KORPORATIVNA SIGURNOST

Mikić, Marko

Sveučilište u Rijeci
Poslijediplomski specijalistički studij
Kriminalističko istraživanje

Marko Mikić

KORPORATIVNA SIGURNOST

(završni rad)

Rijeka, 2018.

Sveučilište u Rijeci
Poslijediplomski specijalistički studij
Kriminalističko istraživanje

Marko Mikić

KORPORATIVNA SIGURNOST

(završni rad)

Student: Marko Mikić

Mentor: Petar Veić, prof.dr.sc

Rijeka, 2018.

Sveučilište u Rijeci

Poslijediplomski specijalistički studij

Kriminalističko istraživanje

Izjava o autentičnosti završnog rada

Ime i prezime: Marko Mikić

JMBAG: 0034017154

Izjavljujem da je završni rad na temu Korporativna sigurnost moje autorsko djelo koje sam samostalno izradio.

Korištena literatura na koju sam se referirao nalazi se u popisu literature i citirana je u radu.

Student:

Marko Mikić

Rijeka, 2018.

SAŽETAK

Korporativna sigurnost jedan je od temeljnih pretpostavki sigurnog poslovanja poduzeća. U svojoj se suštini bavi identifikacijom rizika i pronalaženjem načina da razni rizici na što manje negativan način utječu na poslovanje poduzeća. Korporativna sigurnost podrazumijeva uspostavljenu organizaciju čiji je temeljni cilj obuhvatiti područja koja mogu biti izložena raznim ugrozama, a koje se adekvatnim upravljanjem mogu izbjeći ili ublažiti. Sigurnosni poslovi uključuju uspostavu procesa identifikacije i upravljanja rizicima, business intelligence, klasifikaciju informacija, zaštitu podataka, zaštitu osobnih podataka, informacijsku sigurnost, podizanje svijesti zaposlenika poduzeća o sigurnosti, poslove tehničke sigurnosti, tjelesne i fizičke sigurnosti, zaštite na radu, zaštite od požara i zaštite okoliša, sigurnosti kadrova, sprječavanja pranja novca i financiranja terorizma, i mnoge druge poslove u ovisnosti o djelatnosti kojom se određeno poduzeće bavi. Krajnji cilj korporativne sigurnosti jest osigurati kontinuitet poslovanja u uvjetima krize i što brži opravak od njenih negativnih utjecaja te uspješan nastavak poslovanja poduzeća.

SUMMARY

Corporate security is one of the basic preconditions for safe business operations. It is essentially concerned with identifying risks and finding ways to mitigate the variable risks effects on the company's business in the least negative way. Corporate Security implies an established organization whose basic objective is to cover areas that may be subject to various threats, which can be avoided or alleviated by adequate management. Security activities include the establishment of risk identification and management processes, business intelligence, information classification, data protection, personal data protection, information security, improving employee safety awareness, technical security, proximity and physical security, health and safety at work, fire and environmental protection, personnel security, the prevention of money laundering and terrorist financing and many other activities depending on the activity that a particular company deals with. The ultimate goal of corporate security is to ensure the continuity of business operations in crisis conditions and the quicker rebound from negative impacts and the successful continuation of business operations.

Ključne riječi

Rizik

Kriza

Poduzeće

Upravljanje

Sigurno poslovanje

Poslovni procesi

Kontinuitet poslovanja

Sadržaj:

1. Uvod

Svako poduzeće teži sigurnom poslovnom okruženju. Ovaj rad proučava ulogu korporativne sigurnosti te njezinu ulogu i važnost u poslovanju svakog poduzeća, obzirom da je upravo korporativna sigurnost pretpostavka za sigurno poslovanje poduzeća.

Uvjeti za sigurno poslovanje postižu se na način da se kontinuirano nalaze načini kako eliminirati i umanjiti sve rizike i ugroze koje mogu negativno utjecati na poslovanje.

Rizici se ne mogu uvijek i u potpunosti eliminirati, no cilj je svesti ih na najmanju moguću mjeru, na način da se iste unaprijed što preciznije pokuša identificirati, te da se na potencijalne rizike unaprijed pronađu odgovori, a sve s ciljem da poduzeće normalno posluje u uvjetima raznih poslovnih izazova, poteškoća i kriza. Glavni zadatak korporativne sigurnosti je prevladavanje kriza u poslovanju i uspostava normalnog poslovanja u najkraćem mogućem roku.

Predmet ovog rada je analiza uspostave i funkcioniranja procesa korporativne sigurnosti, detektiranje poslovnih procesa koji podrazumijevaju poslove korporativne sigurnosti, analiza mogućih rizika koji mogu predstavljati opasnost za sigurno poslovanje poduzeća, analiza modela i mogućnosti odgovora na izazove koje pred poduzeća stavlja izuzetno turbulentno i riziku visoko izloženo poslovno okruženje.

Svako poduzeće u svom radu susreće se s pitanjem: „Na koji način spriječiti ili umanjiti rizike i ugroze poslovnih procesa i na koji se način boriti protiv rizika?“ Da bi se dobio najtočniji odgovor na ovo pitanje prije svega je važno dobro poznavati normativni okvir i temeljem njega odabrati svoju sigurnosnu politiku.

U ovom radu analiza normativnog okvira korporativne sigurnosti provest će se temeljem međunarodnih, europskih i hrvatskih pravnih akata i normi koji se bave pitanjima rizika, zaštite podataka (s naglaskom na zaštitu osobnih podataka), informacijske i tehničke sigurnosti, fizičke zaštite, zaštite podataka, osiguravanja kontinuiteta poslovanja, zaštite na radu i zaštite od požara, sprečavanja pranja novca i financiranja terorizma.

Rad također govori i o dizajnu procesa upravljanja korporativnom sigurnosti, organizaciji poslova korporativne sigurnosti u većim i manjim poduzećima, rizicima koji stvaraju prijetnju sigurnom poslovanju poduzeća, business intelligence-u koji poduzećima pomaže u ostvarenju poslovnih ciljeva, važnosti podizanja svijesti o važnosti sigurnosti, upravljanju kontinuitetom poslovanja u uvjetima ugroze i krize, te o neizostavnoj suradnji između organizacijske jedinice poslova korporativne sigurnosti s kontrolnim funkcijama poduzeća.

Analizom će se obuhvatiti međunarodni, europski i hrvatski pravni akti i standardi i to:

Međunarodni standardi i Uredba Europskog parlamenta i Vijeća:

- ISO 27001:2013, Information security management
- ISO 31000:2009, Risk management - Principles and guidelines
- ISO 31010:2009, Risk management - Risk assessment techniques
- ISO 22301:2012, Societal security - Business continuity management systems - Requirements
- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka

Dokumenti i pravni akti Republike Hrvatske:

- Ustav Republike Hrvatske,
- Zakon o informacijskoj sigurnosti,
- Zakon o provedbi opće uredbe o zaštiti podataka,
- Zakon o sprječavanju pranja novca i financiranja terorizma,
- Zakon o zaštiti na radu,
- Zakon o zaštiti od požara,
- Zakon o privatnoj zaštiti,
- Pravilnik o uvjetima i načinu provedbe tehničke zaštite
- Smjernice za upravljanje informacijskom sustavom u cilju smanjenja operativnog rizika.

2. Upravljanje procesima korporativne sigurnosti

Suvremena poduzeća posluju u vrlo dinamičnom okruženju, zahvaćena su velikim turbulencijama koje su posljedica ekonomskih, političkih, društvenih, zakonodavnih i mnogih drugih događaja. Takvi uvjeti ograničavaju predviđanje budućih događaja, povećavaju neizvjesnosti u poslovanju, poslovanje postaje izloženo velikim rizicima. Upravo stoga, sve veća pozornost okrenuta je prema identifikaciji, procjeni i rukovanju rizicima, upravljanju rizicima te uspostavi obrambenih mehanizama (korporativna sigurnost), kako bi strateški ciljevi poduzeća bili ispunjeni.[1]

Svako poduzeće, kako bi kvalitetno ispunilo svoju svrhu, mora definirati svoju misiju i viziju. Proces strateškog menadžmenta upravo i započinje utvrđivanjem vizije i misije.

Misija je jedan od najvažnijih elementa strateškog menadžmenta. Ona je iskaz onoga čime će se poduzeće baviti i odgovara na dva osnovna pitanja:

1) Što je naša svrha?
2) Koja vrsta poduzeća želimo biti?

Misija objašnjava ulogu poduzeća u gospodarstvu i društvu. Definira svrhu poduzeća po kojoj se ono razlikuje od svojih konkurenata, ona se bavi svrhom i razlogom postojanja poduzeća danas.[2]

Vizija se odnosi na sliku stanja poduzeća u budućnosti.

Strategija je pojam koji potječe od starogrčke riječi „*strategus*“, u to doba podrazumijevala je osobu koja ima neki visoki vojni čin. Strategija danas daje odgovore na sljedeća pitanja:

- Kako se prilagoditi promjenjivim uvjetima na tržištu?
- Kako adekvatno rasporediti resurse?
- Kako biti konkurentan i zadovoljiti potrebe kupaca?
- Kako pozicionirati poduzeće na tržištu u odnosu prema konkurenciji i izbjeći poteškoće?
- Kako definirati akcije i pristupe kojima se jača svaki funkcionalni i operativni dio poduzeća[3]

[1] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, udruga hrvatskih menadžera sigurnosti – UHMS, 2011., str. 66.
[2] Buble M.[et.al], Strateški menadžment, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2005., str. 90.
[3] Buble M., Osnove menadžmenta, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2006., str. 106.

„Strategija je proces unaprijed definiranog plana pa se implementacija, odnosno provedba strategije može definirati kao proces zamjene strategije novom, pri čemu se mijenjaju mnogi temeljni strateški elementi kao što su vizija i misija poduzeća, ali i različiti resursi nužni za realizaciju planiranih ciljeva i zadataka.“[4]

Unutar svakog poduzeća, osim definiranja vizije, misije, strategije i strateških ciljeva, potrebno je definirati i kreirati sigurnosnu strategiju i sigurnosne poslovne procese, s ciljem uspostave što sigurnijeg poslovnog okruženja.

Poslovima korporativne sigurnosti podrazumijevaju se poslovi:

- administrativne sigurnosti (uspostava politika i procedura),
- informacijske sigurnosti (sigurnost informacijskih sustava),
- fizičke i tehničke sigurnosti (osiguranje imovine i opreme),
- zaštite podataka (poslovna tajna, zaštita osobnih podataka),
- sigurnosti vlasništva (intelektualno vlasništvo),
- osobna sigurnost (zaštita osoba, zaštita na radu, zaštite od požara)
- suradnje s kontrolnim funkcijama,
- podizanja svijesti o sigurnosti kroz kontinuirane edukcije i usavršavanja, …

Različita poduzeća izložena su različitim sigurnosnim rizicima, tako je, na primjer, bankarska sigurnost bitno različita od one u poduzećima koja se bave naftnim bušotinama ili od korporativne sigurnosti u zdravstvenom sektoru ili inovacijskom sektoru.

Sigurnosna strategija u pravilu je dugoročna i teško podnosi promjene u kraćem vremenskom razdoblju. Kvalitetno definiranom sigurnosnom strategijom gradi se svojevrsna kultura i potrebno je puno vremena da bi se ista implementirala, prihvatila i mijenjala.

Sigurnosna strategija uvijek mora biti u skladu s poslovnom strategijom poduzeća. Uzimajući u obzir da na poslovanje poduzeća utječe puno faktora poput ekonomskih, političnih, zakonodavnih, društvenih, pravnih, jednostavno se može zaključiti da poduzeća posluju u vrlo dinamičnim i turbulentnim uvjetima.

Kako bi ostvarilo svoje poslovne ciljeve, na sve te događaje i okolnosti poduzeće mora unaprijed biti spremno dati odgovor. Stoga je važno precizno utvrditi sve potencijalne rizike koji mogu pogoditi poslovanje poduzeća. Identifikacijom i upravljanjem rizicima, te

[4] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, udruga hrvatskih menadžera sigurnosti – UHMS, 2011., str.23.

uspostavom obrambenih mehanizama može se kvalitetno osigurati kontinuitet poslovanja i ostvarenje poslovnih ciljeva.

Pitanja sigurnosne strategije uređena su raznim zakonima, ISO međunarodnim standardima, direktivama Europske Unije, te na temelju njih izrađenih internih politika i procedura poduzeća.

Procesi korporativne sigurnosti u poduzećima uglavnom su potporni proces (osim u poduzećima koja se bave uslugama razvoja i praćenja sigurnosti), no time što su potporni procesi ne treba im umanjiti važnost, obzirom da su jedna od temeljnih pretpostavki uspješnog poslovanja poduzeća.

3. Dizajn procesa korporativne sigurnosti

Kako bi se uspostavio proces korporativne sigurnosti potrebno je ustrojiti organizacijske jedinice za korporativnu sigurnost. Organizacijska struktura jedinica za korporativnu sigurnost ovisi o veličini poduzeća (broju djelatnika u poduzeću) i o teritorijalnoj rasprostranjenosti poslovnih jedinica poduzeća.

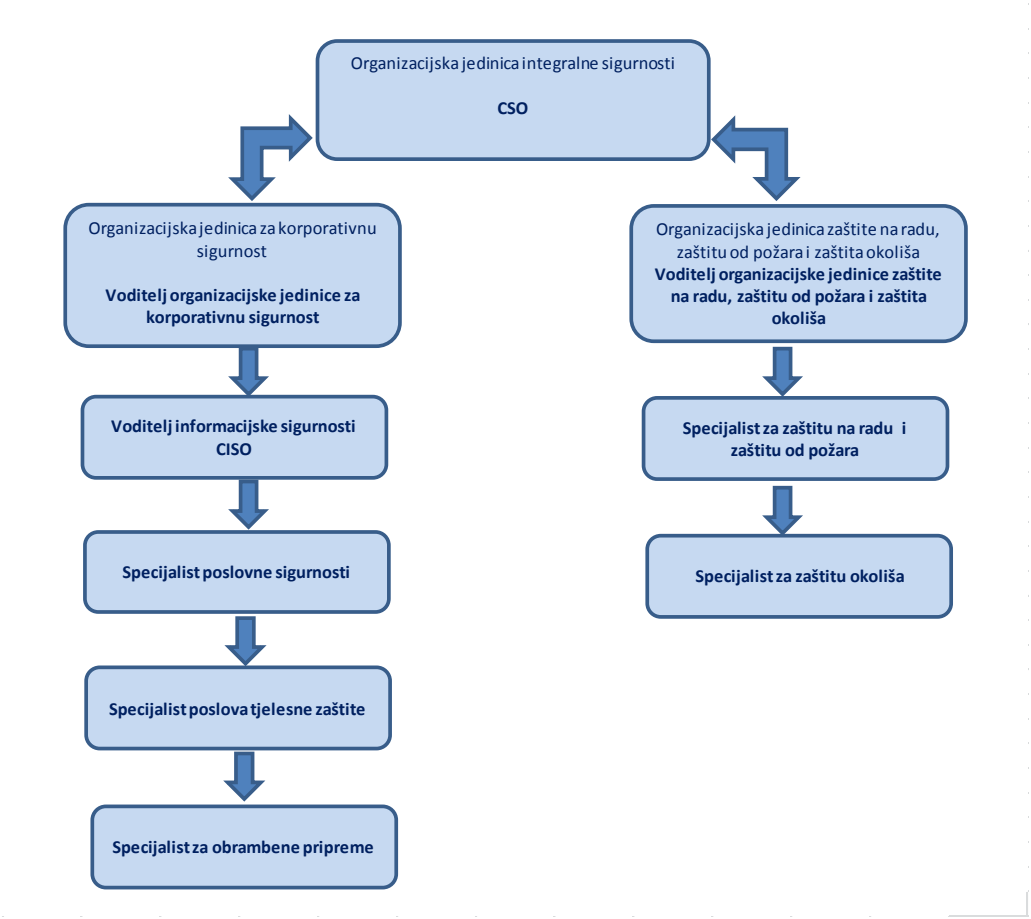
3.1 Korporativna sigurnost u većim poduzećima (integralna sigurnost)

U poduzećima s većim brojem djelatnika ili teritorijalno rasprostranjenim poslovnim jedinicama, jedinica za korporativnu sigurnost na organigramu poduzeća treba biti postavljena visoko, te je preporuka da direktno odgovara upravi poduzeća.

U velikim poduzećima se poslovi korporativne sigurnosti nazivaju još i poslovima integralne sigurnosti.

Jedinica integralne sigurnosti dijeli se na:

- organizacijsku jedinicu za korporativnu sigurnost i
- organizacijsku jedinicu zaštite na radu, zaštite od požara, zaštite okoliša.



Slika 1. Prikaz organizacije organizacijske jedinice integralne sigurnosti

3.1.1 Voditelj organizacijske jedinice integralne sigurnosti

Organizacijskom jedinicom integralne sigurnosti upravlja Chief Security Officer (dalje u tekstu: CSO). Riječ je o najvišoj izvršnoj funkciji, te je za ovu funkciju preporuka da odgovara najvišem upravljačkom tijelu poduzeća, najčešće upravi poduzeća, a u svojoj odgovornosti ima identifikaciju, razvoj, implementaciju i kontrole procesa korporativne sigurnosti.

Osnovna zadaća CSO-a je da kroz uspostavljene politike i procedure osigura postupke kojima je cilj pravodobna identifikacija rizika, smanjenje rizika, te odgovor na rizike i incidente kojima je poduzeće izloženo u svom radu.

CSO je odgovoran za razvoj i primjenu strategija koja će dati odgovor na katastrofalne događaje koji potencijalno mogu ugroziti cjelokupno poslovanje poduzeća. CSO je odgovoran za procjenu ranjivosti poduzeća (procjenu rizika koji mogu ugroziti rad poduzeća), prevenciju incidenata, održavanje spremnosti organizacije u slučaju napada, katastrofe ili drugog sigurnosnog incidenta (na primjer pljačke, prijevare i slično), zaštitu radnika, zaštitu informacijskog sustava, zaštitu podataka, informacija, zaštitu reputacije. CSO je odgovoran uspostaviti sigurnosni proces na način da se osigura kontinuitet poslovanja i onda kada nastupe određeni rizici.

CSO mora imati razne kompetencije i vještine, od kojih valja izdvojiti:

- znanje (specifične činjenice, informiranost, razumijevanje specifičnog posla kojim se poduzeće bavi),
- sposobnost povezivanja i interpretacije velike količine informacija prilikom identificiranja problema i njihova rješavanja,
- akademske kvalifikacije, dovoljan broj godina radnog iskustva na poslovima sigurnosti,
- izraženu osobnost, temperament, visoko razvijene radne navike, sposobnost pokretanja promjena,
- visoko razvijene menadžerske vještine, sposobnost motiviranja zaposlenika, sposobnost upravljanja promjenama,
- orijentiranost ciljevima, upornost u rješavanju prepreka, spremnost na preuzimanje odgovornosti,
- visoku emocionalnu inteligenciju i jasna moralna načela,
- razvijene komunikacijske vještine (verbalne i neverbalne).

3.1.2 Voditelj jedinice za korporativnu sigurnost

Voditelj organizacijske jedinice za korporativnu sigurnost neposredno je odgovoran CSO-u. Unutar jedinice za korporativnu sigurnost mogu biti ustrojeni poslovi odjeli za sljedeće poslove: informacijsku sigurnost, poslovnu sigurnost, tjelesnu zaštitu i obrambene pripreme.

Jedan od najzahtjevnijih poslova unutar jedinice za korporativnu sigurnost odnosi se na informacijsku sigurnost. Uslijed činjenice da se danas u svijetu gotovo sve odvija on-line, da su informacije i podaci na cijeni kao „rudnik zlata“, važno je zaštiti ih od zlonamjernika, organiziranih skupina čiji je cilj ugrožavanje poslovanja ili potpuno uništenje poduzeća.

3.1.2.1 Voditelj odjela informacijske sigurnosti

Organizacijskom jedinicom informacijske sigurnosti upravlja Voditelj informacijske sigurnosti ili Chief information security officer (dalje u tekstu: CISO).

CISO je odgovoran za sljedeće zadatke:

- razvoj i primjena strategija sigurnosti informacijskog sustava,
- procjena rizika sigurnosti informacijskog sustava,
- izrada politika, procedura i smjernica koje imaju za cilj osigurati zadovoljavajuću razinu sigurnosti informacijskog sustava,
- analiziranje sigurnosnih potreba, predlaganje rješenja, analiza isplativosti ulaganja u sigurnosna rješenja,
- razvoj, testiranje i implementacija sigurnosnih rješenja u cilju povećanja sigurnosti informacijskog sustava,
- sudjelovanje u izobrazbi svih zaposlenika koji se u svom radu koriste informacijskim sustavom s ciljem korištenja sustava na siguran način,
- suradnja s IT organizacijskom jedinicom, s revizorima (internim i eksternim), s poslovnim jedinicama, menadžmentom.

3.1.2.2 Specijalist poslovne sigurnosti

Specijalist poslovne sigurnosti je operativna funkcija zadužena za provođenje definiranih politika korporativne sigurnosti, neposredno sudjeluje u organiziranju mjera prevencije incidentnih događaja, kontrolira provode li se politike i procedure sigurnosti, predlaže mjere za poboljšanja, mjere za svladavanje prepreka i mjere za izlazak poduzeća iz krize izazvane određenim incidentom. Specijalist poslovne sigurnosti također predlaže mjere tehničke i tjelesne zaštite radnika i imovine, te educira radnike kroz razne programe osposobljavanja.

3.1.2.3 Specijalist poslova tjelesne zaštite

Specijalist tjelesne zaštite organizira poslove tjelesne zaštite, koordinira i upravlja te daje neposredne upute izvršiteljima usluga tjelesne zaštite, obavlja nadzor nad radom ugovornih izvršitelja tjelesne zaštite, vodi brigu o uspostavi evidencija o posjetiteljima poduzeću, kontinuirano prati rad djelatnika koji rade na poslovima tjelesne zaštite.

3.1.2.4 Specijalist za obrambene pripreme

Specijalist za obrambene pripreme procjenjuje obrambene potrebe, prati zakone koji reguliraju obrambene pripreme, izrađuje plan obrane te koordinira i prati provedbu plana u slučaju potrebe.

3.1.3 Voditelj jedinice za zaštitu na radu, zaštitu od požara i zaštitu okoliša

Voditelj jedinice za zaštitu na radu, zaštitu od požara i zaštitu okoliša neposredno je odgovoran CSO-u. Unutar jedinice za zaštitu na radu, zaštitu od požara i zaštitu okoliša mogu biti zasebno ustrojene jedinice za zaštitu na radu, zaštitu od požara i zaštitu okoliša.

3.1.3.1 Specijalist za zaštitu na radu i zaštitu od požara

Specijalist za zaštitu na radu i zaštitu od požara izrađuje plan aktivnosti zaštite na radu i zaštite od požara, interne akte i pravilnike, organizira i osigurava osposobljavanje radnika za rad na sigurna način, surađuje s inspekcijama rada i inspekcijama zaštite od požara, koordinira s ugovornim izvršiteljima iz područja zaštite na radu (kontrola vida, sluha, razna mjerenja svjetlosti i sličnih uvjeta u radnim prostorijama, udaljenost i pozicija računala u odnosu na radnika, …) provodi nadzor nad provedbom mjera zaštite na radu i zaštite od požara.

3.1.3.2 Specijalist zaštite okoliša

Specijalist zaštite okoliša izrađuje plan zaštite okoliša, procedure i ostale interne akte, nadzire provedbu internih akata i kontinuirano unaprjeđuje procese vezane uz zaštitu okoliša, te surađuje s nadležnim inspekcijama.

3.2 Korporativna sigurnost u manjim poduzećima

U poduzećima s manjim brojem djelatnika potrebno je ustrojiti odbor za sigurnost ili imenovati menadžera za sigurnost. Tako ustrojena jedinica za korporativnu sigurnost treba biti organizirana na način da direktno odgovara top menadžmentu, a ukoliko ni to nije ekonomski isplativo (u slučaju poduzeća s jako malim brojem zaposlenika), jedan od top menadžera poduzeća može ujedno obnašati funkciju menadžera za sigurnost.

4. Rizici i mitigacija rizika

Rizik (engl. *risk*, njem. *Risiko*, *Wagnis*) u širem značenju označava pojam opasnosti.

Rizikom se smatra opasnost koja se do stanovite mjere može predvidjeti i kojoj se može odrediti intenzitet. Rizikom se također smatra eventualni gubitak ili šteta protiv kojih se plaća osigurnina.[5]

Rizici trebaju biti visoko na listi prioriteta svake organizacije.

Prema Normi ISO 31000:2009 (dalje u tekstu: ISO 31000) rizik se definira kao djelovanje nesigurnosti na ciljeve organizacije.[6]

Ciljevi organizacije mogu biti financijski, reputacijski, zdravstveni, pravni, organizacijski, strateški, proizvodni... Rizici su nesigurnosti koje mogu imati za posljedicu odstupanja od očekivanih rezultata, pozitivna i negativna. Rizik se često opisuje kao kombinacija posljedica nekoga događaja na neko poduzeće i pridruženih vjerojatnosti njihovih pojava.

Norma ISO 31000 preporučuje poduzećima da razvijaju, provode i poboljšavaju procese upravljanja rizikom, te da ih implementiraju u upravljanje, strategiju, planiranje, izvješćivanje, politike, vrijednosti i kulturu poduzeća. Cilj preporuka je povećavati vjerojatnost postizanja ciljeva, poboljšavati reakcije na negativne događaje i opasnosti koje oni donose, poboljšati povjerenje svih sudionika koji na bilo koji način sudjeluju u procesima poduzeća.[7]

Kako je osnovni cilj sigurnosne strategije omogućiti ostvarivanje poslovne strategiju, važno je postaviti mehanizme za identifikaciju i sprječavanje rizika ili alate kojima će njihov utjecaj imati minimalne negativne utjecaje na poslovanje. Važno je pronaći adekvatan model za ublažavanje rizika (mitigaciju rizika).

Rizike je važno pravodobno identificirati, analizirati i vrednovati ih i njima upravljati. Kvalitetnom identifikacijom i vrednovanjem potencijalnih rizika poduzeće će biti spremnije na njih odgovoriti.

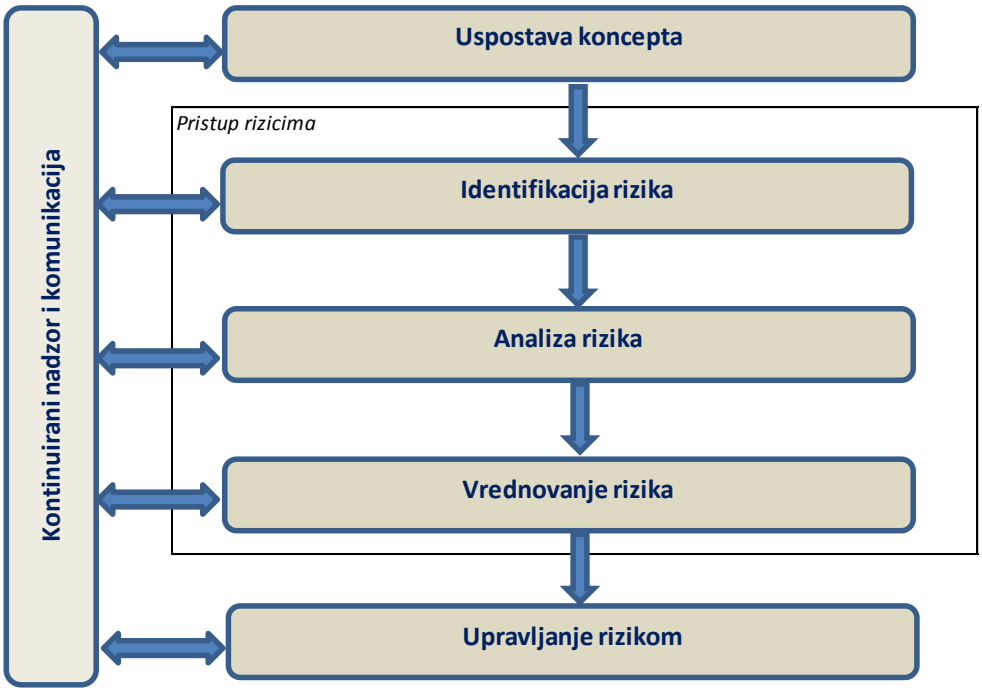
Kada se govori o upravljanju rizicima dobro je spomenuti i normu ISO 31010:2009 (dalje u tekstu: ISO 31010). Riječ je o normi koja predstavlja svojevrsnu potporu normi ISO 31000.

[5] Hrvatski jezični portal, dostupno na: http://hjp.znanje.hr/
[6] ISO 31000:2009, Risk management - Principles and guidelines
[7] Ibid.

ISO 31010 detaljno opisuje proces i metode upravljanja rizicima, te načela koja trebaju biti zadovoljena da bi upravljanje rizikom bilo djelotvorno. [8]

Kvalitetno upravljanje rizicima pouzdan je temelj za donošenje odluka i planiranje, s ciljem da se gubici svedu najmanju moguću mjeru.

Postoje različite podjele rizika, no u sljedećim poglavljima bit će detaljnije opisani oni najzastupljeniji u svakom poslovanju: strateški, poslovni, financijski, operativni.



Slika 2. Proces upravljanja rizikom

[8] Ibid.

4.1 Strateški rizici

Strateški rizik povezan je s promjenama u poslovanju u odnosu na prvobitno donesene strateške odluke. To su rizici proizašli kao posljedica strateških odluka ili odabira poslovnih alternativa pri čemu nije došlo do kršenja pravila, regulativa ili etičkog ponašanja, ili koji nisu inicirani pravnim rizikom.

Strateški rizici podrazumijevaju mogućnosti nastanka negativnih djelovanja na rezultat poslovanja uslijed loših poslovnih odluka ili njihove neodgovarajuće implementacije ili pak nedovoljnog razumijevanja promjena na tržištu.

Strateškim rizicima smatraju se: gubitak ključnih kupaca, promjena ponašanja potrošača, reputacijski rizik, rizik inovacija, rizik brenda, rizik planiranja, rizik istraživanja tržišta i razvoja, rizik investicija, rizik ulaska na nova tržišta…

Kvalitetnim identificiranjem rizika i unaprijed osmišljenim modelima može se na vrijeme prevenirati njihov loš utjecaj na poslovanje. Kontinuiranim preispitivanjem donesenih odluka, sustavnim praćenjem promjena na tržištu, praćenjem potreba kupaca i pravodobnim pronalaskom alternativa koje će nadoknaditi potencijalne gubitke uslijed pogrešnih ili neadekvatnih poslovnih odluka može se smanjiti mogućnost utjecaja strateških rizika na poslovanje poduzeća.

4.2 Poslovni rizik

Poslovni rizik podrazumijeva fluktuacije profita o odnosu na s očekivane rezultate, a koji nije povezan s rizicima poput rizika kamatnih stopa, rizik tečaja, i slično, već je povezan s volatilnosti volumena ili promjena u ukusima klijenata.

Slijedi primjer poslovnog rizika u poslovanju banke. Banka je u svoju ponudu uvrstila kreditni proizvod koji nije konkurentan banka i kojeg ne može plasirati na tržište. Sredstva namijenjena kreditiranju klijenata stoje neiskorištena na računima banaka. Banka povećava svoju likvidnost, sredstva stoje neiskorištena tj. nisu stavljena u svoju funkciju radi čega banka ne ostvaruje prihode od prodaje, a sve radi pogrešne poslovne odluke o karakteristikama proizvoda, obzirom da za takav kreditni proizvod ne postoji potražnja radi njegovih nepovoljnih karakteristika.

4.3 Financijski rizici

Financijski rizik (engl. financial risk, njem. Finanzrisiko), predstavlja rizik kod fiksnih troškova financiranja (rizik da se ostvarenim financijskim rezultatom neće pokriti kamate na dugove poduzeća) i/ili rizik koji proizlazi iz stupnja zaduženosti poduzeća (rizik da poduzeće neće biti u mogućnosti vratiti dug). Stupanj rizika se povećava usporedno sa stupnjem zaduženosti poduzeća.[9]

Financijskim rizikom smatraju se tržišni/sistemski rizik, valutni rizik, kamatni rizik, cjenovni rizik, rizik likvidnosti, kreditni rizik…

Primjer financijskog rizika (kombinacija valutnog rizika, cjenovnog rizika i rizika likvidnosti) na primjeru zaduženja banke kod matične banke u inozemstvu. Banka se zadužuje kod svoje matične banke u inozemstvu u EUR-ima uz kamatu 2%. Trošak izvora za banku, kada se dodaju ostali troškovi, je 3%, što predstavlja minimum ispod koje banka ne može plasirati sredstva čak i bez ikakve zarade. Pribavljena sredstva plasira kroz kredite u kunama. Tečaj kune u trenutku posudbe sredstava u odnosu na EUR bio je 7,500000, nakon toga tečaj kune pada i iznosi 7,300000 (banka u kunskoj protuvrijednosti sada raspolaže s manje kuna koje je planirala plasirati kroz kredite, čime snosi negativne posljedice promjene tečaja – tečajni rizik). Istodobno na tržištu padaju cijene kredita u kunama. Banka je izložena cjenovnom riziku, jer spuštanjem cijene kredita smanjuje maržu (zaradu) u odnosu na cijene svojih izvora. Ne spusti li kamatne stope i ne učini li cijenu kredita konkurentnom, za iste neće postojati potražnja, što će banku dovesti u rizik prekomjerne likvidnosti.

4.4 Operativni rizici

Svako se poduzeće u svom radu susreće s operativnim rizicima, bez obzira o kojoj je djelatnosti riječ.

Operativni rizik teže je identificirati, izmjeriti i njime upravljati. Operativni se rizik može dogoditi u poduzeću na način da je najčešće isprepleten s ostalim rizicima, a upravljanje operativnim rizicima važna je pretpostavka stabilnog i uspješnog poslovnog djelovanja.

Operativnim rizicima smatraju se: greške u procedurama, štetno djelovanje zaposlenika, ozljede, požari, elementarne nepogode, regulatorni rizici, rizici prijevare, tehnološki rizik…

Primjer operativnog rizika je događaj u američkoj banci kada je nakon dugog niza godina prijevarnih radnji otkrivena milijunska interna prijevara zaposlenika (engl. fraud) koji je u

[9] Poslovni dnevnik, leksikon, dostupno na: http://www.poslovni.hr/leksikon/financijski-rizik

centima krao sredstva s računa klijenata. Ovdje je operativni rizik isprepleten sa strateškim rizikom (reputacijskim rizikom) što je u konačnici banci donijelo i financijske gubitke i gubitak povjerenja klijenata.

4.5 Ostali rizici

Osim prethodno navedenih rizika postoji još niz rizika s kojim se poduzeća mogu u svom djelovanju susresti i s kojim se mogu suočiti.

Neki od ostalih rizika su: klimatske promjene, terorizam, pojava i širenje zaraznih bolesti, politički, socijalni, gospodarski (rast ili pad bruto društvenog proizvoda), organizacijski (gubitak ključnih zaposlenika, česta promjena prioriteta od strane upravljačkih funkcija).

5. Business intelligence

Poslovna inteligencija (engl. Business Intelligence, dalje u tekstu: BI) prvi se puta spominje 1989. (spominje ju Howard Dresdner kako bi kategorizirao koncepte i metode koji pomažu u lakšem donošenju poslovnih odluka).[10]

„BI je proces prikupljanja podataka i informacija na temelju kojih se mogu predvidjeti budući procesi, događaji ili kretanja i koji nakon odgovarajuće obrade mogu poslužiti kao temelj i potpora u procesu donošenja poslovnih odluka. Dakle, BI je poslovno obavještajna aktivnost u poslovnom svijetu koja je usmjerena na prikupljanje podataka i informacija potrebnih za donošenje što kvalitetnijih poslovnih odluka u cilju uočavanja pozicije u poslovnom okruženju i postizanja poslovnog uspjeha“.[11]

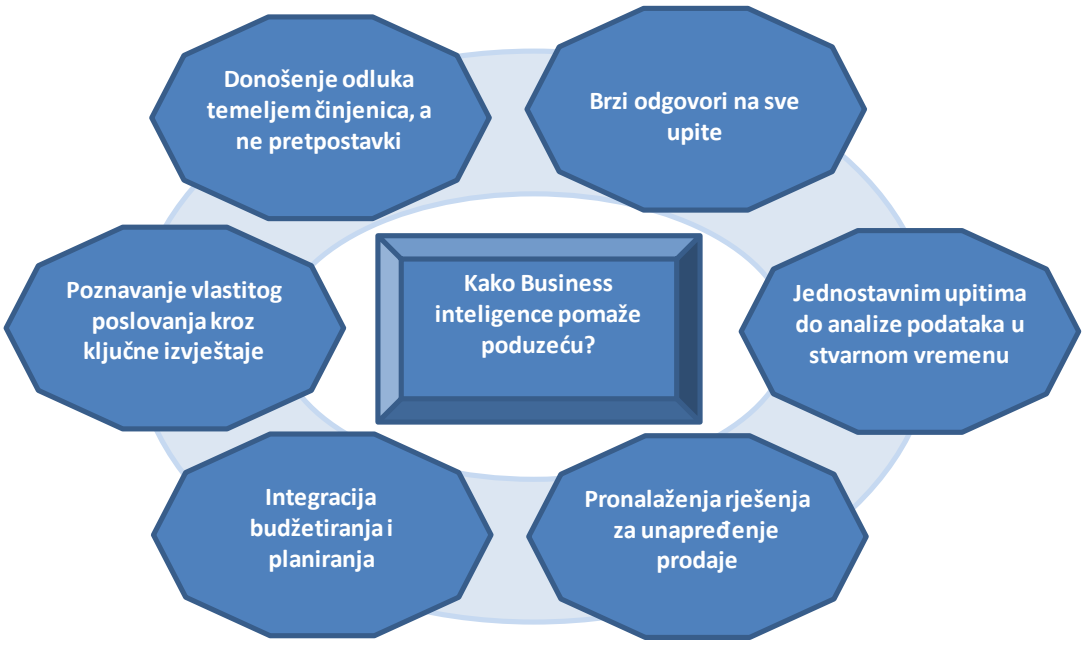
BI je skup metodologija za prikupljanje, analizu i distribuciju informacija uz pomoć različitih softverskih alata. To je transformacija podataka u informacije, a informacija u znanje.

Cilj BI je osigurati inteligentno ponašanje poduzeća, iz podataka donijeti informaciju koja će povećati uspješnost poslovanja, uočiti oku nevidljivo i skriveno, na temelju obrade velike količine internih podataka (poduzeća) i eksternih podataka (okruženja, tržišta).

BI je jedna od tehnika izvještavanja o informacijama koja omogućuje njihovo pronalaženje s ciljem lakšeg i točnijeg donošenja poslovnih odluka. BI može se odnositi na sposobnost shvaćanja i brzog snalaženja poduzeća u novim uvjetima poslovanja, temeljem prethodno prikupljenih, kategoriziranih i analiziranih informacija.

Neke metode poslovne inteligencije uključuju rudarenje podataka (Data Mining), skladištenje podataka (Data Warehousing, DWH) i OLAP (Online Analytical processing) mrežnu analitičku obradu podataka. [12]

[10] Dostupno na: https://hr.wikipedia.org/wiki/Poslovna_inteligencija
[11] Bilandžić M., Poslovno obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb, 2008. Str.71
[12] Dostupno na: https://hr.wikipedia.org/wiki/Poslovna_inteligencija



Slika 3: Prikaz važnosti Business intelligence-a poduzećima.

5.1 Rudarenje (kopanje) podataka

Rudarenje ili kopanje podataka može se definirati kao prikupljanje podataka iz raznih internih i eksternih izvora, njihovo sortiranje, organiziranje i grupiranje velikog broja podataka temeljem kojih se izvlače razumljive i relevantne informacije.

Informacije su korisne ukoliko se iz njih mogu izvući neki korisni podaci, stoga treba znati prepoznati i izdvojiti korisne informacije iz velike količine raznih podataka. Također, potrebno je pronaći vezu među podacima i trendove među njima.

Rudarenje podataka može koristiti svakom poduzeću, ali svoju najveću primjenu ima u sektoru IT-ja, bankarstva, osiguranja, marketinga…u tim sektorima ono pomaže identifikaciji raznih poslovnih događaja, poput navika potrošača, nalaženju prostora za unakrsnu prodaju, identifikaciju profitabilnih proizvoda, identifikaciju poslovnih prijevara i rizika…

5.2 Skladištenje podataka

Skladištenje podataka funkcionira po principu izdvajanja podataka iz baze i njihovo spremanje u posebne baze (skladište podataka).

Podaci u toj posebnoj bazi moraju se pripremiti za zahtjevne analize i pronalaženje informacija za kvalitetno odlučivanje.

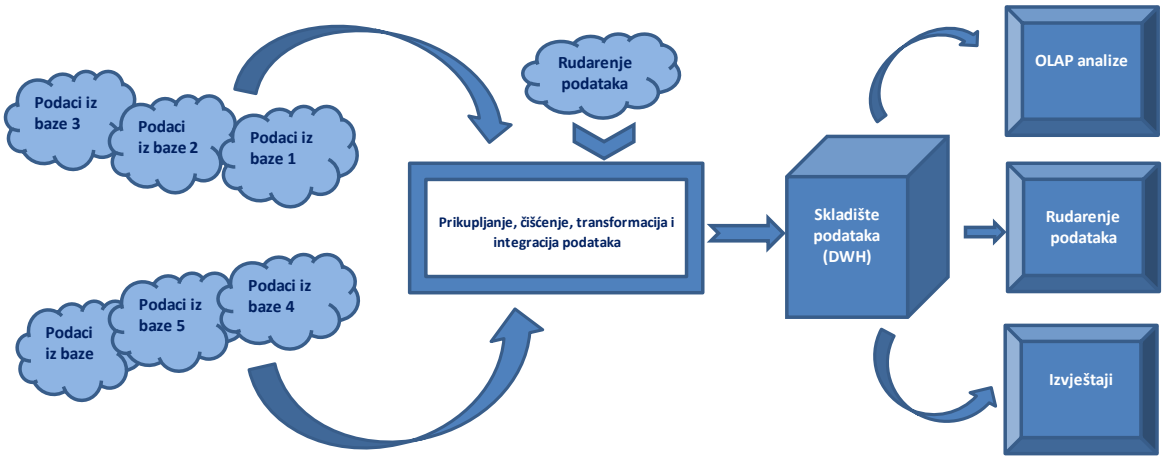
Skladište podataka sadrži podatke dužeg vremenskog perioda, što omogućuje usporedbe, analize i pretpostavke.

Raznim upitima u skladište podataka i analitičkim obradama tih podataka dobivaju se informacije korisne odlučivanje.

5.3 OLAP

OLAP (Online Analytical processing) je vrsta analitičke obrade podataka, koja omogućava brze upite na informacije, što korisnicima daje jednostavne i selektirane analize s raznih točki gledišta.

OLAP daje brzi odgovor na višestruke upite, obuhvaća relacijsko izvješćivanje i rudarenje podataka te iz organiziranih podataka (iz skladišta podataka) pomoću raznih upita kreira izvješte (primjer izvještaja: prikaz podataka o prikupljenim depozitima, po njihovoj vrsti i valuti, po poslovnici usporedno za zadnje 3 godine).



Slika 4: Proces prikupljanja, obrade, pohrane i korištenja informacija.

6. Klasifikacija informacija

Informacijom se može smatrati mnogo toga, ovisno u kojem se kontekstu promatra. Općenito informacija je skup organiziranih podataka koji imaju neko konkretno značenje. Informacije su moć. One su važne, svakim danom sve skuplje, zanimljivije i dragocjenije. Informacije su poslovne tajne, brojevi računa, brojevi kreditnih kartica, financijski podaci, osobni podaci klijenata, dobavljača, zaposlenika, …

Spominjući samo navedene primjere informacija jasno je kakve katastrofalne posljedice mogu imati poduzeća u slučaju njihove zlouporabe, neovlaštene distribucije, krađe. Takve informacije mogu biti korištene od strane konkurencije, korištene kao sredstvo u provođenju krivičnih djela, njihovo objavljivanje može biti prekršaj zakonske regulative i rezultirati velikim kaznama.

Upravo radi navedenog, prikupljanje, pohrana i distribucija informacija jako je osjetljivo područje, jer informacije su, radi svoje visoke vrijednosti, često predmet napada s ciljem njihove neovlaštene uporabe, distribucije i zlouporabe.

Objavljivanje povjerljivih informacija može izazvati ozbiljne financijske gubitke i uništenje reputacije, stoga bi svako poduzeće trebalo osigurati procese kvalitetnog i sustavnog upravljanja informacijama.

Prema normi ISO 27001:2013 (dalje u tekstu: ISO 27001) informacije treba klasificirati (upravljati njihovom sigurnošću) ovisno o njihovoj vrijednosti, zakonskoj reguliranosti, povjerljivosti, osjetljivosti, važnosti za poduzeće.[13]

Klasifikacija informacija pomaže poduzeću da razumije i osvijesti kojim sve informacijama upravlja, te da shodno tome identificira potencijalne rizike vezane uz informacije. Klasificirane informacije su važni resursi poduzeća koji moraju imati određenu razinu zaštite kako bi se osigurala njihova povjerljivost, cjelovitost i raspoloživost.

Neke informacije regulirane su zakonom ili sličnom regulativom (na primjer zaštita osobnih podataka o kojoj će se govoriti u sljedećem poglavlju). Kao primjer informacija reguliranih poslovnom tajnom može se uzeti ugovor s uvjetima suradnje između kupaca i dobavljača.

Neke je informacije potrebno zaštititi radi ostvarenja poslovnih ciljeva (na primjer informacije o novom proizvodu koje poduzeće planira lansirati na tržište). Nedovoljno dobro zaštićene informacije mogu postati dostupne trećim, neovlaštenim stranama, a obzirom da mogu

[13]ISO 27001:2013, Information security management

sadržavati vrlo osjetljive informacije poput poslovne tajne, zakonski zaštićene informacije (osobni podaci, financijski podaci) od izuzetne je važnosti njima upravljati s velikim oprezom. Rizici od prijetnji neovlaštenog pregleda, promjene ili brisanja informacija mogu se efikasno smanjiti uvođenjem procesa klasifikacije informacija u organizaciju, jer neadekvatno upravljanje informacijama može uzrokovati velike reputacijske i financijske gubitke te kazne.

7. Zaštita osobnih podataka

Upravo radi činjenice da se u informacijskim sustavima nalazi najveći broj raznih podataka informacijski sustavi predmet su najrazličitijih napada. Za neke od podataka, poput osobnih podataka, postoje zakonske obveze koje poduzećima nameću obvezu da osigura podacima povjerljivost, cjelovitost i raspoloživost.

Ustav Republike Hrvatske u svom članku 37 o zaštiti osobnih podataka nalaze sljedeće: „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita i nadzor nad djelovanjem informacijskih sustava u zemlji. Zabranjena je uporaba osobnih podataka suprotno utvrđenoj svrsi njihovog prikupljanja.“[14]

Trenutno zaštitu osobnih podataka u Republici Hrvatskoj regulira Zakon o provedbi opće uredbe o zaštiti podataka.[15]

Zakon o provedbi opće uredbe o zaštiti podatka na snazi je od 25. svibnja 2018., a donesen je kako bi se osigurala provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. Uredba je poznata pod nazivom General Data Protection Regulation (dalje: GDPR).[16]

Osobnim podatkom u smislu GDPR smatra se: ime, adresa, e-mail adresa, IP i MAC adresa, GPS lokacija, telefonski broj, fotografija, video snimka, OIB, biometrijski podaci (otisak prsta, snimka šarenice oka), genetski podaci, podaci o plaći, kreditnim obvezama, računima, podaci o obrazovanju, stručnoj spremi, zdravlju, seksualnoj orijentaciji, glas i mnogi drugi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se iz pribavljenih podataka može utvrditi.

Osnovni cilj GDPR uredbe je osigurati da se za prikupljaju i obrađuju isključivo podaci neophodni za određeni posao, a za koje postoji pravna, zakonska osnova, o čemu osoba koja ustupa osobne podatke mora biti jasno upoznata te mora biti suglasna (dati pisanu privolu) da se njegov osobni podatak prikuplja, čuva i obrađuje.[17]

---

[14] Ustav Republike Hrvatske, pročišćeni tekst, NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14, članak 37.
[15] Zakon o provedbi opće uredbe o zaštiti podataka, NN 42/2018
[16] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)
[17] Dostupno na: https://gdpr2018.eu/

Poduzeća u svakom trenutku moraju znati gdje se nalaze koji podaci i vrlo jasno odrediti u koju se svrhu oni smiju koristiti (prikupljati, obrađivati i distribuirati). Podaci se ne smiju prikupljati i obrađivati bez privole osobe o čijim je osobnim podacima riječ. Nepoštivanje odredaba GDPR uredbe kažnjivo je milijunskim kazne (do 20 milijuna eura).

GDPR uredba obvezuje sva poduzeća koja posluju na području Europske unije, a koja prikupljaju osobne podatke. Osobnim podacima poduzeća se mogu koristiti isključivo po pristanku osobe, koja svoju privolu može dati i opozvati u bilo kojem trenutku.

U slučaju kompromitiranja sigurnosti osobnih podataka, poduzeća su dužna obavijestiti nadležne službe, ali i pojedinca čiji su osobni podaci kompromitirani. Ugrožen može biti informacijski sustav kao cjelina, računala i podaci u računalima, podaci o poslovnim suradnicima, podaci o zaposlenicima, evidencije i baze podataka, poslovni procesi, telefonija, tehničko-sigurnosni sustavi, intelektualno vlasništvo.[18]

Primjenu GDPR uredbe svi su, u posljednje vrijeme, na neki način iskusili, bilo kao dio timova koji su u raznim poduzećima radili na njezinoj implementaciji, bilo kao privatne osobe koje su sa svih strana (od strane raznih institucija i privatnih poduzeća, web stranica, newsletter-a, nagradnih igara, raznih marketinških akcija,…) informirane o primjeni uredbe i o pravima koji iz nje proizlaze, a tiču se zaštite njihovih osobnih podataka.

[18] Dostupno na: https://gdpr2018.eu/

8. Informacijska sigurnost

U vremenu sve većeg razvoja tehnologije i njenu sveprisutnost, možda i ne treba posebno naglašavati važnost sigurnosti informacijskih sustava poduzeća. Temeljna načela informacijskog sustava su: povjerljivost, integritet, raspoloživost, neporecivost, dokazivost, autentičnost i pouzdanost.

Informacijska sigurnost nije isto što i informatička sigurnost. Informacijska sigurnost odnosi se zaštitu svih oblika informacija i podataka, bez obzira gdje se podaci i informacije nalaze.[19]

Posljedice narušavanja temeljnih načela informacijskog sustava su:

- gubitak integriteta (informacije moraju biti zaštićene od neovlaštene i neispravne izmjene),
- gubitak raspoloživosti (neraspoloživost sustava može negativno utjecati na ciljeve poduzeća i kontinuitet poslovanja).
- gubitak povjerljivosti (neovlašteno otkrivanje podataka može negativno utjecati na povjerenje u poduzeće, narušiti reputaciju poduzeća i donijeti financijske gubitke u slučaju sporova ili kazni)

Svako poduzeće se u svom djelovanju bavi prikupljanjem raznih vrsta podataka, počevši od osobnih podataka zaposlenika, do podataka o kupcima, dobavljačima, poslovnim suradnicima, podataka o tehnološkim inovacijama, poslovnim planovima i slično. Od iznimne je važnosti podacima koji se prikupljaju, obrađuju i dalje distribuiraju pristupiti s najvećom mogućom pažnjom.

Kada se govori o informacijskoj sigurnosti važno je djelovati s ciljem sprječavanja prijetnji i opasnosti koje prijete informacijskim sustavima. Ugrožen može biti svaki dio informacijskog sustava, sustav kao cjelina, računala i podaci u računalima, podaci o suradnicima, zaposlenicima, evidencije, mobilni telefoni, poslovni procesi, intelektualno vlasništvo, poslovne tajne, tehničko sigurnosni sustavi. Informacijski resursi izloženi su raznim prijetnjama i rizicima, oni mogu biti namjerni (prisluškivanje, neovlaštena izmjena informacija, hakiranje, maliciozni kod, krađa), ili slučajni (pogreške, slučajno brisanje podataka, slučajno uništenje informacijske opreme). Informacijski resursi mogu biti izloženi i prirodnim nepogodama poput požara, poplave, udara groma.

[19] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, udruga hrvatskih menadžera sigurnosti – UHMS, 2011., str. 94.

Cilj je osigurati zaštitu informacijskog sustava od neovlaštenog pristupa i distribucije informacija, poslovne špijunaže, malicioznih programa, krađe, uništenja opreme, prirodnih nepogoda i ostalih rizika kojima je informacijski sustav izložen.

U Republici Hrvatskoj informacijsku sigurnost, među ostalim aktima, regulira Zakon o informacijskoj sigurnosti[20]. Njime su definirani pojam, mjere i standardi informacijske sigurnosti, tijela za donošenja Zakona i nadzor nad provedbom mjera informacijske sigurnosti. Zakon je obvezujući za tijela državne uprave, jedinice lokalne samouprave i sve pravne osobe koje u svom poslovanju koriste klasificirane i neklasificirane podatke.

Jedna od osnovnih normi za upravljanje informacijskom sigurnošću je norma ISO 27001.[21]

Norma daje smjernice i pravila o upravljanju sustavom informacijske sigurnosti, definira potrebu za uspostavom, nadzorom, održavanjem i stalnim poboljšavanjem sustava upravljanja informacijskom sigurnošću. Norma postavlja smjernice koje mogu pomoći poduzećima da razviju vlastite kvalitetne sustave upravljanja informatičkom sigurnošću, na način da u sustav budu uključeni djelatnici, procesi, informacijski sustav i politike poduzeća (Information Security Management System). Nakon što poduzeće osigura primjenu ISO 27001 može ishoditi certifikat kojim potvrđuje da posluje u skladu s normama, da je informacijska sigurnost provedena na najbolji mogući način što, u konačnici, povećava kredibilitet poduzeća i njegovu poziciju na tržištu. Norma ISO 27001, osim što propisuje kako organizirati informacijsku sigurnost organizacije, propisuje i pravila osiguravanja tehničke sigurnosti pristupa prostorima i podacima, upravljanje ljudskim resursima, pravnu zaštitu, klasifikaciju informacija, razmjenu informacija, zaštitu opreme, zaštitu prostora, i slično.

Poduzeća koja su u svoju poslovnu kulturu odlučila implementirati visoke standarde sigurnosti informacijskih sustava uspostavit će kontrole prijave i odjave svojih korisnika, napravit će distinkciju između krajnjih korisnika sustava, povlaštenih korisnika i administratora i redovito će revidirati ovlaštenja svojih korisnika. Dodatno, bilježit će sve zapise korisnika koji su radili na sustavima na način da se točno zna tko je i kada izvršio koju operaciju, transakciju ili zapis. Ozbiljan proces upravljanja korisničkim računima i korisničkim pravima jedna je od zahtjevnih, ali vrlo učinkovitih i svrsishodnih procesa i to je jedan od učinkovitih načina kvalitetnog upravljanja sustavima.

[20] Zakon o informacijskoj sigurnosti, NN 79/07
[21] ISO 27001:2013, Information security management

Kako bi upravljanje informacijskom sigurnošću bilo učinkovito, sustav upravljanja sastoji se od četiri faze koje se ciklički ponavljaju, a to su:

- Planiranje (podrazumijeva definiranje politika upravljanja informacijskom sigurnošću, opseg zaštite, odabir metodologije za procjenu rizika, analizu rizika, identifikaciju resursa i prijetnji, analizu ranjivosti sustava, …)
- Implementacija (podrazumijeva izradu plana postupanja s rizicima, implementaciju potrebnih mjera za ublažavanje rizika, procjenu i preispitivanje učinkovitosti mjera obrane ili ublažavanja rizika, senzibilizaciju i edukaciju djelatnika, provedbu procedura za upravljanje incidentima…)
- Nadzor (podrazumijeva provedbu uspostavljenih procedura, procjenu učinkovitosti upravljanja procesima informacijske sigurnosti, procjenu točnosti i sveobuhvatnosti prethodno identificiranih rizika, vođenje evidencija o rizicima, ažuriranje sigurnosnih planova…)
- Održavanje i poboljšavanje (podrazumijeva kontinuirano poboljšavanje postavljenih procedura s ciljem unaprjeđivanja sustava informacijske sigurnosti, provođenje korektivnih mjera…)

Virusi i sav ostali maliciozni kod predstavljaju veliku prijetnju informacijskoj sigurnosti i mogu rezultirati gubitkom povjerljivosti, cjelovitosti i raspoloživosti informacija i aplikacija.

Poduzeća trebaju donijeti politike vezane uz potrebne mjere zaštite odnosno minimalan skup pravila koje je potrebno provoditi kako bi se ostvarila adekvatna zaštita od malicioznog koda. Maliciozni kod predstavlja zlćudni kod odnosno softver koji je razvijen s namjerom narušavanja sigurnosti informacija: računalni virusi, mrežni crvi, trojanski konji, logičke bombe, spyware, adware… U cilju zaštite od malicioznog koda, poduzeća trebaju osigurati zaštitne programe za pravovremeno otkrivanje, sprječavanje i oporavak od zlćudnog koda.

Kvalitetan program za zaštitu od malicioznog koda treba omogućavati detekciju i uklanjanje zlćudnog koda te izradu zapisa o svim događajima, takav program treba biti stalno aktivan i ažuran, zaštićen od deaktivacije od strane korisnika.

Zaštitu od malicioznih kodova potrebno je postaviti na sve informacijske sustave poduzeća, „core“ aplikacije kojima se koriste ovlašteni korisnici poduzeća, ali i na aplikacije kojima se koriste ostali vanjski korisnici (poput internetskog bankarstva, mobilnog bankarstva, web stranica).

U svrhu zaštite informacijskog sustava i svih informacija koje on sadrži potrebno je, osim tehničkih mjera zaštite, provoditi i kontinuiranu poduku korisnika na način da se stvori „kultura opreza“. Ona podrazumijeva edukaciju o sigurnom korištenju informacijskih sustava i opreme.

Većina autora smatra da se svaka poduka sastoji od 4 faze a to su: identifikacija potrebe za podukom, planiranje poduke, izvođenje poduke i evaluacija provedene poduke.[22]

[22] Buble M., Osnove menadžmenta, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2006., str. 275.

9. Svijest o sigurnosti

Svijest o sigurnosti (Security awareness) važna je tema kada se govori o korporativnoj sigurnosti. Podizanje svijesti o korporativnoj, a posebice o informacijskoj sigurnosti jedan je od izazovnijih zadataka za sva poduzeća koja vode računa o razini informacijske sigurnosti.

Kako bi se postigla učinkovitost edukacije važno je edukativne materijale kvalitetno osmisliti, na način da oni budu prilagođeni svim zaposlenicima u poduzeću. Osim što edukacije moraju biti osmišljene na način da zainteresiraju i senzibiliziraju zaposlenike, dodatni izazov predstavlja činjenica da redovito provođenje ovakvih edukacija zahtjeva dosta vremena.

Govoreći o podizanju svijesti o sigurnosti neizostavna je kontinuirana edukacija i podizanje svijesti o:

- važnosti pridržavanja politika i procedura poduzeća,
- sigurnosti autentifikacijskih zaporki pri korištenju informacijskih sustava,
- pridržavanju politike čistog stola i čistog monitora,
- pridržavanju politika sigurnosti prilikom ulaska u prostorije poduzeća u kojima su povjerljivi podaci, pri čemu se koriste alarmi ili identifikacijske kartice za ulazak u poslovne prostorije poduzeća,
- pridržavanju politika rukovanja s povjerljivim informacijama,
- pridržavanju pravila koja se odnose na zaštitu na radu.
- pridržavanju pravila koja se odnose na zaštitu od požara,
- pridržavanju pravila koja se odnose na zaštitu okoliša…

9.1 Politike, procedure i drugi interni akti

Kako bi poduzeće osiguralo rad u sigurnom poslovnom okruženju, ono mora donijeti vlastite interne akte kojima će opisati i definirati pravila postupanja u raznim poslovnim situacijama, a koje propisuju poslovanje na siguran način. Takvi akti trebaju biti usklađeni s relevantnim zakonima, podzakonskim aktima, slijediti odgovarajuće norme (poput ISO standarda). Kvalitetni akti također trebaju slijediti pozitivne poslovne prakse.

Poštivanje internih akata i procedura temeljna je kultura zaposlenika svakog dobro organiziranog poduzeća, stoga svako poduzeće treba osigurati kontinuiranu edukaciju svojih zaposlenika, s ciljem osvješćivanja zaposlenika o njihovoj važnosti i senzibilizaciji zaposlenika u odnosu na djelovanja koja se tiču korporativne sigurnosti, a definiraju ih razne politike, procedure i upute za rad.

9.2 Zaporke

Kada se govori o podizanju svijesti o sigurnosti, kao neizostavan pojam nameće se zaporka. To je oblik tajnog podatka koji se koristi za autentifikaciju pri kontroli prava pristupa pojedinim dijelovima informacijskog sustava.

Jednostavno rečeno, zaporka je potpis korisnika. Imajući to vidu, svaki korisnik svih vrsta aplikacija i opreme za obradu informacija mora voditi računa o njenoj sigurnosti.

Što korisnik može učiniti da poveća vlastitu sigurnost i sigurnost svoje zaporke? Još u nedavnoj prošlosti sigurnom zaporkom smatrala se ona koja ima 8 znakova (uključujući slova, brojeve i interpunkcijske znakove), danas ovo više nije dovoljno sigurna zaporka, svaki će program za probijanje zaporki uzeti ovakve kombinacije u obzir. Sigurnost zaporke povećava se povećavanjem njene duljine, jer to će broj kombinacija povećati na vrijednosti koje je teško sustići današnjim, ali i budućim računalnim tehnologijama.

Uzimajući obzir važnost zaštite zaporki svako bi poduzeće trebalo donijeti svoju politiku ili sličan dokument kojim se propisuje proces upravljanja zaporkama i način njihove uporabe u okružju informacijskog sustava. Cilj izrade takvog dokumenta je povećanje stupnja kontrole pristupa informacijama, opremi za obradu informacija i aplikacijama koje pomažu odvijanje poslovnih procesa, te osiguranje pristupa ovlaštenim korisnicima i sprječavanje neovlaštenog pristupa. Takva politika ili sličan dokument treba obuhvatiti sve zaporke koje se kreiraju za bilo koji dio informacijske imovine koja sačinjava informacijski sustav poduzeća, a koje služe za autentifikaciju svih korisnika i korisničkih računa.

Norma ISO 27001[23] opisuje kontrolu pristupa. Ona definira potrebu uspostavljanja, dokumentiranja i naknadnih kontrola pristupu informacijama, te potrebu uspostave procedura koje propisuju postupke registriranja ovlaštenih korisnika i postupanja u slučaju prestanka prava korisnicima, a sve s ciljem da se samo ovlaštenim korisnicima osigura pristup informacijskim sustavima i da se spriječi svaki neovlašten pristup. Prema navedenoj normi potrebno je dati i poštivati smjernice „dobre sigurnosne prakse“ za izradu i čuvanje zaporki.

Zaporke imaju sljedeća svojstva:

1. Dužina zaporke: određuje se minimalan broj znakova koje zaporka mora imati, što je zaporka dulja to je sigurnija,

[23] ISO 27001:2013, Information security management

2. Složenost zaporke: zaporka je složena ako sadrži barem tri od četiri grupe znakova (velika slova, mala slova, interpunkcijski i ostali specijalni znakovi),
3. Maksimalna starost zaporke: period koliko je zaporka valjana tj. do kada se može koristiti u radu,
4. Minimalna starost zaporke: minimalno vrijeme važenja zaporke (minimalno vrijeme koje mora proteći između korištenja dvije zaporke),
5. Trajanje obavijesti o prestanku važenja zaporke: period nakon kojeg zaporka prestaje važiti,
6. Povijest zaporke: koliko se zadnjih lozinki pamti tj. kada se ista zaporka smiju ponoviti,
7. Broj krivih uzastopnih pokušaja prije zaključavanja korisničkog računa: nakon kojeg broja unosa pogrešne zaporke će se korisnički račun zaključati,
8. Trajanje zaključavanja: vrijeme koliko je korisnički račun zaključan,
9. Sustav može sam promijeniti lozinku: da li je sustavu dopušteno da sam mijenja lozinku upotrebom metode pitanje – odgovor ,
10. Zaporka se može promijeniti zahtjevom službi za pomoć korisnicima: da li se zaporka može promijeniti telefonskim pozivom, elektroničkom poštom i sl.,
11. Zaporka se može osobno promijeniti: da li je korisniku ili ovlaštenom djelatniku dozvoljeno da sam mijenja lozinku ili to mora učiniti uz pomoć administratora,
12. Korisnički račun se postavlja u nevažeći ako je zaporka otkrivena: u slučaju namjernog ili nenamjernog otkrivanja zaporke, treba li se korisnički račun zaključati.
13. Korisnički račun mora koristiti dvije ili više metoda za autentifikaciju: koristi se kombinacija dvije ili više metoda autentifikacije, na primjer pin i kartica ili otisak prsta i pin),
14. Potrebno odobrenje za promjenu: da li je za promjenu zaporke potrebno nečije dodatno odobrenje.

9.3 Politika čistog stola i ekrana

Još jedan od pojmova koji zaslužuju da se o njima piše i da ga se primjenjuje u kontekstu korporativne sigurnosti je politika čistog stola i ekrana (Clear desk and clear screen).

Politika čistog stola i čistog monitora odnosi se na postupke čuvanja povjerljivih informacija, u elektronskom ili u papirnatom obliku. Ova politika također podrazumijeva zabranu ostavljanja računala otključanima čak i kada je riječ o najkraćem mogućem trajanju, jer to čini povjerljive informacije lako dostupnima, čime ih se dovodi u opasnost kompromitiranja.

Norma ISO 27001[24] govori i o temi politike čistog stola i ekrana.

Budući da su informacije jedna od najranjivijih podataka, prihvaćanje politike čistog stola i čistog ekrana jedna je od važnijih politika pri pokušaju smanjenja rizika sigurnosti. Implementacija takve politike je vrlo jednostavna i ne zahtjeva visoku tehnologiju.

U svrhu zaštite podataka na papirnatom mediju preporučljivo je korištenje zaštićenih područja popuno vatrootpornih ormara, sefova i slično. Na ovaj način provodi se, osim zaštite od neovlaštenog pristupa, zaštita od požara, vatre, poplave, eksplozije i slično.

U svrhu smanjenja rizika od neovlaštenog pristupa informacijama koje su dostupne na elektroničkim medijima, preporučljivo je da se računala i slična oprema (poput mobitela) koriste na način da se sadržaji pohranjeni na takvim medijima učine nedostupnima neovlaštenim osobama, koristeći zaporke, privremene odjave iz informacijskog sustava, zaključavanje ekrana. Dodatno se preporučuje tijekom dužeg nekorištenja elektroničke opreme istu ugasiti, kako bi se dodatno smanjio rizik od neovlaštenog korištenja.

Ispisivanje i preslikavanje dokumenata također povećava rizik neovlaštenog pristupa informacijama, posebno u poduzećima gdje više korisnika koristi iste uređaje za ispis i preslikavanje. U takvim okolnostima dodatnu je pažnju potrebno posvetiti pravodobnom uklanjanju ispisanih dokumenata s uređaja za ispis. Mnoga poduzeća su, s ciljem smanjenja rizika ove vrste, uvela dodatne kontrole na način da uređaji izvršavaju zadane ispise tek po unosu zaporke koju korisnik koji je zatražio ispis unese u uređaj za ispisivanje.

Općenito, u svrhu smanjenja rizika od neovlaštenog pristupa informacijama, te dodatno u svrhu zaštite okoliša, poduzeća trebaju razvijati kulturu minimalnog bespotrebnog ispisivanja dokumenata.

[24] Ibid.

Radi čega je toliko važno pridržavati se politike čistog stola i čistog ekrana pokazat će sljedeći primjer – pridržavanje pravila čuvanja bankarske tajne. Kako je dobro poznato, podaci o klijentima, njihovim računima stroga su poslovna tajna, posebice u bankama i financijskim institucijama. Curenje bilo kakve takve informacije značilo bi tešku povredu iz radnog odnosa i moguće vrlo oštre sankcije za prekršitelja (zaposlenika i banku). Stoga su mnoge banke uvele linije diskrecije koje označavaju prostor u koji klijenti ne trebaju ulaziti u slučajevima kada na šalteru ispred njih već klijent obavlja svoje transakcije ili poslovne razgovore. Cilj takvih linija diskrecije je osigurati zaštitu informacija o klijentima i njihovim računima ili transakcijama, na taj se način omogućava da ostali klijenti ne pristupaju dovoljno blizu kako im ne bi bili vidljivi tuđi ugovori i dokumenti koji proizlaze iz poslovanja s klijentom koji obavlja transakcije. Dodatno ekrani računala uvijek trebaju biti smješteni u prostoriji na način da je sadržaj na njima dostupan isključivo osobama (zaposlenicima) koji imaju pravo vidjeti njihov sadržaj. Nakon rada s klijentom svi dokumenti se arhiviraju neposredno po završetku rada s odnosnim klijentom kako bi se zaštitili njegovi podaci i dokumenti od pogleda ili dohvata neovlaštenih osoba.

9.4 Identifikacijske kartice

Zaposlenici mnogih poduzeća danas za ulazak u službene prostorije koriste identifikacijske kartice. Riječ je o financijski malom ulaganju uz pomoć kojeg se može postići viša razina sigurnosti. Identifikacijske kartice su još uvijek najzastupljeniji medij za identifikaciju u sustavima kao što su kontrola pristupa i evidencija radnog vremena. Osnovne prednosti identifikacijskih kartica su mogućnost personalizacije i vizualne identifikacije, a mogu se koristiti u različite svrhe, poput:

- kontrole pristupa,
- evidencije radnog vremena,
- evidencije posjetitelja.

Identifikacijske kartice su najčešće personalizirane, tada sadrže osobne podatke korisnika čime poduzeću omogućavaju točnu detekciju svih ulazaka i izlazaka u sve ili samo određene prostorije poduzeća.

10. Tehnička zaštita

Način provedbe tehničke zaštite reguliran je Pravilnikom o uvjetima i načinu provedbe tehničke zaštite prema kojemu se tehnička zaštita opisuje kao skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini kao što su: protuprovalno djelovanje, protuprepadno djelovanje i protusabotažno djelovanje[25].

Sredstva tehničke zaštite koriste se u svrhu sprječavanja nedopuštenog pristupa u štićeni objekt ili u svrhu zaštite štićenih osoba. Sredstvima tehničke zaštite smatraju se specijalne ograde, rampe, protuprovalna vrata, neprobojna stakla, sefovi, trezori, uređaji za detekciju metalnih predmeta, rendgenski uređaji, protuprovalni sustavi, dojavni sustavi, sustavi registracije prolaza, sustavi za neposrednu zaštitu ljudi, ručna ogledala za pregled podvozja vozila…

Osiguravanju objekata prethodi prosudba ugroženosti. Ona se izrađuje se na temelju podataka o vrsti, namjeni, veličini i lokaciji objekta, vrsti o broju korisnika, načinu korištenja objekta, opremi i dokumentima koji će se u objektu nalaziti te o mogućnosti rizika od njihova oštećenja, krađe ili uništenja. [26]

Na temelju prosudbe ugroženosti izrađuje se sigurnosni elaborat kojim se određuje optimalna razina tehničke zaštite. Sigurnosni elaborat sadrži podatke o tome što moraju ispunjavati sustavi koji nisu sustavi tehničke zaštite ali na njih utječu (poput napajanja električnom energijom). Sigurnosni elaborat definira građevne i slične uvjete koji su važni za ispravno funkcioniranje sustava tehničke zaštite.[27]

Temeljem sigurnosnog elaborata izrađuje se projektni zadatak kojim se određuje vrsta tehničke zaštite, smještaj centra tehničke zaštite, uređaja i opreme, definira se način polaganja instalacija, i slično. Projektnu dokumentaciju smiju izrađivati samo osobe registrirane za obavljanje takve vrste poslova, a njihov je rad reguliran Zakonom o privatnoj zaštiti.[28]

[25] Pravilnik o uvjetima i načinu provedbe tehničke zaštite, NN 198/2003
[26] Ibid., članak 6
[27] Ibid., članak 7
[28] Zakon o privatnoj zaštiti, NN 68/03, 31/10, 139/10

11. Fizička zaštita

Kako bi poduzeća bila spremna odgovoriti na prijetnje i izazove s kojima se može suočiti u redovnom radu, trebaju razmotriti i potrebu za implementacijom procesa fizičke sigurnosti i sigurnosti okruženja.

Politiku fizičke sigurnosti i sigurnosti poslovnog okruženja obrađuje norma ISO 27001.[29]

Norma definira kontrole koje je potrebno postaviti s ciljem prevencije neovlaštenog pristupa, oštećenja i ometanja prostora i informacija koje čine imovinu poduzeća, te sprječavanje gubitka, oštećenja, krađe ili ugrožavanja imovine te prekida aktivnosti poduzeća.

Osigurati sigurno okruženje znači uspostaviti:

- granice fizičkog sigurnosnog prostora,
- fizičke kontrole pristupa (primjer: ulazi koje otključavaju personalizirane kartice, recepcija na ulaz u prostor u kojemu se nalaze informacije i slično, odvojen prostor u koji je zabranjen ulazak neovlaštenim osobama),
- fizičko osiguranje ureda i prostorija i zaštita od negativnih vanjskih utjecaja i opasnosti (primjer: zaštita od požara, poplave, potresa, eksplozija, građanskih nemira…),
- zaštitu opreme od neovlaštenog pristupa, negativnih vanjskih utjecaja i opasnosti s ciljem smanjenja opasnosti (promjer: opremu treba zaštiti od prestanka napajanja strujom, prekida uzrokovanih zasojima u pratećim uslugama i opremi…)
- proces ispravnog načina kontrole i održavanja opreme.

Ovisno o tome kakvom se djelatnošću poduzeće bavi, implementirat će različita pravila pristupa određenim dijelovima svojih poslovnih prostorija, pa će, na primjer, u određene poslovne prostorije poduzeća biti dopušten ulazak klijentima, dok u određene prostorije neće biti dopušten ulazak neovlaštenim osobama ili će pristup biti dopušten samo određenim zaposlenicima poduzeća.

Uzmimo na primjer fizičku zaštitu sefa u trezorima banaka. Trezori su je posebna prostorija u bankama i drugim institucijama s kasama i sefovima, koji su namijenjeni čuvanju novca i drugih vrijednosti. Uvijek su u poslovnim prostorijama smješteni na način da nisu dostupni pogledima klijenata, osigurani su posebnim ulaznim šiframa s dualnim bravama/šiframa (trezore ili sefove mogu otključati isključivo dva zaposlenika koristeći svatko svoju šifru, tek

[29] ISO 27001:2013, Information security management

kombinacija dviju točnih šifri otključava trezor). Sefovi nerijetko prema standardima i prema dobroj poslovnoj praksi imaju ugrađeno vremensko kašnjenje prilikom otključavanja (nakon unosa šifri treba proteći određeni rok da se trezor može otvoriti), što je još jedan sigurnosni alat koji ima za cilj smanjenje rizika od interne pronevjere ili pljačke. Postojanje dualnih brava smanjuje rizik od interne prijevare obzirom da niti jedan zaposlenik koji je ovlašten ulaziti u trezor ne može samostalno otvoriti ga, a to znači da je za internu pronevjeru potrebno udruživanje dva ili više zaposlenika, čime je rizik od prijevare značajno smanjen u odnosu na situaciju kada samo jedan zaposlenik može samostalno otključati trezor. Vremensko kašnjenje na trezorima jedan je od način zaštite od pljačke. Podatak o postojanju trezora koji se otključavaju s vremenskim kašnjenjem u svakoj je financijskog instituciji vidljiv je na samim ulaznim vratima (informativna naljepnica – poruka), a to je također jedan način odvraćanja zlonamjernika od počinjenja pljačke ili razbojstva.

12. Zaštita na radu

U Republici Hrvatskoj područje zaštite na radu regulira Zakon o zaštiti na radu, koji u pravni poredak Republike Hrvatske implementira mnoge direktive Europske unije, a donosi opća načela prevencije i zaštite na radu, prava i obveze radnika, obveze poslodavaca. Zakon regulira djelatnosti koje su u svezi sa zaštitom na radu i prekršajne odredbe u slučaju nepridržavanja odredbi Zakona. Svrha Zakona o zaštiti na radu je unaprjeđenje zaštite zdravlja radnika, sprečavanje ozljeda, profesionalnih bolesti i slično. Sve pravne osobe koje zapošljavaju radnike obveznici su ovog Zakona, bez obzira na djelatnost kojom se bave.

Zaštita na radu obuhvaća:

- pravila pri projektiranju i izradi sredstava rada,
- pravila pri uporabi, održavanju, pregledu i ispitivanju sredstava rada,
- pravila koja se odnose na radnike te prilagodbu procesa rada njihovom spolu, dobi, fizičkim, tjelesnim i psihičkim sposobnostima,
- načine i postupke osposobljavanja i obavješćivanja radnika i poslodavaca sa svrhom postizanja odgovarajuće razine zaštite na radu,
- načine i postupke suradnje poslodavca, radnika i njihovih predstavnika i udruga te državnih ustanova i tijela nadležnih za zaštitu na radu
- zabranu stavljanja radnika u nepovoljniji položaj zbog aktivnosti poduzetih radi zaštite na radu,
- ostale mjere za sprječavanje rizika na radu, sa svrhom uklanjanja čimbenika rizika i njihovih štetnih posljedica.[30]

Zaštita na radu mora se provoditi temeljem načela izbjegavanja, procjene i sprječavanja rizika, prilagođavanja rada radnicima (u smislu oblikovanja radnih mjesta, odabirom radne opreme…), prilagođavanja tehničkom napretku, zamjene opasnog onim manje opasnim ili neopasnim, odgovarajućeg osposobljavanja radnika za rad na siguran način, besplatnosti mjera zaštite na radu.

Sredstvo rada kada je u uporabi mora zadovoljavati sljedeće uvjete zaštite

- zaštitu od mehaničkih opasnosti
- zaštitu od udara električne struje
- sprječavanje nastanka požara i eksplozije
- osiguranje mehaničke otpornosti i stabilnosti građevine

[30] Zakon o zaštiti na radu, pročišćeni tekst zakona, NN 71/14, 118/14, 154/14, članak 10, stavak 1

- osiguranje potrebne radne površine i radnog prostora
- osiguranje potrebnih putova za prolaz, prijevoz i evakuaciju radnika i drugih osoba
- osiguranje čistoće
- osiguranje propisane temperature i vlažnosti zraka i ograničenja brzine strujanja zraka
- osiguranje propisane rasvjete
- zaštitu od buke i vibracija
- zaštitu od štetnih atmosferskih i klimatskih utjecaja
- zaštitu od fizikalnih, kemijskih i bioloških štetnih djelovanja
- zaštitu od prekomjernih napora
- zaštitu od elektromagnetskog i ostalog zračenja
- osiguranje prostorija i uređaja za osobnu higijenu[31].

Poduzeća su dužna organizirati i provoditi zaštitu na radu na način da zaposlenicima osigura najveću moguću razinu zaštite na radu, uvažavajući prirodu posla kojim se radnik bavi, uvijek vodeći računa da na najbolji mogući način smanji izloženost radnika opasnostima i štetnostima. Svako poduzeće mora imati izrađenu procjenu rizika, a temeljem te procjene primjenjivati pravila zaštite na radu, preventivne mjere i radnje s ciljem smanjenja rizika i svođenja opasnosti od ozljeda i profesionalnih oboljenja na najmanju moguću mjeru. Poduzeća su dužna prije početka rada osposobiti radnika za rad na siguran način, ukoliko radnik prije početka rada nije osposobljen za rad na siguran način, najduže 60 dana smije raditi pod neposrednim nadzorom radnika osposobljenog za rad na siguran način, ali ne dulje od 60 dana. Jednako tako, poduzeća su dužna provesti postupak osposobljavanja za rad na siguran način u slučaju promjena u radnim postupcima, kod uvođenja nove opreme ili njezinih značajnih promjena, kod uvođenja novih tehnologija, kada se radnika premješta na novo radno mjesto, kod utvrđenog narušavanja zdravlja zaposlenika uzrokovanog opasnostima ili štetnostima vezanim uz njegovo mjesto rada.

Poduzeća su dužna, u smislu zaštite na radu, posebnog računa voditi o posebno osjetljivoj skupini zaposlenika i to maloljetnih radnika, trudnica, zaposlenica koje su nedavno rodile, zaposlenica koje doje, zaposlenika oboljelih od profesionalne bolesti te zaposlenika kod kojih je utvrđena smanjena radna sposobnost ili postoji neposredni rizik od smanjenja radne sposobnosti.

[31] Ibid., članak 12, stavak 1

13. Zaštita od požara

U Republici Hrvatskoj sustav zaštite od požara reguliran je Zakonom o zaštiti od požara[32].

Sustav zaštite od požara podrazumijeva planiranje zaštite od požara, propisivanje mjera zaštite od požara građevina, ustrojavanje subjekata zaštite od požara, provođenje mjera zaštite od požara, financiranje zaštite od požara te osposobljavanje i ovlašćivanje za obavljanje poslova zaštite od požara, s ciljem zaštite života, zdravlja i sigurnosti ljudi i životinja te sigurnosti materijalnih dobara, okoliša i prirode od požara, uz društveno i gospodarski prihvatljiv požarni rizik.[33]

S ciljem zaštite od požara važno je kontinuirano poduzimati mjere i radnje vezane uz otklanjanje opasnosti od nastanka požara, rano otkrivanje požara, obavješćivanje u slučaju nastanka požara, sprječavanje širenja i učinkovito gašenje požara, sigurno spašavanje ljudi i životinja u područjima ugroženima požarom. Cilj je u što većoj mjeri smanjiti štetne posljedice požara. Od velike je važnosti utvrđivanje uzroka nastanka požara, kako bi se lakše preveniralo u budućnosti.[34]

Sve su fizičke i pravne osobe dužne djelovati na način kojim se ne može izazvati požar i provoditi mjere zaštite od požara.

Svi vlasnici i korisnici građevina i drugih nekretnina dužni su osigurati provedbu mjera zaštite od požara i poduzimati mjere za smanjenje opasnosti od požara.

Poduzeća su dužna osigurati osposobljavanje zaposlenika za:

- provedbu preventivnih mjera zaštite od požara,
- gašenje početnih požara,
- spašavanje ljudi i imovine ugroženih požarom.

Poduzeća su o prethodno navedenim osposobljavanjima dužna voditi evidenciju.[35]

[32] Zakon o zaštiti od požara, NN 92/10
[33] Ibid., članak 1, stavak 2
[34] Ibid., članak 1, stavak 3
[35] Ibid., članak 16

14. Sigurnost kadrova

Ljudski resursi čine živi faktor organizacije poduzeća, koji svojim radom, znanjem, vještinama, sposobnošću i kreativnošću najviše doprinosi uspješnom ostvarivanju ciljeva poduzeća. Nazivaju se još i „ljudskim kapitalom“.[36]

Upravo radi značaja i važnosti tog „ljudskog kapitala“ prilikom provedbe procesa zapošljavanja valja voditi računa da potencijalni kandidat svojim karakteristikama i osobinama odgovara uvjetima koje zahtjeva radno mjesto za koje je kandidat aplicirao.

Cilj svakog poslodavca je zaposliti što bolje kadrove za svako radno mjesto, u okviru svojih financijskih i drugih mogućnosti, uz što manji rizik da će zaposlenici tijekom svog rada posegnuti za krađom, prijevarom ili bilo kojim drugim oblikom zlouporabe. Da bi se odabrao kvalitetan kandidat, potrebno ga je dobro procijeniti.

Kandidata se procjenjuje kroz razne psiho testove, testove osobnosti i testove znanja. Dodatno se od kandidata zahtjeva da novom poslodavcu predoči potvrdu o nekažnjavanju. U nekim poduzećima se za određena radna mjesta potvrda o nekažnjavanju traži redovito (na primjer u bankama, za visoke upravljačke funkcije prilikom procjene primjerenosti potvrda o nekažnjavanju traži se svake godine).

Pisma preporuka izrađena od strane prethodnih poslodavaca jedan su od dobrih alata sigurnosne i kvalitativne provjere potencijalnih kandidata prilikom zapošljavanja.

Svako poduzeće treba osigurati da svi zaposlenici razumiju svoje odgovornosti. S tim ciljem poduzeće izrađuje za svako radno mjesto dokument kojim jasno definira opis posla. Riječ je o sistemskom evidentiranju svih poslova koji se obavljaju na pojedinim radnim mjestima. Osim toga u istom je dokumentu nerijetko sadržana i specifikacija posla, kojom su definirane posebne kvalifikacije i radno iskustvo potrebno za obavljanje određenog posla.[37]

Poduzeće koje kvalitetno upravlja svojim zaposlenicima istima postavlja ciljeve, evaluira ih, procjenjuje razloge uspješnosti ili neuspješnosti zaposlenika i na kraju ih na razne načine stimulira ili destimulira.

Kada je riječ o kadrovskoj politici važno je da svako poduzeće procijeni svoje ključne funkcije i zaposlenike, poduzeće koje na kvalitetan način vodi računa o svom imidžu i poslovnim rezultatima ne bi smjelo svoje poslovanje organizirati da ovisi o pojedincu. Uvijek

[36] Bahtijarević-Šiber F., Management ljudskih potencijala, Golden marketing, Zagreb, 1999., str. 25.
[37] Buble M., Osnove menadžmenta, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2006, str. 255.

je korisno ići s pretpostavkom da će pojedinac iz bilo kojeg razloga napustiti poduzeće, a da ono u tim uvjetima mora nastaviti s normalnim radom uz minimalni stres.

Govoreći o prestanku ugovora o radu (i njegovih inačica), poduzeća trebaju uspostaviti mehanizme koji će, u slučaju odlaska radnika iz poduzeća, osigurati jasne uvjete prekida ugovara na korist obiju ugovornih strana. Svako razilaženje u očekivanjima i zahtjevima može predstavljati rizik od pravnih sporova iz okvira radnog prava (i drugih prava), a u tom slučaju poduzeću potencijalno donijeti i gubitke.

15. Sprečavanje pranja novca i financiranje terorizma

Zakon o sprječavanju pranja novca i financiranja terorizma[38] (dalje u tekstu: ZSPN i FT) zakon je koji regulira mjere i postupke koje su obveznici dužni provoditi u svrhu sprječavanja i otkrivanja pranja novca i financiranja terorizma.

ZSPN i FT propisuje preventivne mjere koje obveznici i nadležna državna tijela moraju provoditi u svrhu praćenja transakcija i računa fizičkih i pravnih osoba, kako bi se pravodobno otkrile radnje koje upućuju na pranje novca i/ili financiranje terorizma.

Ovim Zakonom su u pravni poredak Republike Hrvatske implementirane razne direktive i uredbe Europske unije.[39]

Pranjem novca podrazumijeva se:

- zamjena ili prijenos imovine, kada se zna da je ta imovina stečena kriminalnom aktivnošću ili sudjelovanjem u takvoj aktivnosti, u svrhu skrivanja ili prikrivanja nezakonitoga podrijetla imovine ili pomaganja bilo kojoj osobi koja je uključena u počinjenje takve aktivnosti u izbjegavanju pravnih posljedica djelovanja te osobe
- skrivanje ili prikrivanje prave prirode, izvora, lokacije, raspolaganja, kretanja, prava povezanih s vlasništvom ili vlasništva imovine, kada se zna da je ta imovina stečena kriminalnom aktivnošću ili sudjelovanjem u takvoj aktivnosti
- stjecanje, posjedovanje ili korištenje imovine ako se zna, u vrijeme primitka, da je ta imovina stečena kriminalnom aktivnošću ili sudjelovanjem u takvoj aktivnosti ili
- sudjelovanje u počinjenju, udruživanje radi počinjenja, pokušaj počinjenja i pomaganja u počinjenju, poticanje, savjetovanje i olakšavanje ostvarenja bilo koje od aktivnosti navedene u točkama 1., 2. i 3. ovoga stavka.
- aktivnosti kojima je stvorena imovina koja je predmet pranja novca provedene na državnome području druge države članice ili treće zemlje.[40]

Financiranjem terorizma smatra se prikupljanje sredstava ili pokušaj pribavljanja sredstava s namjerom da se upotrijebe od strane terorista ili terorističke organizacije u bilo koju svrhu.[41]

[38] Zakon o sprječavanju pranja novca i financiranja terorizma, NN 108/17
[39] Ibid., članak 2
[40] Ibid., članak 3, stavak 1 i 2
[41] Ibid., članak 3, stavak 3

„Obveznici ZSPN i FT:

- kreditne institucije
- kreditne unije
- Hrvatska banka za obnovu i razvitak
- HP – Hrvatska pošta d. d. u dijelu poslovanja koji se odnosi na poštanske novčane uputnice
- institucije za platni promet
- društva za upravljanje investicijskim fondovima i investicijski fondovi s pravnom osobnošću s unutarnjim upravljanjem
- mirovinska društva u dijelu poslovanja koje se odnosi na dobrovoljne mirovinske fondove te mirovinska osiguravajuća društva u dijelu poslovanja koji se odnosi na izravne jednokratne uplate osoba u takva društva i društva za dokup mirovine
- društva ovlaštena za pružanje investicijskih usluga i obavljanje investicijskih aktivnosti
- društva za osiguranje koja imaju odobrenje za obavljanje poslova životnih osiguranja i drugih osiguranja povezanih s ulaganjima
- pravne i fizičke osobe koje se bave djelatnošću zastupanja u osiguranju pri sklapanju ugovora o životnome osiguranju i drugih osiguranja povezanih s ulaganjima
- pravne i fizičke osobe koje se bave djelatnošću posredovanja u osiguranju pri sklapanju ugovora o životnome osiguranju i drugih osiguranja povezanih s ulaganjima
- faktoring-društva
- leasing-društva
- institucije za elektronički novac
- ovlašteni mjenjači
- priređivači igara na sreću za: lutrijske igre, igre u kasinima, igre klađenja, igre na sreću na automatima, igranje na daljinu preko interneta, telefona ili drugih interaktivnih komunikacijskih uređaja (online igranje)
- pravne i fizičke osobe koje se bave djelatnošću: odobravanja kredita i zajmova, uključujući potrošačke kredite, ako je to dopušteno posebnim zakonom, i financiranje komercijalnih poslova, uključujući izvozno financiranje na osnovi otkupa s diskontom i bez regresa dugoročnih nedospjelih potraživanja osiguranih financijskim instrumentima (engl. forfeiting), uključujući i otkup dospjelih potraživanja, izdavanja ostalih sredstava plaćanja i upravljanja njima (putnički čekovi i bankovne mjenice),

ako ta djelatnost nije platna usluga u smislu zakona kojim se uređuje platni promet, izdavanja garancija i jamstava, upravljanja ulaganjima za treće osobe i savjetovanja u vezi s tim, iznajmljivanja sefova, pružanja usluga povezanih s trustovima ili trgovačkim društvima, prometa plemenitih metala i dragoga kamenja, trgovine umjetničkim predmetima i antikvitetima, organiziranja ili provođenja dražbi, posredovanja u prometu nekretninama

- pravne i fizičke osobe u obavljanju profesionalnih djelatnosti: revizorsko društvo, samostalni revizor, vanjski računovođa koji je fizička ili pravna osoba koja obavlja računovodstvene usluge, porezni savjetnik, društvo za porezno savjetništvo, odvjetnik, odvjetničko društvo, javni bilježnik (ako sudjeluje, bilo da djeluje uime svoje stranke bilo za svoju stranku, u bilo kojoj vrsti financijskih transakcija ili transakcija koje uključuju nekretnine ili pak pružaju pomoć u planiranju ili provođenju transakcije za svoju stranku u vezi s:
    - kupnjom ili prodajom nekretnina ili poslovnih subjekata,
    - upravljanjem novčanim sredstvima, vrijednosnim papirima ili drugom imovinom u vlasništvu stranke,
    - otvaranjem i upravljanjem bankovnih računa, štednih uloga ili računa za poslovanje s financijskim instrumentima,
    - prikupljanjem sredstava potrebnih za osnivanje, poslovanje ili upravljanje trgovačkim društvom,
    - osnivanjem, poslovanjem ili upravljanjem trustovima, trgovačkim društvima, zakladama ili sličnim pravnim uređenjima.“[42]

Slijedom prethodno navedenog popisa obveznika ZSPN i FT vidljivo je da je ova tema obvezujuća za mnoga poduzeća, a ovisno o djelatnosti kojom se ona bave.

Poduzeća obveznici ovog Zakona dužni su izraditi vlastite politike i procedure u kojima će biti opisani postupci koji se provode s ciljem sprječavanja pranja novca i financiranja terorizma.

[42] Ibid., članak 9, stavak 2 i 3

15.1 Dubinska analiza

Dubinska analiza stranke podrazumijeva identifikaciju stranke temeljem identifikacijskog dokumenta, utvrđivanje identiteta stvarnog vlasnika stranke (poslovnog subjekta), prikupljanje podataka o namjeni i prirodi poslovnog odnosa kojeg namjerava sklopiti s obveznikom, stalno praćenje poslovnog odnosa i kontrolu transakcija koje se obavljaju, podatke o izvoru sredstava klijenta. Primjena potrebnih mjera dubinske analize ovisi o procjeni rizika pojedinog klijenta.[43]

Dubinska analiza klijenta provodi se

- prilikom uspostavljanja poslovnoga odnosa,
- prilikom provođenja jedne ili više povezanih transakcija u vrijednosti 105.000,00 kuna i većoj,
- prilikom provođenja jedne ili više povezanih transakcija i protuvrijednosti 1.000 EUR,
- prilikom jedne ili više povezanih transakcija proizišlih iz igara na sreću u vrijednosti 15.000 HRK,
- kada postoji sumnja u vjerodostojnost prethodno dobivenih podataka o klijentu,
- uvijek kada u vezi s transakcijom ili strankom postoje razlozi za sumnju na pranje novca ili financiranje terorizma, bez obzira na vrijednost transakcije.[44]

U slučaju da nije moguće provesti dubinsku analizu klijenta, obveznik je dužan prekinuti prethodno uspostavljeni poslovni odnos ili odbiti sklopiti poslovni odnos. [45]

ZSPN i FT detaljno su definirani obvezni podaci i dokumentacija potrebna za provođenje dubinske analize za pojedinu vrstu poslovnog odnosa ili provođenja transakcija.

Dubinska analiza klijenta može biti:[46]

- pojednostavljena (smanjen opseg potrebnih podataka, manje učestalo ažuriranje podataka o klijentu,…),
- pojačana (veći opseg potrebnih podataka, češće ažuriranje podataka o klijentu i njegovom poslovanju…).

[43] Ibid., članak 15. stavak 1, članak 16. stavak 1, članak 17
[44] Ibid., članak 16, stavak 1
[45] Ibid., članak 19, stavak 1 i 2
[46] Ibid., članak 43 i 44

15.2 Stalno praćenje poslovnog odnosa

Osim prethodno navedenih mjera provođenja dubinske analize, obveznici su dužni provoditi stalno praćenje poslovnog odnosa sa klijentima.

Stalno praćenje poslovnog odnosa podrazumijeva praćenje poslovne aktivnosti i transakcija koje klijent obavlja kod obveznika, uključujući, kada je to potrebno, i poznavanje izvora sredstava, primjenjujući najmanje sljedeće mjere:

- praćenje usklađenosti stvarnog poslovanja s predviđenom prirodom poslovnog odnosa i transakcija,
- praćenje usklađenosti izvora sredstava s onim što je klijent naveo kao moguće izvore priliko uspostave poslovnog odnosa ili provođenja transakcija
- praćenje usklađenosti poslovanja i transakcija stranke s klijentovim uobičajenim opsegom poslovanja i uobičajenim transakcijama i
- redovito ažuriranje dokumentacije o klijentu, stvarnom vlasniku klijenta (poslovnom subjektu), političkoj izloženosti klijenta i profilu klijentove rizičnosti [47]

15.3 Ured za sprječavanje pranja novca

Obveznik je dužan obavijestiti Ured za sprječavanje pranja novca o:

- namjeri, planiranju ili pokušaju obavljanja sumnjive transakcije (bez obzira na njenu vrijednost kada transakcija upućuje na sumnju na pranje novca ili financiranje terorizma,
- svakoj transakciji ili više povezanih u vrijednosti 200.000 HRK i više.

15.4 Ovlaštene osobe

Obveznik je dužan imenovati osobu ovlaštenu za sprječavanje pranja novca i financiranja terorizma. ZSPN i FT detaljno propisuje uvjete koju ovlaštena osoba i zamjenik ovlaštene osobe moraju zadovoljavati. Zakon također detaljno propisuje obveze i odgovornosti koje proizlaze iz obavljanja poslova ovlaštene osobe ili njenog zamjenika.[48]

[47] Ibid., članak 15, stavak 1
[48] Ibid., članak 70

16. Upravljanje kontinuitetom poslovanja

Upravljanje kontinuitetom poslovanja (Business Continuity Management; dalje u tekstu: BCM) je proces stvaranja sustava prevencije i oporavka u slučaju nastanka krizne situacije u nekom poduzeću. BCM je proces izrade i održavanja logističkog plana koji daje smjernice kako izbjeći neželjene događaje, ublažiti posljedice takvih događaja i što brže se od istih oporaviti, ukoliko do njih dođe.

BCM je proces upravljanja u kriznim i hitnim situacijama, a obuhvaća upravljanje posljedicama realiziranih rizika, te predlaže mjere i aktivnosti za minimaliziranje potencijalne štete u slučaju incidenta te minimaliziranja negativnih učinka na daljnje poslovanje.

Incident je jedan ili više vezanih, neplaniranih, neželjenih ili neočekivanih događaja koji mogu narušiti sigurnost i funkcionalnost bilo kojeg resursa neophodnog za odvijanje važnih poslovnih procesa.

Cilj upravljanja incidentima je:

- pravovremen i učinkovit odgovor na incidente radi ograničavanja njegova utjecaja na poslovanje poduzeća,
- što brži oporavak u skladu s planom oporavka i ciljanim vremenom oporavka,
- sprječavanje ponavljanja incidenata koji su se već jednom dogodili,
- implementacija sigurnosnih kontrola s ciljem sprječavanja odnosno smanjivanja vjerojatnosti pojave incidenata.

Upravljanje kontinuitetom poslovanja kreće od pretpostavke da će se katastrofa sigurno dogoditi u nekom trenutku i priprema planove za osiguranje kontinuiteta, nastavka poslovanja.

Radi se o nizu procesa koji identificiraju potencijalne prijetnje (iz gotovo svih prethodno obrađenih područja) i osiguravaju unaprijed osmišljen okvir za pravodobnu i učinkovitu reakciju. U nekim poduzećima ni najmanji prekid normalnog rada nije prihvatljiv, stoga je pravodobna i brza sanacija izuzetno važna.

Uzmimo za primjer neku veliku banku sa sjedištem u Zagrebu. Serveri na kojima se obrađuju svi podaci su smješteni u Zagrebu. Grad pogađa razorni potres i to upravo na datum isplate mirovina. Nekoliko desetaka tisuća klijenata taj dan treba podići mirovinu, a banka ne radi. Kako bi osigurala nastavak poslovanja i posljedice nastale katastrofe svela na najmanje razmjere, banka pokreće svoje rezervne servere na drugoj lokaciji, u Zadru. Nakon nekoliko sati sve ostale poslovnice banke i svi ostali bankomati koji se nalaze na lokacijama koje nisu

zahvaćene katastrofom nastavljaju s normalnim radom i veći dio klijenata može podići svoje mirovine.

Postoje djelatnosti (na primjer bolnice) kojima ni najmanji prekid normalnog kontinuiranog rada nije prihvatljiv te je sanacija štete dugotrajna i često s neizvjesnim ishodom i katastrofalnim posljedicama. Posebice u takvim djelatnostima izuzetno je važno da je poduzeće spremno i uvježbano za reakciju na takve situacije. U slučaju kada u poduzeću, državnoj instituciji ili bilo kojoj drugoj ustanovi incident preraste u katastrofu, potrebno je pokrenuti postupak za ponovnu uspostavu elementarnih poslovnih procesa.

Norma ISO 22301:2012[49] govori o procesima BCM-a. Također i norma ISO 27001[50] u jednom poglavlju definira potrebu za upravljanjem kontinuitetom poslovanja. Uz to, nikada se ne smije zanemariti važnost identifikacije i upravljanja rizicima, što je pretpostavka da se na njih osigura pravodobna reakcija i osigura kontinuitet poslovanja.

[49] ISO 22301:2012 Societal security - Business continuity management systems - Requirements
[50] ISO 27001:2013, Information security management

17. Suradnja s kontrolnim funkcijama

Govoreći o korporativnoj sigurnosti neizostavno je naglasiti njezinu povezanost s kontrolnim funkcijama. One se razlikuju od poduzeća do poduzeća ovisno o tome kakva je priroda posla s kojim se poduzeće bavi.

U nastavku su opisane dvije kontrole funkcije koje su prisutne u gotovo svim poduzećima:

- Funkcija zadužena za usklađenost s propisima (engl. Compliance). Funkcija zadužena za usklađenost s propisima osigurava poslovanje poduzeća u skladu sa svim relevantnim propisima koje se na poslovanje poduzeća odnose. Ona se često naziva čuvarom reputacije i ugleda poduzeća.
- Funkcija zadužena za provođenje internih kontrola (engl. Internal audit). Cilj ove kontrolne funkcije je kontrola poslovanja zaposlenika u skladu s internim aktima poduzeća i u skladu sa zakonima, kontrola ispravnosti poslovnih izvješća, zaštita imovine poduzeća, preventivno djelovanje i sprječavanje prijevara i pogrešaka, otkrivanje prijevarnih radnji i pogrešaka, predlaganje mjera za poboljšanje i slično.

Osim interne revizije valja spomenuti i eksternu reviziju. Eksternu reviziju provode ovlašteni revizori koji svoju licencu i reputaciju čuvaju temeljitim i objektivnim pregledima, njihova je uloga da kontroliraju rad poduzeća, verificiraju točnost financijskih izvještaja koji se koriste za izvješćivanje države, vlasnika i ostalih zainteresiranih dionika.[51]

[51] Buble M., Osnove menadžmenta, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2006, str. 428.

18. Zaključak

Ovim radom prikazana je važnost korporativne sigurnosti u svim poduzećima, bez obzira na njihovu veličinu, teritorijalnu rasprostranjenost njegovih organizacijskih jedinica i djelatnost kojom se poduzeće bavi.

Rad kroz više poglavlja opisuje najvažnije komponente korporativne sigurnosti.

Početak rada obrađuje pitanje kreiranja sigurnosne strategije i pojašnjava kako organizirati poslovne procese i funkcije zadužene za uspostavu sigurnog poslovnog okruženja. Prikazani su neki od mogućih organizacijskih rješenja prikladnih za velika i mala poduzeća.

U nastavku rada velika je važnost posvećena temi rizika, a tema rizika i raznih pristupa rizicima može se pronaći u gotovo svakom poglavlju ovog rada. Tema rizika neodvojiva je od teme korporativne sigurnosti. Rizike je važno kontinuirano identificirati i njima upravljati. Pravodobnom reakcijom na nastale rizike smanjuje se mogućnost štetnih, čak i katastrofalnih utjecaja na poduzeće. Obrađene su neke od najzastupljenijih vrsta rizika poput strateških, financijskih, operativnih, poslovnih i sl. Rizici su uvijek prisutni i potencijalno se uvijek mogu dogoditi. Samo njihovim pravodobnim predviđanjem i kvalitetnim upravljanjem rizicima mogu se izbjeći katastrofalne posljedice njihova utjecaja na poslovanje.

Završni rad Korporativna sigurnost obrađuje i temu Business intelligence-a, što se objašnjava kao skup metodologija za prikupljanje, analizu i distribuciju informacija uz pomoć različitih alata s ciljem da se prikupljene informacije pretvore u znanje, što predstavlja pomoć u donošenju poslovnih odluka i snalaženju poduzeća u određenim poslovnim okolnostima. Obrađene su metode poput rudarenja podataka, skladištenja podataka i analitičke obrade podataka. Business intelligence je alat pomoću kojega se mogu brzo donositi važne korporativne odluke. Svaki zahtjev za donošenje odluka, analizu i planiranje poslovanja kao i razumijevanje poslovanja potpada pod definiciju Business intelligence-a.

Rad obrađuje i temu klasifikacije podataka i temu zaštite osobnih podataka. Govoreći o klasifikaciji podataka u uvodnim rečenicama naglašeno je da su informacije moć, koliko su one su važne, skupe i dragocjene. Zlouporaba informacija ili njihova neovlaštena distribucija poduzećima može donijeti katastrofalne posljedice u obliku uništenja reputacije, visokih kazni i slično. Posebno osjetljivim informacijama smatraju se osobni podaci. Razni obvezujući pravni akti stavljaju veliki naglasak na važnost zaštite osobnih podataka, a nepridržavanje tih akata za poduzeća znače potencijalno milijunske kazne.

Jedan od važnih segmenata korporativne sigurnosti je informacijska sigurnost i svijest o sigurnosti. Kako se nalazimo u vremenu visoke tehnološke razvijenosti, na važnost zaštite informacijskih sustava treba gledati s visokom razinom razumijevanja i uvažavanja. U radu su obrađena temeljna načela informacijskog sustava (povjerljivost, integritet, raspoloživost, neporecivost, dokazivost, autentičnost i pouzdanost). Naglašena je važnost zaštite informacijskog sustava od neovlaštenog pristupa, distribucije informacija, malicioznih programa, krađe, uništenja opreme i ostalih rizika kojima je informacijski sustav izložen. U doba visoke tehnološke razvijenosti jednako su tehnološki visoko razvijeni i napadi na sustave, podatke i informacije, te se stoga zaštiti informacijske sigurnosti valja pristupiti s visokom razinom opreza i pripravnosti.

Nakon teme informacijske sigurnosti u radu je posvećena posebna pažnja svijesti o sigurnosti, koja je neodvojiva od teme informacijske sigurnosti. Rad naglašava važnost kontinuirane edukcije i podizanja svijesti o sigurnosti kod svih sudionika u procesima korporativne sigurnosti. Detaljno je obrađena tema važnosti korištenja autentifikacijskih obilježja (poput zaporki) na adekvatan način, važnost pridržavanja politika zaštite podataka od neovlaštenog pristupa (poput politike čistog stola i čistog ekrana). Zaštita podataka je temeljna pretpostavka uspješnog poslovanja, stoga su zaposlenici jedan od ključnih faktora zaštite te je njihova svijest o sigurnosti od neizmjerne važnosti za sigurno poslovanje poduzeća.

Poglavlje koje govori o tehničkoj zaštiti obrađuje temu zaštite ljudi i imovine raznim sredstvima tehničke zaštite . Poglavlje opisuje što se sve smatra sredstvima tehničke zaštite i koji su postupci izrade prosudbe ugroženosti, sigurnosnog elaborata i projektnog zadatka tehničke zaštite.

Nakon teme o tehničkoj zaštiti rad donosi temu fizičke zaštite. Govoreći o fizičkoj zaštiti govori se o osiguravanju sigurnog poslovnog okruženja od neovlaštenog pristupa, ometanja prostora i informacija koje čine imovinu poduzeća. Ovisno o tome kakvom se djelatnošću poduzeće bavi potrebno je implementirati različita pravila pristupa određenim dijelovima svojih poslovnih prostorija.

Ovim radom obuhvaćena je tema zaštite na radu i zaštite od požara. Rad opisuje najvažnije dijelove relevantnih zakona koji se bave pitanjima zaštite na radu i zaštite od požara, a fokusirani su na zaštitu zaposlenika u poduzećima u njihovom poslovnom okruženju i na obveze poduzeća i zaposlenika koje proizlaze iz Zakona o zaštiti od požara.

Sigurnost kadrova još je jedan od važnih čimbenika uspostave sigurnog poslovnog okruženja. Kako je cilj svakog poslodavca zaposliti što bolje kadrove za svako radno mjesto, potrebno je potencijalne kandidate za zaposlenje dobro procijeniti. Rad opisuje neke od načina koji se uobičajeno korite prilikom zapošljavanja kao na primjer dostavljanje potvrdu o nekažnjavanju, razni testovi znanja, preporuke prijašnjih poslodavaca. Također se pojašnjava važnost upravljanja kadrovima na način da svi zaposlenici jasno razumiju svoje obveze i odgovornosti te da se uspjesi zaposlenika evaluiraju te stimuliraju ili destimuliraju. Rad opisuje i važnost detaljnog definiranja opisa posla i specifikacija kvalifikacija za određeno radno mjesto, čime se nedvojbeno i jasno određuju zaduženja zaposlenika na određenom radnom mjestu, kao i uvjeti zaposlenja za određeno radno mjesto. U poglavlju koje govori o sigurnosti kadrova naglašena je važnost prepoznavanja ključnih zaposlenika i važnost stvaranja poslovnog okruženja u kojemu poduzeće ne ovisi isključivo o pojedincima.

Nakon teme o sigurnosti kadrova obrađena je tema koja nije primjenjiva na sva poduzeća, ali se ipak odnosi na mnoga poduzeća. Riječ je o sprječavanju pranja novca i financiranja terorizma. Ova je tema regulirana Zakonom o sprječavanju pranja novca i financiranja terorizma i vrlo detaljno opisuje tko su obveznici tog Zakona, procese i radnje koji su obveznici Zakona dužni poduzimati s ciljem sprječavanja pranja novca, poput dubinske analize klijenta, stalnog praćenja poslovnog odnosa, prijave sumnjivih transakcija i transakcija većih iznosa nadležnom uredu.

Pred kraj rada obrađena je tema upravljanja kontinuitetom poslovanja. Riječ je o procesu upravljanja u kriznim i hitnim situacijama. Upravljanje kontinuitetom poslovanja obuhvaća upravljanje posljedicama realiziranih rizika, te mjerama za minimaliziranje štete kod nastanka incidenta, kako bi se njegovi učinci što manje odrazili na daljnje poslovanje poduzeća. Upravljanje kontinuitetom poslovanja kreće od pretpostavke da će se katastrofa sigurno dogoditi u nekom trenutku i priprema planove za osiguranje kontinuiteta, nastavka poslovanja.

Zadnje poglavlje rada opisuje kontrolne funkcije koje postoje u većini poduzeća a koje čine vrlo važne faktore u procesima korporativne sigurnosti. Riječ je o funkciji za praćenje usklađenosti s propisima koji, koja , kada postoji u poduzeću, osigurava poslovanje poduzeća u skladu sa svim relevantnim propisima. Druga je funkcija interne kontrole koja je zadužena provoditi kontrole poslovanja u skladu s internim aktima poduzeća i zakonima, kontrolirati ispravnost poslovnih izvješća, otkrivati i sprječavati prijevare i pogrešaka, predlagati mjere

poboljšanje poslovanja i slično. Poglavlje također obrađuje temu eksterne revizije od strane ovlaštenog revizora koji temeljitim i objektivnim pregledima kontroliraju rad poduzeća i verificiraju točnost financijskih izvještaja koji se koriste za izvješćivanje države, vlasnika i ostalih zainteresiranih dionika.

Kroz čitav rad obrađene su teme koje su regulirane raznim zakonima,podzakonskim aktima i ISO standardima što ukazuje na činjenicu da je tema upravljanja korporativnom sigurnosti jako važna i vrlo visoko regulirana, upravo radi svoje važnosti.

Uzimajući sve prethodno navedeno u obzir, svako ozbiljno i odgovorno poduzeće će pitanje korporativne sigurnosti svrstati vrlo visoko na razinu svojih prioriteta, s ciljem osiguravanja sigurnog poslovnog okruženja, kvalitetnog upravljanja raznim oblicima rizika i adekvatnog i pravodobnog postupanja u slučaju da se rizici ipak realiziraju.

Marko Mikić

19. Popis kratica

Kratica	Značenje
BCM	Business Continuity Management
CSO	Chief Security Officer
CISO	Chief information security officer
DWH	Data Warehousing
Itd.	I tako dalje
Sl.	Slično
ZSPN i FT	Zakon o sprječavanju pranja novca i financiranja terorizma

20. Popis literature

Međunarodni standardi:

1. ISO 27001:2013, Information security management
2. ISO 31000:2009, Risk management - Principles and guidelines
3. ISO 31010:2009, Risk management - Risk assessment techniques
4. ISO 22301:2012, Societal security - Business continuity management systems – Requirements

Uredba (EU) 2016/679 Europskog parlamenta i vijeća

1. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka

Zakoni i podzakonski akti Republike Hrvatske:

1. Ustav Republike Hrvatske,
2. Zakon o informacijskoj sigurnosti,
3. Zakon o provedbi opće uredbe o zaštiti podataka,
4. Zakon o sprječavanju pranja novca i financiranja terorizma,
5. Zakon o zaštiti na radu,
6. Zakon o zaštiti od požara,
7. Zakon o privatnoj zaštiti,
8. Pravilnik o uvjetima i načinu provedbe tehničke zaštite
9. Smjernice za upravljanje informacijskom sustavom u cilju smanjenja operativnog rizika

Literatura:

1. Bahtijarević-Šiber F., Management ljudskih potencijala, Golden marketing, Zagreb, 1999.
2. Bilandžić M., Poslovno obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb, 2008.
3. Buble M., Osnove menadžmenta, Zagreb, Sinergija nakladništvo d.o.o. Zagreb, 2006.
4. Buble M., [et.al], Strateški menadžment, Sinergija nakladništvo d.o.o, Zagreb, 2005.
5. Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, udruga hrvatskih menadžera sigurnosti – UHMS, 2011.

Internetski članci:

1. www.hnb.hr
2. https://www.zakon.hr/
3. https://www.iso.org/
4. https://narodne-novine.nn.hr/
5. https://gdpr2018.eu/
6. https://hrcak.srce.hr/
7. http://www.poslovni.hr/leksikon/financijski-rizik
8. http://hjp.znanje.hr/
9. https://hr.wikipedia.org/wiki/Poslovna_inteligencija

21. Popis slika