, RATEL, Beograd 2018.

79. Sherman R., *Business Intelligence Guidebook – From Data Integration to Analytics*, Elsevier Inc., Waltham MA 2015.

80. Scarfone K., Grance T., Masone K., *Computer Security Incident Handling Guide,* NIST Special Publication 800-61, Revision 2, NIST, Gaithersburg MD, 2008.

81. Talbot J., Jakeman M., *Security Risk Management Body of Knowledge*, John Wiley and Sons, Hoboken NJ, 2009.

82. *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, Gaithersburg MD, 2008.

83. *Top Security Threats and Management Issues Facing Corporate America*, Securitas Security Services USA, Parsippany NJ, 2016.

84. *Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1*, United Nations, New York NY, 2015.

85. Trivan D., *Osnovi korporativne bezbednosti*, Fakultet za poslovne studije i pravo Univerziteta «Union – Nikola Tesla», Beograd, 2017.

86. *The EDPS Video-Surveillance Guidelines*, European Data Protection Supervisor, Brussels, 17 March 2010.

87. *The State of Security Convergence in the United States, Europe, and India*, ASIS International, Alexandria VA 2019.

88. *Threat Landscape Report 2018*, Version 1.0, The European Union Agency for Cybersecurity (ENISA), Athens, 2019.

89. *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji*, Republički zavod za statistiku, Beograd, 2019.

90. Fay J. J., *Contemporary Security Management*, Third Edition, Butterworth-Heinemann, Burlington MA, 2011

91. Feldman D., Himmelstein J., *Developing Business Intelligence Apps for SharePoint*, O'Reilly Media, Inc., Sebastopol CA 2013.

92. Fehringer D., Hohhof B. (eds.), *Competitive Intelligence Ethics: Navigating the Gray Zone*, Competitive Intelligence Foundation, Alexandria VA 2006.

93. *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018., NIST, Gaithersburg MD, 2018.

94. *Fraud Risk Management Guide*, COSO, Morristown NJ, 2016.

95. *Handbook - Security risk management, HB 167:2006,* Standards Australia & Standards New Zealand, Sydney AU-Wellington NZ, 2006.

96. Coker F., *Pulse - Understanding the Vital Signs of Your Business*, Ambient Light Publishing, Bellevue WA, 2014.

97. *Convergence of Enterprise Security Organizations*, Alliance for Enterprise Security Risk Management, Booz Allen Hamilton, McLean VA, 2005.

98. *Critical Security Controls*, Version 8, Center for Internet Security, East Greenbush NY, 2016.

99. *CCTV surveillance: The differing aims and functions of CCTV within the corporate stratum*, Research Online, 8th Australian Security and Intelligence Conference, Edith Cowan University, Joondalup AU, 2015.

100. *Cybersecurity Assessment Tool*, FFIEC, Washington DC, 2017.

101. *Cyber Security Incident Response Supplier Selection Guide*, Version 1. 2013., CREST, Slough UK, 2013.

102. Čaleta D., Vršec M., Bertoncelj B., Vršec M., Kandžič A., Podgoršek Ž., Študija "Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture", ICS Institut, Ljubljana, 2019.

103. *Who Cares Wins*, Swiss Federal Department of Foreign Affairs & United Nations, Bern CH-New York NY, 2004.

Članci i prilozi

104. Blumberg R., Atre S., "The Problem with Unstructured Data", *DM Review*, Daman Consulting, Austin TX 2003, pp. 42–46.

105. Dedić N., Stanier C., „Measuring the Success of Changes to Existing Business Intelligence Solutions to Improve Business Intelligence Reporting", *10th*

International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS), Vienna 2016, pp. 225–236.

106. Kennard A., „The Enemy of My Enemy: When Firms Support Climate Change Regulation", *International Organization*, Vol. 74, Issue 2, Cambridge University Press, Cambridge UK 2020, pp. 187-221.

107. Klasan V., „Poslovne izvjesnice i vojno-gospodarska diplomacija", *Polemos*, Vol. 14, No. 27, Hrvatsko sociološko društvo & Naklada Jesenski i Turk, Zagreb 2011., str. 77-95.

108. Lečić B., „Place and role of corporate security in the national safety system", In: Trivan D., *Contemporary Concept of Corporate Security*, Faculty of Business Studies and Law, University „Union-Nikola Tesla", Belgrade & Austrian Institute for European and Security Policy/AIES Wien & Institute for Corporative Security Studies, ICS, Ljubljana, 2018., pp. 175 - 191.

109. Rao R., "From unstructured data to actionable intelligence", *IT Professional*, Vol. 5, Issue 6, IEEE Computer Society, Washington DC 2003, pp. 29–35.

110. Stipanović C., „Izazovi poslovne inteligencije u turizmu", *UTM Revija*, Vol. 58, No. 5, UTM Revija, UT Ugostiteljstvo i turizam, Zagreb 2010., str. 32-34.

111. Herring P. J., „World-Class Intelligence Programs", in: *Competitive Intelligence Magazine*, Vol. 10, No. 2, Issue 3, Alexandria VA, May-June 2006, pp. 20-25.

Pravni izvori

General Data Protection Regulation (GDPR), OJ L 119, Brussels, 4.5.2016.

Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) OJ L 335, Brussels, 17 December 2009.

Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU() No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainibility reporting, OJ L 322, Brussels, 16.12.2022.

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for high common level of cybersecurity across the Union, OJ L 333, Brussels, 27 December 2022.

Directive (EU) 2022/2557 (The Critical Entities Resilience Directive), OJ L 333, Brussels, 27 December 2022.

EU Security Union Strategy, COM/2020/605 final, European Commission, Brussels, 2020.

Zaključak o usvajanju Etičkih smernica za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije, „Službeni glasnik RS“, br. 23/2023.

Zakon o bankama, „Službeni glasnik RS“, br. 107/2005, 91/2010 i 14/2015.

Zakon o bezbednosti i zdravlju na radu, „Službeni glasnik RS”, br. 35/2023.

Zakon o vojnoj, radnoj i materijalnoj obavezi, „Službeni glasnik RS“, br. 88/2009, 95/2010 i 36/2018.

Zakon o detektivskoj delatnosti, „Službeni glasnik RS“, br. 104/2013 i 87/2018.

Zakon o digitalnoj imovini, „Službeni glasnik RS”, br. 153/2020.

Zakon o državnim službenicima, „Službeni glasnik RS“, br. 79/2005, 81/2005 - ispravka, 83/2005 - ispravka, 64/2007, 67/2007 - ispravka, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018 i 157/2020.

Zakon o zabrani diskriminacije, „Službeni glasnik RS”, br. 22/2009 i 52/2021.

Zakon o zaštiti životne sredine, „Službeni glasnik RS“, br. 135/2004, 36/2009, 36/2009 - dr. zakon, 72/2009 - dr. zakon, 43/2011 - odluka US, 14/2016, 76/2018, 95/2018 - dr. zakon i 95/2018 - dr. zakon.

Zakon o zaštiti novčarskih institucija, „Narodne novine“, br. 56/2015, 46/2021 i 114/2022.

Zakon o zaštiti od požara, „Službeni glasnik RS“, br. 111/2009, 20/2015, 87/2018 i 87/2018 - dr. zakoni.

Zakon o zaštiti poslovne tajne, „Službeni glasnik RS”, br. 72/2011.

Zakon o zaštiti podataka o ličnosti, „Službeni glasnik RS”, br. 87/2018.

Zakon o zaštiti uzbunjivača, „Službeni glasnik RS”, br. 128/2014.

Zakon o igrama na sreću, „Službeni glasnik RS”, br. 18/2020.

Zakon o informacionoj bezbednosti, “Službeni glasnik RS”, br. 6/2016, 94/2017 i 77/2019.

Zakon o javnim nabavkama, “Službeni glasnik RS”, br. 01/2019 i 92/2023.

Zakon o kritičnoj infrastrukturi, „Službeni glasnik RS”, br. 87/2018.

Zakon o odbrani, „Službeni glasnik RS“, br. 116/2007, 88/2009, 88/2009 - dr. zakon, 104/2009 - dr. zakon, 10/2015 i 36/2018.

Zakon o odgovornosti pravnih lica za krivična dela, „Službeni glasnik RS“, br. 97/2008.

Zakon o oznakama geografskog porekla, „Službeni glasnik RS“, br. 18/2010 i 44/2018 - dr. zakon.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, „Službeni glasnik RS“, br. 61/2005, 104/2009, 10/2023 i 10/2023 – dr. zakon.

Zakon o osiguranju, “Službeni glasnik RS”, br. 139/2014.

Zakon o patentima, „Službeni glasnik RS“, br. 99/2011, 113/2017 - dr. zakon,

72/2009 - dr. zakon, 95/2018, 66/2019 i 123/2021.

Zakon o platnim uslugama, "Službeni glasnik RS", br. 139/2014 i 44/2018.

Zakon o pravnoj zaštiti industrijskog dizajna, „Službeni glasnik RS", br. 104/2009, 45/2015 i 44/2018 - dr. zakon.

Zakon o privatnom obezbeđenju, „Službeni glasnik RS", br. 104/2013, 42/2015 i 87/2018.

Zakon o privrednim društvima, „Službeni glasnik RS", br. 36/2011, 99/2011, 83/2014 - dr. zakon, 5/2015, 44/2018, 95/2018, 91/2019 i 109/2021.

Zakon o radu, "Službeni glasnik RS", br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - US, 113/2017 i 95/2018 - Autentično tumačenje.

Zakon o računovodstvu, "Službeni glasnik RS", br. 73/2019 i 44/2021 - dr. zakon.

Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama, „Službeni glasnik RS", br. 87/2018.

Zakon o sprečavanju zlostavljanja na radu, „Službeni glasnik RS", br. 36/2010.

Zakon o sprečavanju korupcije, „Službeni glasnik RS", br. 35/2019, 88/2019, 11/2021 - Autentično tumačenje, 94/2021 i 14/2022.

Zakon o sprečavanju pranja novca i finansiranja terorizma, "Službeni glasnik RS", br. 113/2017, 91/2019, 153/2020 i 92/2023.

Zakon o tajnosti podataka, „Službeni glasnik RS", br. 104/2009.

Zakon o tržištu kapitala, „Službeni glasnik RS", br. 129/2021.

Kodeks korporativnog upravljanja, „Službeni glasnik RS", br. 99/2012.

Kodeks medicinske etike Lekarske komore Srbije, "Službeni glasnik RS", br. 104/2016.

Kodeks policijske etike, "Službeni glasnik RS", br. 85/2023.

Krivični zakonik, „Službeni glasnik RS", br. 85/2005, 88/2005 - ispravka, 107/2005 - ispravka, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

Odluka o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, "Službeni glasnik RS", br. 45/2019 i 112/2020.

Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, "Službeni glasnik RS", br. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 i 100/2023 - dr. odluka.

Odluka o objektima od posebnog značaja za odbranu, „Službeni glasnik RS", br. 112/2008.

Odluka o određivanju velikih tehničkih sistema od značaja za odbranu, "Službeni glasnik RS", br. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019 i 67/2021.

Odluka o određivanju pravnih lica od značaja za odbranu Republike Srbije, „Službeni glasnik RS“, br. 52/2008.

Odluka o određivanju proizvoda i usluga od posebnog značaja za odbranu Republike Srbije, „Službeni glasnik RS“, br. 58/2008 i 26/2019.

Odluka o određivanju subjekata od posebnog značaja za zaštitu i spasavanje u Republici Srbiji, "Službeni glasnik RS", br. 69/2019.

Odluka o upravljanju rizicima banke, "Službeni glasnik RS", br. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 - dr. odluka, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016, 119/2017, 76/2018, 57/2019, 88/2019, 27/2020, 67/2020 - dr. odluka, 89/2022 i 77/2023.

Odluka o uslovima i načinu poveravanja aktivnosti u vezi sa informacionim sistemom finansijske institucije trećim licima, „Službeni glasnik RS", br. 100/2023.

Pravilnik o bližim uslovima koje moraju ispunjavati pravna lica za obavljanje poslova organizovanja zaštite od požara u subjektima prve, druge i treće kategorije ugroženosti od požara, „Službeni glasnik RS“, br. 6/2021.

Pravilnik o vrsti i količini opasnih supstanci na osnovu kojih se sačinjava Plan zaštite od udesa, "Službeni glasnik RS", br. 34/2019.

Pravilnik o načinu vršenja poslova tehničke zaštite i korišćenja tehničkih sredstava, "Službeni glasnik RS", br. 91/2019.

Pravilnik o načinu izrade i sadržaju Plana zaštite od požara autonomne pokrajine, jedinice lokalne samouprave i subjekata razvrstanih u prvu i drugu kategoriju, „Službeni glasnik RS", br. 73/2010.

Pravilnik o načinu izrade i sadržaju Plana zaštite od udesa, "Službeni glasnik RS", br. 41/2019.

Pravilnik o načinu i postupku procene rizika na radnom mestu i u radnoj okolini, "Službeni glasnik RS", br. 72/2006, 84/2006 - ispravka, 30/2010 i 102/2015.

Pravilnik o načinu unutrašnjeg uzbunjivanja, načinu određivanja ovlašćenog lica kod poslodavca, kao i drugim pitanjima od značaja za unutrašnje uzbunjivanje kod poslodavca koji ima više od deset zaposlenih, "Službeni glasnik RS", br. 49/2015 i 44/2018 - dr. zakon.

Pravilnik o organizovanju zaštite od požara prema kategoriji ugroženosti od požara, „Službeni glasnik RS", br. 6/2021.

Pravilnik o poklonima javnih funkcionera, "Službeni glasnik RS", br. 118/2020.

Pravilnik o popisu normi i prihvaćenih pravila struke u primjeni zaštite novčarskih institucija, „Narodne novine“, br. 102/2016.

Pravilnik o pravilima ponašanja poslodavaca i zaposlenih u vezi sa prevencijom i zaštitom od zlostavljanja na radu, „Službeni glasnik RS", br. 62/2010.

Pravilnik o programima i načinu obavljanja stručne obuke za vršenje poslova privatnog obezbeđenja i redarske službe, "Službeni glasnik RS", br. 15/2019.

Pravilnik o radu poverenika i zamenika poverenika civilne zaštite i kriterijumima za njihovo imenovanje, "Službeni glasnik RS", br. 102/2020.

Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms, OJ L 176, Brussels, 26 June 2013.

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, OJ L 333, Brussels, 27 December 2022.

Regulation (EU) 2019/881 on ENISA, OJ L 151, Brussels, 7.6.2019.

Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States, Council of Europe, Strasbourg FR, 1 April 2015.

Strategija nacionalne bezbednosti Republike Srbije, "Službeni glasnik RS", br. 94/2019.

Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godina, "Službeni glasnik RS", br. 96/2019.

Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine, „Službeni glasnik RS", br. 86/2021.

Uputstvo za izradu i sprovođenje plana integriteta, „Službeni glasnik RS", br. 119/2022.

Uputstvo o Metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja, „Službeni glasnik RS", br. 80/2019.

Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja, „Službeni glasnik RS", br. 94/2016.

Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja, „Službeni glasnik RS", br. 94/2016.

Uredba o kriterijumima za identifikaciju kritične infrastrukture i načinu izveštavanja o kritičnoj infrastrukturi Republike Srbije, "Službeni glasnik RS", br. 69/2022.

Uredba o minimalnim tehničkim uslovima kod obavezne ugradnje sistema tehničke zaštite u bankama i drugim finansijskim organizacijama, "Službeni glasnik RS", br. 9/2021.

Uredba o obrascu za vođenje evidencije i načinu vođenja evidencije o obradi podataka o ličnosti, "Službeni glasnik RS", br. 50/2009.

Uredba o podacima i poslovima značajnim za sistem odbrane koji se moraju čuvati i štititi u skladu sa zakonom kojim se uređuje zaštita tajnosti podataka i o kriterijumima za popunu radnih mesta na kojima se ti zadaci i poslovi obavljaju, „Službeni glasnik RS", br. 8/2020.

Uredba o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa, „Službeni glasnik RS", br. 63/2013.

Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, "Službeni glasnik RS", br. 53/2011.

Uredba o posebnim merama nadzora nad postupanjem sa tajnim podacima, „Službeni glasnik RS", br. 90/2011.

Uredba o posebnim merama fizičko-tehničke zaštite tajnih podataka, „Službeni glasnik RS", br. 97/2011.

Uredba o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, "Službeni glasnik RS", br. 11/2020.

Uredba o razvrstavanju objekta, delatnosti i zemljišta u kategorije ugroženosti od požara, „Službeni glasnik RS", br. 76/2010.

Uredba o sadržaju, načinu izrade i obavezama subjekata u vezi sa izradom procene rizika od katastrofa i planova zaštite i spasavanja, „Službeni glasnik RS", br. 102/2020.

Uredba o utvrđivanju Liste delatnosti u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja, „Službeni glasnik RS", br. 94/2019.

Council Decision 2013/488/EU on the security rules for protecting EU classified information, OJ L 274/1, Brussels, 15. October 2013.

Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessments of the need to improve their protection, OJ L 345, Brussels, 8 December 2008.

Standardi

ANSI/ISA-62443-3-3-2013, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels.

BSI - BS 10501:2014, *Guide to implementing procurement fraud controls*, BSI, London UK, 2014.

BSI Standard 100-4: Business Continuity Management, Version 1.0, London UK, 2009.

BS 7499:2013, Static site guarding and mobile patrol service – Code of practice, The British Standards Institution, London UK 2013.

BS 7858:2019, Screening of individuals working in a secure environment: Code of practice BS 7499:2013, Static site guarding and mobile patrol service – Code of practice, The British Standards Institution, London UK 2019.

BS 9347:2024, Facial recognition technology. Ethical use and deployment in video surveillance-based systems. Code of practice, The British Standards Institution, London UK 2024.

International Standards for the Professional Practice of Internal Auditing (Standards), The Institute of International Auditors - IIA, Lake Mary FL, 2016.

EN 15602:2022, Private security services – Terminology, CEN-CENELEC, Brussels 2022.

EN 16352:2013 - Logistics - Specifications for reporting crime incidents, Brussels 2013.

Z1600-17, Emergency and continuity management program, Canadian Standards Association, Torontto CA, 2017.

ISA-62443-2-1-2009, Security for industrial automation and control systems, Part 2-1: Establishing an industrial automation and control systems security program.

ISO 22300:2018, Security and Resilience – Vocabulary.

ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.

ISO/Guide 73:2009, Risk management — Vocabulary.

ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security controls.

ISO/IEC 27004:2016, Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation-

ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management.

ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.

ISO/IEC TS 27008:2019, Information technology — Security techniques — Guidelines for the assessment of information security controls.

ISO/IEC 27011:2016, Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.

ISO/IEC 27019:2017, Information technology — Security techniques — Information security controls for the energy utility industry.

ISO/IEC 27032:2023, Cybersecurity — Guidelines for Internet security.

ISO/IEC 27035-1:2023, Information technology - Information security incident management - Part 1: Principles and process.

ISO/IEC 27035-2:2023, Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident respons.

ISO/IEC 27035-3:2020, Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations.

ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines.

ISO/IEC 31010:2019, Risk management – Risk assessment techniques.

ISO/IEC 38500:2015, Information technology — Governance of IT for the organization.

ISO 9000:2015, Quality management systems - Fundamentals and vocabulary.

ISO 9001:2015, Quality management systems — Requirements.

ISO 14298:2021, Graphic technology, Management of security printing processes.

ISO 18788:2015, Management system for private security operations - Requirements with guidance for use.

ISO 19011:2018, Guidelines for auditing management systems.

ISO 20858:2007, Ships and marine technology — Maritime port facility security assessments and security plan development.

ISO 22300:2021, Security and resilience - Vocabulary.

ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.

ISO 22316:2017, Security and resilience - Organizational resilience - Principles and attributes.

ISO 22398:2013, Societal security — Guidelines for exercises.

ISO 28000:2022, Security and resilience - Security management systems – Requirements.

ISO 31000:2018, Risk management — Guidelines.

ISO 39001:2012, Road traffic safety (RTS) management systems — Requirements with guidance for use.

ISO 45001:2018, Occupational health and safety management systems — Requirements with guidance for use.

ISO 45001:2018/Amd 1:2024, Occupational health and safety management systems — Requirements with guidance for use; Amendment 1: Climate action changes.

ISO 45003:2021, Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks.

ISO/TS 22317:2015, Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA).

ISO/TS 22375, Security and resilience — Guidelines for complexity assessment process.

ÖNORM S 2414-1:2018, Security management system - Part 1: Guidance for embeddinginformation security in the security management system.

NFPA 1600, Standard on Disaster/Emergency Management and Business Conti-

nuity/Continuity of Operations Programs, National Fire Protection Association, Quincy MA, 2016.

Risk Assessment, RA.1-2015, ANSI/ASIS/RIMS, Washington DC-Alexandria VA-New York NY 2015.

Security and Resilience in Organizations and Their Supply Chains, ORM.1-2017, ANSI & ASIS, Washington DC-Alexandria VA, 2017

Social Accountability International 8000, SAI, New York NY, June 2014.

SRPS A.L2.001:2008, Društvena bezbednost - Usluge privatnog obezbeđenja – Rečnik, Institut za standardizaciju Srbije, Beograd, 2008.

SRPS A.L2.002:2015, Društvena bezbednost — Usluge privatnog obezbeđenja — Zahtevi i uputstvo za ocenjivanje usaglašenosti.

SRPS A.L2.003:2017, Bezbednost i otpornost društva — Procena rizika, Institut za standardizaciju Srbije, Beograd, 2017.

SRPS EN ISO/IEC 29101:2021, Informacione tehnologije – Tehnike bezbednosti – Okvir arhitekture privatnosti, Institut za standardizaciju Srbije, Beograd, 2021.

SRPS EN ISO/IEC 29151:2022, Informacione tehnologije – Tehnike bezbednosti – Pravila dobre prakse za zaštitu ličnih identifikacionih informacija, Institut za standardizaciju Srbije, Beograd, 2022.

SRPS ISO/IEC 27031:2013, Informacione tehnologije — Tehnike bezbednosti — Smernice za spremnost informacionih i komunikacionih tehnologija za kontinuitet poslovanja, Institut za standardizaciju Srbije, Beograd, 2013.

SRPS ISO/IEC 27701:2019, Tehnike bezbednosti – Proširenje ISO/IEC 27001 i ISO/IEC 27002 za menadžment informacijama o privatnosti – Zahtevi i smernice, Institut za standardizaciju Srbije, Beograd, 2019.

SRPS ISO/IEC 29100:2019, Informacione tehnologije – Tehnike bezbednosti – Okvir privatnosti, Institut za standardizaciju Srbije, Beograd, 2019.

SRPSENISO 22361:2023, Bezbednost i otpornost – Krizni menadžment – Smernice, Institut za standardizaciju Srbije, Beograd, 2020.

SRPSENISO/IEC 29147:2020, Informacione tehnologije – Tehnike bezbednosti – Otkrivanje ranjivosti, Institut za standardizaciju Srbije, Beograd, 2020.

SRPSISO 14001:2015, Sistemi menadžmenta životnom sredinom — Zahtevi sa uputstvom za korišćenje, Institut za standardizaciju Srbije, Beograd, 2015.

SRPSISO 37001:2017, *Sistemi menadžmenta protiv mita – Zahtevi sa uputstvom za korišćenje*, Institut za standardizaciju Srbije, Beograd, 2017.

SRPS ISO/TS 22317:2018, Društvena bezbednost – Sistem menadžmenta kontinuitetom poslovanja – Smernice za analizu uticaja na poslovanje (BIA), Institut za standardizaciju Srbije, Beograd, 2018.

SRPS TR A.L2.003-5:2020, Bezbednost i otpornost društva – Procena rizika – Deo 5: Uputstvo za izradu plana obezbeđenja, Institut za standardizaciju Srbije,

Beograd, 2020.

Standard 2000-1, Wirtschaftsgrundschutz, Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik i ASW Bundesverband, Berlin DE, 2016.

Trucking Security Requirements(TSR) 2017, TAPA Standards, Boca Raton FL 2017.

Facility Security Requirements (FSR) 2017, TAPA Standards, Boca Raton FL, 2017.

Elektronski izvori

http://www.ariscommunity.com/aris-express, 10.09. 2024.

http://www.asisonline.org/security-management-magazine/articles/2024/10/culture/new-technology-security-culture, 24.10.2024).

http://www.acfe.com/fraud-101.aspx, 02.04.2019.

http://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach, 02.09.2021.

http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=329062638, 10.06.2019.

http://www.businesstechweekly.com/legal-and-compliance/nist/implementing-nist-cybersecurity-framework/, 29.08.2024.

http://www.vectorsolutions.com/resources/blogs/levels-of-a-risk-matrix/, 11.09.2024).

http://www.gartner.com/en/information-technology/topics/digital-transformation, 14.09. 2024.

http://www.ibm.com/reports/threat-intelligence

http://www.iss.rs/sr_Cyrl/shta-je-standard_p13.html) 30.1.2024.

http://www.korporativnabezbednost.rs/, 26.3.2024.

http://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/why-an-agile-transformation-office-is-your-ticket-to-real-and-lasting-impact, 22.08.2024.

http://www.netsetglobal.rs/biometrijska-autentikacija/, 21.09. 2024.

http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:510000-Beograd-Blagajniku-SPC-devet-godina-i-tri-meseca-zatvora-za-proneveru, 14.09.2014.

http://www.nsa.gov.rs/extfile/sr/1485/Umanjivanje_insajderske_pretnje-skripta_.pdf, 26.4.2024.

http://www.nsa.gov.rs/tekst/80/obuke.php, 26.4.2024

http://www.osha.gov/workplace-violence, 31.03.2022.

http:/www./officerreports.com/blog/the-role-of-technology-in-security-guard-operations/, 02.09. 2024).

http://www.ratel.rs/uploads/documents/empire_plugin/Model%20Akta%20o%20bezbednosti%20lat.pdf, 18.10.2023.

http://www.seecsa.org/, 26.3.2024.

http://www.securelist.com/spam-and-phishing-in-q1-2017/78221/, 15.12.2020.

http://www.securityinfowatch.com/, 03.09.2024.

http://www.securitymagazine.com/keywords/5974-iot-security, 22.08.2024.

http://www.securityskills.eu/, 08.11.2023.

http://www.silabs.com/security, 03.09.2024.

http://www.sr.economy-pedia.com/11040327-return-on-investment-roi#google_vignette, 21.09.2024.

http://www.forrester.com/report/topic-overview-business-intelligence/RES39218, 30.06.2024.

http://hbr.org/webinar/2018/02/artificial-intelligence-for-the-real-world, 18.08.2024.

http://www.cert.rs/publikacije.html?kategorija=sve-publikacije&page=3,12.01.2023.

http://www.cert.rs/files/shares/Sajber%20Kultura%20Ratel%20web%20V0.5.6.pdf, 2.2.2024.

http://www.youtube.com/watch?v=j94ErQD8Uo, 01.09.2024.

http://www.youtube.com/watch?v=vx51DtgBEBQ, 09.08.2024).

http://www.youtube.com/watch?v=mIQHr1cevis, 19.08.2024).

http://www.youtube.com/watch?v=qN6nnJ8ncL0, 18.09. 2024.

http://www.youtube.com/watch?v=-rOdYR-OZfM&list=PLz97rFi-OzLfkBjxjtkICApnRKIzjjFtD&index=1

http://www.youtube.com/watch?v=r8NGNxtm9hI, 14.08.2024).

http://www.youtube.com/watch?v=CLQD54CYt64, 03.09.2024).