Uloga korporativne sigurnosti u poslovanju poduzeća

Relota, Danijel

LIBERTAS MEĐUNARODNO SVEUČILIŠTE
ZAGREB

DANIJEL RELOTA

ULOGA KORPORATIVNE SIGURNOSTI U POSLOVANJU PODUZEĆA

ZAVRŠNI RAD

Zagreb, travanj, 2019.

LIBERTAS MEĐUNARODNO SVEUČILIŠTE
ZAGREB

Preddiplomski stručni studij
Menadžment poslovne sigurnosti

ULOGA KORPORATIVNE SIGURNOSTI U POSLOVANJU PODUZEĆA

ZAVRŠNI RAD

KANDIDAT: Danijel Relota
KOLEGIJ: Korporativna sigurnost
MENTOR: mr.sc. Zoran Stanko

Zagreb, travanj, 2019.

1. UVOD

Zbog uvjeta današnjice korporativna sigurnost posatje sve važniji dio funkcija svakog poduzeća. Veličina i vidljivost korporativne sigurnosti su povezani sa područjem poslovanja tvrtke te njezinom veličinom. Uspostavljanje korporativne sigurnosne službe povećava i doprinosi otpornosti poduzeća. Ona postaje poslovni standard rastućih kompanija, masovno se primjenjuje te potreba za njezinom implementacijom u poslovanje poduzeća postaje neophodna.

Proces globalizacije, tehnološke inovacije, jaka konkurencija i brze društvene promjene, koji mnoge poduzetnike potiču na neetično ponašanje u odnosu na konkurente, su razlog moje želje za upoznavanjem zakonskih osnova i propisa, te kaznenih sankcija koje slijede ukoliko se isti ne poštuju.

Rad obrađuje normativni okvira korporativne sigurnosti i njezine glavne dimenzije koje se smatraju važnima za sprječavanje ugroze poslovnih procesa ili smanjenje ugroze i pronalazak najbolje sigurnosne politike za poduzeće.

Cilj ovog rada je prikazati osnovne i bitne mjere zaštite poslovanja kako malih tako srednjih i velikih poduzeća, uz što se vežu zaštita na radu, procjene rizika, kontinuitet poslovanja, zaštita osoba i imovine (privatna zaštita), zaštita okoliša, zaštita osobnih podataka, zaštite od požara, zaštite intelektualnog vlasništva, informacijske sigurnosti, upravljanje poslovnim informacijama (business intelligence), pa sve do sprečavanja pranja novca i financiranja terorizma. Središnje pitanje koje se postavlja je- kako uspostaviti kvalitetnu korporativnu sigurnost nekog poduzeća.Većina navedenih pojmova ima zakonsku osnovu, ali problem je i dalje prisutan kada se analiziraju važeći zakoni i pravilnici i kada se shvati da je dio njihovih odredbi kontradiktoran. Neizostavno je spominjanje pojma business intelligenc, koji danas predstavlja strateški menađerski resurs.

Rad se također bavi najbitnijim faktorima ugrožavanja poslovanja poduzeća, njihovim uzrocima te mogućnostima zaštite od njih. Ukazuje se i na potrebu komunikacije i usklađenosti pojedinih segmenata s korporativnom sigurnošću.

.

2. DEFINICIJA POJMA KORPORATIVNE SIGURNOSTI

Korporativna sigurnost kao sustav zaštite poduzeća nije nigdje definirana kao pojam ni u jednom zakonu u Republici Hrvatskoj. Iako postoje teškoće u samom definiranju korporativne sigurnost radi njezine kompleksnosti i ne postoji univerzalna definicija, ipak uvaženo je da korporativna sigurnost predstavlja suvremenu poslovnu funkciju zaštite osoba, imovine i poslovne djelatnosti u okvirima organizacijske strukture poslovnih sustava.[1] Dakle, ona se odnosi na zaštitu informacijskog i računalnog sustava, fizičku zaštitu, tehničku zaštitu, zaštitu intelektualnog vlasništva te zaštitu poslovnih tajni. Kada je riječ o obavljanju njezine temeljne djelatnost u kontekstu zaštite korporativnih interesa i definiranih ciljeva, kontekst doprinosa korporativne sigurnosti se ogleda i u širim okvirima. Ona kroz promociju odgovornog korporativnog ponašanja u području sigurnosti u svom okruženju i društvenoj zajednici u kojoj posluje, pozitivno utječe na povećanje ukupne razine nacionalne sigurnosti konkretne države. Po prirodi svojih aktivnosti, polazeći od vlasničke strukture organizacijskog konteksta funkcije, korporativna sigurnost pripada području privatne sigurnosti, i kao takva formalno pronalazi svoje mjesto u sustavu nacionalne sigurnosti. Budući da se suvremeno korporativno okruženje ubrzano mijenja zbog kompleksnih i brojnih faktora, rizici i prijetnje po poslovanje kompanija danas više nego ikada ranije pokazuju veliku raznolikost kao i vrlo čestu promjenu načina i oblika ispoljavanja.[2] Upravo zato se pod djelokrugom korporativne sigurnosti ubraja veliki broj zaštitnih funkcija, među kojima su najznačajnije otkrivanje i sprječavanje korporativnog kriminala, zaštita poslovanja u kriznim situacijama i kriznim područjima, upravljanje rizicima, zaštita imovine, zaštita osoba, kao i zaštita poslovne tajne i intelektualnog vlasništva. Dakle, korporativna sigurnost ima za cilj da osigura vitalne vrijednosti kompanije u skladu sa važećim zakonskim odredbama države u kojoj posluje i na taj način opravda svoje mjesto i ulogu u sustavu nacionalne sigurnosti. Budući da korporativna sigurnost ne može samostalno egzistirati, potreban joj je prikladni funkcionalni okvir.

Iskustvo pokazuje da korporativna sigurnost najčešće biva ugrožena radi:

- ignoriranja potencijalnih prijetnji te nedostatka svijesti o mogućoj poslovnoj ugroženosti

- nepostojanja sigurnosne zaštite

[1] Mihaljević B., Nađ I., Osnove korporativne sigurnosti, Zagreb, 2018., str. 16.
[2] Mihaljević B., Nađ I., Osnove korporativne sigurnosti, Zagreb, 2018., str. 18.

- fokusa na pogrešne izvore moguće prijetnje[3]

Važno je obratiti pozornost na eksterne, vanjske uzročnike (zlonamjerni hakerski napadi, industrijska špijunaža, cyber kriminal) i interne uzročnike tzv. insidere (zaposlenici unutar kompanije) te isto tako treba analizirati slabosti, ranjivosti sustava i sukladno tome implementirati adekvatnu zaštitu. Također treba pripaziti i na insidere tj. zaposlenike unutar kompanija koji su dokaz da u sve većem broju slučajeva korporativna sigurnost biva ugrožena upravo zahvaljujući ljudskom faktoru. Dubinske provjere zaposlenika i potencijalnog ljudskog kadra postaju neminovne.

Korporativna sigurnost je prvenstveno usmjerena na zaštitu u svrhu ostvarenja zadanih ciljeva te održavanja poslovnih uspjeha poduzeća. Sredstva koja se ulože u zaštitu predstavljaju maleni ulog u odnosu na potencijalne poslovne gubitke do kojih može doću ukoliko se ignorira sigurnosi aspekt. Statistika i iskustvo pokazuju da nije pitanje hoće li korporativna sigurnost biti ugrožena, nego kada.

2.1. Elementi korporativne sigurnosti

Sukladno smjernicama Europske unije koristi se pojam *integralna sigurnost* i ona se dalje dijeli na poslove sigurnosti (engl. security) i zaštite (engl. safety) na radu, zaštite od požara i zaštite okoliša[4] .

Integracijom navedenih smjernica dobio bi se odjel koji bi pokrivao kompletno područje zaštite i služio za provođenje i nadzor poslovnih procesa. Praksa u dosta velikih poduzeća je pokazala da se za određene segmente zaštite, a pogotovo koji se odnose na zaštitu na radu, zaštitu od požara te zaštitu okoliša angažiraju vanjske tvrtke kao suradnici za ispunjavanje zakonskih normi. Broj zaposlenih u takvom odjelu povećava se razmjerno povećanjem brojem zaposlenih u poduzeću. Kao što je već spomenuto, upravljanje poslovnim procesima korporativne sigurnosti dijeli se na sljedeće podskupine[5]:

[3] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str.30.
[4] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str.66.
[5] Ibid., str.78

1. Informacijska sigurnost

2. Privatna zaštita

3. Zaštita intelektualnog vlasništva

4. Zaštita podataka

5. Privatna istražna djelatnost

6. Poslovna istraživanja (engl. business intelligence)

7. Sprečavanje pranja novca i financiranje terorizma

8. Zaštita na radu

9. Zaštita od požara

10. Zaštita okoliša i održivo gospodarenje otpadom

11. Zaštita i spašavanje

12. Obrambene pripreme

Kako bi se stekao dojam o potencijalnoj veličini odjela za korporativnu sigurnost potrebno je analizirati zakone koji propisuju broj osoba sukladno broju zaposlenih odnosno veličini poduzeća, a to su Zakon o zaštiti na radu, Zakon o zaštiti od požara, Zakon o zaštiti osobnih podataka i Zakon o održivom gospodarenju otpadom.

Poštujući direktivu Europske unije o podjeli integralne sigurnosti, struktura odjela za korporativnu sigurnost poduzeća može se sažeti u dva odjela i to:

1. Informacijska sigurnost - zaštita poslovnih podataka
   - zaštita intelektualnog vlasništva
   - zaštita osobnih podataka
   - privatna zaštita

2. Zaštita - zaštita na radu
   - zaštita od požara

- zaštita i spašavanje

- zaštita okoliša i održivo gospodarenje otpadom[6]

Elementi korporativne sigurnosti će se u nastavku rada bolje objasniti kroz normativni okvir i metode zaštite korporativne sigurnosti u poslovanju poduzeća.

2.2. Izvođenje sustava zaštite

Uspostava korporativne sigurnosti u poduzeća je složen i kompleksan projekt. Mora se odvijati po fazama i poštovati pravila izrade. Kako ne postoji pravilnik, zakon ili naputak za implementaciju korporativne sigurnosti, kao predložak se može koristiti ISO norma 27003 Smjernice za uvođenje sustava menadžmenta informacijske sigurnosti. Uz ISO 27003 koristi se ISO 27001 u kojoj su postavljeni zahtjevi za sustave upravljanja informacijskom sigurnošću. Ako se odluči za implementaciju korporativne sigurnosti bez certificiranja i pripreme za ISO 27001 može se to učiniti na sljedeći način. Da bi se došlo do krajnjeg cilja postavljaju se šest koraka:

1. Popisivanje ključnih parametara potrebnih za rad

2. Raspodjela odgovornosti i prava

3. Izrada sigurnosne politike

4. Tehnička podrška sustavu korporativne sigurnosti

5. Provođenje postavljenih mjera i obuka djelatnika

6. Provjera i unaprjeđivanje sustava.

[6] Mihaljević B., Nađ I., Osnove korporativne sigurnosti, Zagreb, 2018., str. 39.

Ovih šest koraka predstavlja pojedinačne faze koje se ne bi trebale preskakati te svakoj od njih treba pristupiti sistematično i sve korake treba kvalitetno dokumentirati. Ovisno o djelatnosti tvrtke koja uvodi sustav korporativne sigurnosti neke od faza mogu biti većeg, a neke manjeg opsega od navedenih smjernica.

Postoje dvije politike koje bi se također trebale provoditi kao nulta faza. Prva preporučena politika bi trebala biti politika praznog stola. Svrha ove politike je naučiti djelatnike da dokumenti koji nisu u radu i koji ne bi trebali biti javno dostupni budu uklonjeni sa stola kada se na njima ne radi i svakako nakon radnog vremena. Ako postoji tehnička mogućnost svakako bi trebali biti u zaključanim ormarima/ladicama. Osim dokumentacije u papirnatom obliku ista politika se primjenjuje na elektroničke medije kao što su CD, DVD, memorijske kartice, USB, mali diskovi i diskovi za pohranu podataka odnosno diskovi za izradu pričuvnih kopija. Preporuka za diskove na koje se sprema pričuvna kopija je da ne budu konstantno uključeni u računalo, već u trenutku odluke za izradu pričuvne kopije se izvade, spoje na računalo i nakon izrade pričuvne kopije vrate nazad u ormar/ ladicu pod ključ.[7]

Druga preporučena politika je politika prazne radne površine na računalu (desktop). Svrha ove politike je da se korisnici odviknu od spremanja podataka na radnu površinu čime ih čine lako dostupnim ako se netko pokuša poslužiti njihovim računalom. Isto tako ista politika se odnosi na vođenje poslovnih ili radnih sastanaka u prostorijama gdje se nalaze računala. U trenutku kada osoba koja nije iz sustava (stranka) dolazi u ured na sastanak trebalo bi zatvoriti/sakriti sve otvorene dokumente da uslijed potencijalnog odlaska iz ureda ne bi postali lako dostupni.[8]

Prva i osnovna faza koju moramo riješiti je popisati i dokumentirati sve bitne procese, podatke, baze podataka, specifikacije ili dokumente koje je potrebno zaštititi. Za svaku od navedenih stvari potrebno je jasno definirati gdje se ona nalazi, da li postoji sigurnosna kopija i gdje se ona nalazi, što je sve potrebno za kontinuitet rada u slučaju nekog nepredviđenog događaja. Uz navedenu listu bitna stvar je i pripremiti popis tvrtki i pojedinaca koji mogu pomoći u slučaju neke katastrofe. Da pobliže objasnim, Server koji smo kupili za centralnu bazu podataka je marke XY , kupljen je u tvrtki YZ i njegove specifikacije su XX. Tvrtka se

[7] Mihaljević B., Nađ I., Osnove korporativne sigurnosti, Zagreb, 2018., str. 41.
[8] Ibid., str.42.

nalazi na adresi BB i kontakt osoba je AB i može se dobiti na broj telefona/mobitela BBB, radno vrijeme tvrtke je OD - DO. Isto tako potrebno je dokumentirati najbitniju opremu potrebnu za rad (napraviti popis 5-6 najosnovnijih stvari s tehničkim karakteristikama). Izrađeni popis u papirnatom obliku spremiti na jedno do dva mjesta. Zašto? Uzmimo banalan realan primjer. Ako zbog npr. udara groma se ošteti sva oprema u npr. server sali, više se ne može pogledati u konfiguraciji računala što je u njemu, treba izgubiti puno vremena da se nađu ulazni računi za tu opremu a vrijeme je presudan faktor. S ispisanim podatcima dovoljan nam je samo telefon da započnemo postupak vračanja poslovanja u normalu. Isto tako je bitno dokumentirati sve parametre spajanja na internet, elektronsku poštu, podatke o pristupnim podatcima za web stranicu tvrtke gdje se može postaviti obavijest da smo na korporativnom druženju tri dana. Krajnji korisnik ali i konkurencija ne mora znati što se dogodilo i koji su razmjere štete.

Nakon što smo sve dokumentirali i shvatili što nam je sve bitno krećemo na sljedeću fazu koja se odnosi na dodjelu/raspodjelu odgovornosti i prava. Za svaki od navedenih dokumenata, podataka koji smo proglasili ključnim za poslovanje definiramo tko ima prava i ovlasti: koristi ti ih, davati na uvid drugima, tko se brine o izradi sigurnosnih kopija, način autorizacije u neki sustav s razinama pristupa, tko od vanjskih suradnika mora odnosno može imati pristup ključnim podatcima i na koji način im mogu pristupiti. Za sve djelatnike bilo bi dobro da potpišu izjavu o zaštiti i tajnosti poslovnih podataka ako već ista nije definirana u ugovoru o radu. Ali prije nego što krenemo s potpisivanjem trebamo proći još jednu fazu koju možemo objediniti u izjavu koju će djelatnici potpisati. Ako već ne postoji obavezno je sa svim dobavljačima i poslovnim partnerima potpisati ugovor ili sporazum o tajnosti podataka.

Kada se odredi tko i pod kojim uvjetima ima pristup ključnim podatcima preporuka je da se takvi podatci također pohrane izvan računalnog sustava u pisanom obliku. Do sada smo napravili dva bitna koraka jer smo odredili što nam je ključno i tko ima pristup takvim podatcima te pod kojim uvjetima. U sklopu ove faze bitno je podijeliti i zaduženja i razine pristupa administratorima sustava. Osim zaduženja što rade u normalnim okolnostima potrebno je predvidjeti i njihove ulogu u slučaju incidentne situacije te odrediti vrijeme njihove reakcije na incident.[9]

[9] Mihaljević B., Nađ I., Osnove korporativne sigurnosti, Zagreb, 2018., str. 44.

Sigurnosna politika je dio sustava upravljanja sigurnošću informacijskog sustava. Njezina je svrha da definira prihvatljive i neprihvatljive načine ponašanja, da jasno raspodijeli zadatke i odgovornosti, te da propiše sankcije u slučaju nepridržavanja. Sigurnosne politike su ovisne o promjenama tehnologija i organizacijske strukture pa postoji vjerojatnost da će se i češće mijenjati da bi imali svoju pravu svrhu.[10] Moguća su znatna odstupanja u potrebama sigurnosnih politika što pretežito ovisi o djelatnosti kojom se tvrtka bavi. Sigurnosnu politiku je bitno dati svim djelatnicima na uvid kako bi je znali primijeniti u svakodnevnom poslovanju i u izvanrednim okolnostima i kako bi znali ispravno koristiti tehnologije koje su im potrebne za normalan rad. Određivanje sigurnosne politike trebalo bi se temeljiti na unaprijed definiranim smjernicama vezanima uz popisane ključne parametre za rad. Uvođenje sigurnosne politike ima za cilj jasno utvrđivanje pravila ponašanja i odgovornosti kako bi se mogućnost potencijalne štete nastale namjernim ili nenamjernim pogreškama u radu.[11] Sigurnosna politika ima za cilj postavljanje pravila čije se kršenje može i mora sankcionirati na način proporcionalna težini pogreške, propusta. Gledajući podatak da neka tvrtka ima uvedenu formalnu sigurnosnu politiku smatra se da su sigurnost i zaštita informacijskog sustava na visokoj razini. Sigurnosna politika treba imati jasno definiranu: svrhu, doseg, pravilnik, mjere za nepridržavanje za korisnike i administratore.

Tehnička podrška sustavu može se podijeliti na dva segmenta i to na sustave potrebne za uspostavu tehničke zaštite tvrtke i sustave potrebne za kontinuirano poslovanje nakon incidentne situacije. Iako ovaj elaborat nije obavezan za većinu tvrtki preporuka struke je da se elaborata izradi jer može direktno ukazati na potencijalne prijetnje i kritične točke koje je potrebno posebno štititi. Sustave tehničke zaštite treba ugraditi neovisno. Ako je potrebno ugrađivati više sustava osobna preporuka da se ide na zasebne sustave a ne na integralne, upravljane s jednog mjesta. Po pitanju korporativne sigurnosti je bitno da sustavi budu neovisni, mogu biti međusobno povezani ali nikako da su jedna cjelina. Korisnici često ne razlikuju tipove sustava pa se kao sustav kontrole pristupa ugrađuju elektroprihvatnici koji se otvaraju kada dođe napon na njih a ostatak vremena su zaključani. Ispravna ugradnja navedenog sustava bi bila "fail safe" (engl. bez napona otključano). međutim to znači da se u slučaju nekog generalnog kvara sva vrata otključavaju što je i sukladno Zakonu o zaštiti od požara te Zakonu o zaštiti i spašavanju. Ako je generalni problem na integralnom sustavu tehničke zaštite kada sustav ne radi , ne radi ni protuprovalni sustav, videonadzor. Sustavi

[10] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 91.
[11] Ibid., str.92.

potrebni za kontinuitet poslovanja se u našim prilikama svode na jedno računalo za pohranu pričuvnih kopija podataka koje se najčešće nalazi na istoj lokaciji gdje se nalazi i centralno računalo i računalni sustav za koji je potrebno izraditi pričuvne kopije. Nemaju sve tvrtke mogućnost smještaja takvog računala na drugu tektonsku ploču i u sigurnim uvjetima. U Republici Hrvatskoj se otvara se veći broj farmi s ogromnim brojem računala za prihvat pričuvnih kopija ili čak i za operativni rad. Takva "postrojenja" se grade u posebnim uvjetima sa strogo kontroliranim mikroklimatskim uvjetima i izrazito naprednim sustavima zaštite od neovlaštenog pristupa što fizički računalima što podatcima koji se na njima nalaze. Svaka tvrtka bi trebala biti spremna na incidentnu situaciju otkazivanja računalne opreme. Pitanje je samo materijalne prirode koliko smo voljni investirati da postignemo kontinuitet poslovanja. Bez adekvatnih tehničkih uređaja i opreme sustav korporativne sigurnosti je ugrožen sam po sebi.

Najbitnija točka sustava je početak njegove primjene. Najbolji način je postupno uvođenje mjera sigurnosti počevši od politike praznog stola pa dalje prema sigurnosnim politikama. Za implementaciju sustava potrebno je imati bezrezervnu podršku i odluku uprave koja će se i sama pridržavati propisanih pravila. Ako postoji bilo kakav otpor menadžmenta za uvođenje sustava korporativne sigurnosti postoji velika mogućnost da kompletne implementacije nikada ne dođe. U korporativnoj sigurnosti ne postoje iznimke već pravila kojih se svi moraju pridržavati. Kvalitetna komunikacija i obuka svih zaposlenih može dovesti do bezbolne i kvalitetne implementacije i primjena sustava korporativne sigurnosti. Nakon implementacije potrebna je kontinuirana obuka i podsjećanje djelatnika na njihove obveze. najučinkovitiji način je nažalost stegovno kažnjavanje prvog koji se prestane pridržavati pravila iz sigurnosnih politika. Najčešće su to radnje koje same po sebi nisu strašne (u pričuvnoj kopiji su osim poslovnih podataka snimke s nečijeg vjenčanja koje zauzimaju ogromnu količinu diskovnog prostora).[12] Upravo takve radnje su idealne za kazne jer nije ugrožena sigurnost, kazna može biti materijalna i ako se objavi javno imat će veliki učinak za pridržavanje sigurnosnih politika koje su stvarno bitne i važne za korporativnu sigurnost.

Svaki sustav je potrebno provjeravati, dograđivati i testirati. Bez kvalitetne analize učinjenog i testiranog ne možemo biti sigurni u kvalitetu korporativne sigurnosti koju smo implementirali.

[12] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 98.

Provjera sustava se može vršiti od razina pristupa podatcima pa sve do razine detalja obuhvaćenih u sigurnosnim politikama. Nikada se u startu implementacije nije uspjelo postići savršenstvo da sve radi besprijekorno. Podatak se odnosi na velike sustave s nekoliko stotina zaposlenih kada se rad odvija na više lokacija i postoji veliki otpor u implementaciji. Kod manjih sustav uspješnost ovisi o čvrstini stavova uprava.

Testiranje sustava se obično provodi uz simulaciju nekih od tehničkih kvarova da se vidi spremnost i brzina potrebna za nastavak poslovanja.[13] U takva testiranja uključen je najčešće mali broj ljudi pretežno administratora sustava da se vidi vrijeme reakcije. Iz iskustva mogu reći da u trenutku pravog incidenta se vrlo brzo zaboravljaju hijerarhijska pravila, redoslijed radnji i cijela situacija je vrlo konfuzna i kontraproduktivna. Testiranje je izrazito bitan segment jer jedino on može dati kvalitetne odgovore što ne valja i što je potrebno poboljšati ili u konačnici kompletno promijeniti da bi sustav savršeno funkcionirao.

Iako se ovih šest koraka oslanja na normu ISO 27001 za postizanje nivoa informacijske sigurnosti koju propisuje ISO 27001 potrebno je puno više i stručna pomoć stručnjaka, audita za to područje.

3. NORMATIVNI OKVIR KORPORATIVNE SIGURNOSTI

3.1. Informacijska sigurnost

Poslovnu informaciju predstavlja svaka informacija potrebna za obavljanje poslovnih aktivnosti te za ostvarivanje poslovnih interesa i ciljeva poslovnog subjekta.[14] Ona predstavlja temeljni resurs svakog poslovnog sustava te mu posjedovanje informacija daje prednost u odnosu na konkurente. Informacije omogućavaju prepoznavanje i iskorištavanje poslovnih prilika, donošenje kvalitetnih odluka, poboljšanje produktivnosti te uočavanje tržišnih trendova, što dovodi do ostvarenja poslovnog uspjeha i boljeg pozicioniranja u odnosu na konkurente. Iz tog razloga svako poduzeće stvara i razvija vlastito područje poslovnih podataka i informacija.

[13] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 97.
[14] Javorović B., Bilandžić M., Poslovne informacije i business intelligence, Zagreb, 2007., str. 116.

Povjerljivost informacija znači da je informacija dostupna samo osobama koje imaju ovlaštenje za njezino korištenje. Integritet je zaštita podataka od namjernog ili slučajnog neovlaštenog mijenjanja, a dostupnost je jamstvo ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku.[15]

Informacijska sigurnost je jedan od segmenata korporativne sigurnosti koji ima zakonsku podlogu.

Zakon o informacijskoj sigurnosti (NN 79/07) utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područje informacijske sigurnosti te tijela nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.[16] On je u osnovi pisan za primjenu u državnim tijelima, tijela jedinica lokalne i područne samouprave te za sve pravne i fizičke osobe koje u svom djelovanju koriste ili imaju pristup klasificiranim i neklasificiranim podacima. Zakon se u osnovi temelji na ISO 27001 standardu. ISO 27001 je međunarodni standard objavljen od strane Međunarodne Organizacije za Standardizacije (ISO) i opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Najnovija revizija ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. ISO 27001 može biti implementiran u bilo kojoj organizaciji bez obzira na njezinu veličinu i bez obzira radi li se o profitnoj ili neprofitnoj, privatnoj ili državnoj. Postao je najpopularniji standard informacijske sigurnosti u svijetu, te su mnoge kompanije certificirane prema njemu.[17] Za razliku od zakona o informacijskoj sigurnosti, ISO 27001 postepeno vodi kroz kvalitetnu uspostavu informacijske sigurnosti u svakom poduzeću. Nedovoljna informiranost i težnja da sve bude jednostavno po pitanju informacijske sigurnosti dovodi do propusta koji u nekim slučajevima mogu imati i katastrofalne razmjere u smislu gubitaka podataka, nastavka poslovanja i repozicioniranja poduzeća nazad na tržište nakon katastrofe. U informacijskoj sigurnosti postoje točno određeni zahtjevi za uspostavu, primjenu, nadzor, održavanje i stalno poboljšavanje sustava informacijske sigurnosti.

Zakon o zaštiti osobnih podataka odnosi se na područje informacijske sigurnosti i utvrđuje zaštitu osobnih podataka o fizičkim osobama, a primjenjuje se na obradu osobnih podataka od strane državnih tijela, tijela jedinica lokalne i regionalne samouprave te na sve pravne i fizičke osobe i predstavništva koja obrađuju osobne podatke.[18]

---

[15] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 94.
[16] Ibid., str.95.
[17] https://advisera.com/27001academy/hr/sto-je-iso-27001/ , 21.03.2019
[18] NN 103/03, 118/06 i 41/08

Zakon o zaštiti i tajnosti podataka propisuje mjere i postupke za utvrđivanje, upotrebu i zaštitu podataka, koji predstavljaju profesionalnu i poslovnu tajnu.[19]

Zakon o elektroničkoj ispravi uređuje pravo fizičkih i pravnih osoba na upotrebu elektroničke isprave u poslovnim djelatnostima. On sadrži odredbe koje se odnose na informacijsku sigurnost, a propisuje mjere koje se moraju primijeniti u odnosu na elektroničku arhivu s ciljem ostvarenja sigurnosti elektroničkih isprava i podataka pohranjenih u njima.[20]

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske uključuje sustavno prikupljanje, analize, obrade i ocijene podataka značajnih za državnu sigurnost koji su nužni za donošenje odluka značajnih za ostvarivanje državnih interesa u području državne sigurnosti. Tim zakonom se osniva Sigurnosno – obavještajna agencija i Vojno sigurnosna obavještajna agencija, te Ured Vijeća za nacionalnu sigurnost. Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo odgovorno za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u Republici Hrvatskoj, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.[21]

Zakon o sigurnosnim provjerama propisuje sustav sigurnosne provjere osoba koje ostvaruju pristup klasificiranim podacima.

Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite poslovnih kategorija osobnih podataka propisuje mjere održavanja i provjere ispravnosti rada računalne, telekomunikacijske i programske opreme, te sustava za vođenje zbirki posebnih kategorija osobnih podataka i osiguranje radnih prostorija u kojima je smještena oprema.[22]

Uredba o mjerama informacijske sigurnosti propisuje mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima.

Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima određuje osobe za koje se provodi sigurnosna provjera, vrste i postupci sigurnosne provjere.

[19] NN 108/96 i 79/07
[20] NN 150/05
[21] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 96.
[22] NN broj 139/04

Pravilnikom o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost su utvrđeni kriteriji za ustrojavanje radnih mjesta i imenovanje savjetnika za informacijsku sigurnost.

Odluka o primjerenom upravljanju informacijskim sustavom propisuje obveze kreditnih institucija koje se odnose na upravljanje informacijskim sustavom.

Odlukom o upravljanju rizicima se utvrđuje obveza kreditnih institucija na primjereno upravljanje informacijskim sustavom i njegovim rizikom.

Svaki poslovni subjekt prikuplja i obrađuje određenu vrstu podataka. Za neke od tih podataka postoji zakonska obveza njihove zaštite, dok će za druge podatke biti u interesu poslovnog subjekta da oni ostanu povjerljivi, cjeloviti i raspoloživi.[23] U današnjici informacijski sustavi izloženi su različitim sigurnosnim prijetnjama koje ugrožavaju cjelokupno poslovanje. Predmet ugroženosti može biti svaka vrijednost u informacijskom sustavu kao npr. Informacijsko-komunikacijski sustav kao cjelina, računala i podaci koji se u njima nalaze, podaci o poslovnim suradnicima, osobni podaci zaposlenika, evidencije i baze podataka, informacijsko-komunikacijska tehnologija, poslovni i proizvodni procesi, tehnologija, zaposlenici u informacijski-komunikacijskim sustavima, tehničko-sigurnosnisustavi, intelektualno vlasništvo, poslovne organizacije i korisnici informacijsko-komunikacijskih sustava.[24] Uspješna primjena informacijske sigurnosti zahtijeva sustavno upravljanje različitim aspektima informacijske sigurnosti u skladu s odgovarajućim standardima i normama.

Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet cjelina s ciljem sustavne i učinkovite realizacije, donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti. Podjela područja informacijske sigurnosti su:

1. sigurnosna provjera

2. fizička sigurnost

3. sigurnost podataka

4. sigurnost informacijskog sustava

[23] NN 1/09, 41/09, 75/09 i 2/10
[24] Javorović B., Bilandžić M., Poslovne informacije i business intelligence, Zagreb, 2007., str. 296

5. sigurnost poslovne suradnje[25]

Standardi područja informacijske sigurnosti propisani su pravilnicima koje je donio Ured Vijeća za nacionalnu sigurnost. Ured Vijeća za nacionalnu sigurnost trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima informacijske sigurnosti, te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

3.1.1. Zaštita osobnih podataka

U Republici Hrvatskoj Zakonom o zaštiti osobnih podataka se uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Osobni podaci su najtraženiji podaci i najčešći predmet nedopuštene trgovine te sukladno tome je donesena Uredba (EU) 2016/679 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi obrade osobnih podataka i o slobodnom kretanju takvih podataka. Uredba donosi rigorozne mjere po pitanju prikupljanja, obrade ili neovlaštene distribucije osobnih podataka. Kao primjer se može navesti visinu upravnih kazni za kršenje uredbe koje iznose 20.000.000,00 Eura ili u slučaju poduzetnika do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Voditelj zbirke osobnih podataka za svaku zbirku osobnih podataka koju vodi, dužan je uspostaviti i voditi evidenciju koja sadrži temeljne informacije o zbirci osobnih podataka. Evidencije se dostavljaju Agenciji za zaštitu osobnih podataka, gdje se onda objedinjuju u Središnjem registru. Prije uspostave zbirke osobnih podataka, voditelji zbirke dužni su o namjeravanoj uspostavi zbirke osobnih podataka obavijestiti Agenciju za zaštitu podataka. Agenciju za zaštitu podataka dužni su obavijestiti i o svakoj daljnjoj namjeravanoj obradi tih podataka i to prije poduzimanja bilo kakvih aktivnosti obrade.

Evidencije osobnih podataka sadrže temeljne podatke o zbirci osobnih podataka. Upisivanje podataka u evidenciju zbirke osobnih podataka i druge poslove vezane uz evidenciju zbirke provodi osoba odgovorna za vođenje pojedine zbirke osobnih podataka. Evidencije se mogu voditi ručno ili sredstvima za automatsku obradu podataka. Način vođenja evidencije osobnih

[25] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 310.

podataka detaljno je propisan Uredbom o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka.[26]

Osobni podaci u zbirkama osobnih podataka moraju biti pod odgovarajućom zaštitom, radi sprječavanja slučajne ili namjerne zlouporabe, uništenja, gubitka, te neovlaštenih promjena ili dostupnosti. Voditelj zbirke osobnih podataka i korisnik dužni su poduzeti tehničke i kadrovske, te organizacijske mjere zaštite osobnih podataka koje su potrebne da bi se osobni podaci zaštitili.

Uredbom se jasno definiraju koji podaci se smiju prikupljati, pod kojim uvjetima, način korištenja istih te način zaštite istih. Bitan aspekt zaštite osobnih podataka biti će tehnička i integrirana zaštita podataka opisana u članku 25. Uredbe koji glasi:

1. Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.

2. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.

3. Odobren mehanizam certificiranja sukladno članku 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavaka 1. i 2. ovog članka[27]

Nadzor nad obradom osobnih podataka provodi Agencija za zaštitu osobnih podataka na zahtjev ispitanika ili po službenoj dužnosti. Zakon obvezuje Agenciju na razmatranje svih zahtjeva koji se odnose na utvrđivanje povrede prava u obradi osobnih podataka i

[26] NN broj: 105/04
[27] http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/ , 13.ožujka.2019.

izvješćivanje podnositelja zahtjeva o mjerama koje su poduzete u vezi s utvrđenim činjeničnim stanjem. Agencija ima pravo pristupa svim osobnim podacima, bez obzira jesu li evidencije o tim podacima objedinjene u središnji registar ili ne. Agencija također ima pravo pristupa svim spisima i dokumentaciji koja se odnosi na obradu osobnih podataka, kao i sredstvima elektronske obrade bez obzira na stupanj njihove tajnosti.

3.1.2. Zaštita poslovnih podataka

U Republici Hrvatskoj Zakonom o tajnosti podataka definirani su pojmovi zaštite poslovnih podataka. Zakonom je objašnjeno da poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.[28] Zakon predstavlja osnovu za izradu općeg akta u poduzećima kojima se definira koji sve podatci se klasificiraju kao poslovna tajna te tko sve može i u kojim uvjetima dati takve podatke. Općim aktom se ne može odrediti da se svi podaci koji se odnose na poslovanje pravne osobe smatraju poslovnom tajnom niti se poslovnom tajnom mogu odrediti podaci čije priopćavanje nije razložno protivno interesima te pravne osobe. Poslovnom tajnom ne mogu se odrediti podaci koji su od značenja za poslovno povezivanje pravnih osoba niti podaci koji se odnose na zaštićeno tehničko unapređenje, otkriće ili pronalazak. Pravna osoba dužna je čuvati kao tajnu i podatke:

1. koje je kao poslovnu tajnu saznala od drugih pravnih osoba

2. koji se odnose na poslove što ih pravna osoba obavlja za potrebe oružanih snaga, redarstvenih vlasti Republike Hrvatske ili drugih javnih tijela, ako su zaštićeni odgovarajućim stupnjem tajnosti,

3. podatke koji sadrže ponude na natječaj ili dražbu - do objavljivanja rezultata natječaja odnosno dražbe,

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

[28] NN 108/96 i 78/07

Podatke koji se smatraju poslovnom tajnom na temelju općeg akta mogu drugim osobama priopćavati samo ovlaštene osobe određene općim aktom.

Općim aktom pobliže se određuju slučajevi te način zaštite kad se podaci mogu priopćavati drugim osobama, ovlaštene osobe koje ih mogu priopćavati, te osobe kojima se takvi podaci mogu priopćavati.

U pravnoj osobi određuje se ovlaštena osoba ili se osniva posebno tijelo koje ima uvid u poslovne tajne, zadaću njihovoga čuvanja, te odlučivanja koje se osobe zaposlene u toj pravnoj osobi mogu ovlastiti za čuvanje poslovne tajne, odnosno kojim se osobama poslovna tajna može priopćiti. Podaci koji se smatraju poslovnom tajnom ne smiju se priopćavati niti činiti dostupnim neovlaštenim osobama, ako posebnim zakonom nije što drugo određeno. Poslovnu tajnu dužni su čuvati svi zaposlenici koji na bilo koji način saznaju za podatak koji se smatra poslovnom tajnom. Kad je to iz razloga obavljanja poslova pravne osobe nužno, podatke klasificirane kao poslovna tajna može drugim osobama priopćiti samo osoba ovlaštena općim aktom uz prethodnu pisanu suglasnost pravne osobe koja je sukladno svom općem aktu odredila da se ti podaci smatraju poslovnom tajnom i uz prethodnu pisanu suglasnost zainteresirane pravne ili fizičke osobe ako su u pitanju podaci iz ponuda za natječaj ili dražbu.[29]

U zahtjevu kojim se traži suglasnost za pristup klasificiranim poslovnim podacima mora se navesti:

1. koji su podaci u pitanju,
2. kojoj se osobi oni imaju priopćiti,
3. koja je osoba ovlaštena obaviti takvo priopćenje,
4. razlozi zbog kojih je priopćavanje nužno,
5. način na koji će se podaci priopćiti odnosno koristiti[30]

Odavanje i neovlašteno pribavljanje poslovne tajne regulirano je Kaznenim zakonom Republike Hrvatske. Članak 262. propisuje zatvorsku kaznu u trajanju od tri godine za osobu

[29] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 221
[30] Ibid., str 222

koja neovlašteno drugom priopći, preda ili na drugi način učini pristupačnim podatke koji su poslovna tajna kao i tko pribavlja takve podatke s ciljem da ih preda neovlaštenoj osobi. Međutim u stavku 3 navedenog članka Zakon propisuje da nema kaznenog djela ako je učinjeno djelo počinjeno u pretežito "javnom interesu". Ako je osoba koja je odala poslovnu tajnu sebi ili drugome pribavila znatnu imovinsku korist ili prouzročila znatnu štetu kaznit će se kaznom zatvora od 6 mjeseci do 5 godina.[31]

Prilikom uvođenja informacijske sigurnosti u odluci uprave bitno je i klasificirati podatke koji su bitni za poslovanje pravne osobe i definirati koje osobe i pod kojim uvjetima imaju pristup istima.

3.1.3. Zaštita intelektualnog vlasništva

Pod intelektualnim vlasništvom se smatra skup prava na proizvodima ljudskog uma kao nematerijalnim dobrima. Sa stajališta poslovnog subjekta intelektualno vlasništvo je nematerijalna imovina tvrtke kojoj se pridaje knjigovodstvena vrijednost i u koju se ulaže s ciljem ostvarenja što veće dobiti.[32] Kako je intelektualno vlasništvo danas postalo jedna od najvrednijih stavki u imovini poslovnog subjekta, potrebno ga je zaštititi od zlouporabe te njime planski upravljati.

Prava intelektualnog vlasništva u gospodarskom su kontekstu zakonsko sredstvo pomoću kojeg njihovi nositelji pretvaraju svoja intelektualna postignuća u trajne poslovne vrijednosti. Pravima intelektualnog vlasništva može se ostvariti povoljniji položaj na tržištu u odnosu na konkurenciju, te štititi svoje proizvode i usluge od neovlaštenog kopiranja, korištenja i krivotvorenja. Iskorištavanjem prava intelektualnog vlasništva gospodarstvenici mogu proširiti tržište na kojemu nastupaju i učvrstiti svoj marketinški položaj. Organiziranim upravljanjem intelektualnim vlasništvom može se postići bolja prepoznatljivost na ciljnim tržištima, poboljšati promet roba i usluga, te povećati dobit, a dugoročno i ukupna vrijednost poduzeća. Organizirano upravljanje intelektualnim vlasništvom donosi i druge prednosti poduzetniku, kao što su izbjegavanje kršenja tuđih prava, olakšani tehnološki razvoj,

[31] NN 118/18
[32] Mintas-Hodak Lj., Pravno okruženje poslovanja, Zagreb, 2010., str.:172-173.

inovativnost u poslovanju, dodatni prihodi od ustupanja licencija. Stjecanje, održavanje i provedba prava intelektualnog vlasništva zahtjeva (nerijetko značajna) materijalna sredstva.[33]

Intelektualno vlasništvo se dijeli na pravo industrijskog vlasništva, autorsko pravo i autorskom pravu srodna prava. Za intelektualno vlasništvo u Republici Hrvatskoj nadležan je Državni zavod za intelektualno vlasništvo, gdje se vrši i sama registracija intelektualnog vlasništva. Osim toga Državni zavod za intelektualno vlasništvo provodi propisane postupke za priznavanje svih oblika intelektualnog vlasništva, pruža usluge pretraživanja informacija iz te promiče zaštitu i poštivanje prava intelektualnog vlasništva.

Zaštita intelektualnog vlasništva u Republici Hrvatskoj je regulirana Zakonom o autorskom pravu i srodnim pravima, Zakonom o žigu, Pravilnikom o Žigu, Zakonom i Pravilnikom o industrijskom dizajnu, Zakonom i Pravilnikom o patentu, Zakonom o oznakama zemljopisnog podrijetla i oznakama izvornosti proizvoda i usluga te nizom podzakonskih akata.

Državni zavod za intelektualno vlasništvo Republike Hrvatske tijelo je državne uprave koje obavlja poslove iz područja zaštite prava intelektualnog vlasništva. Zavod provodi postupke za priznanje prava industrijskog vlasništva (patenti, žigovi, industrijski dizajn, oznake zemljopisnog podrijetla i oznake izvornosti, topografije poluvodičkih proizvoda), te se bavi pratećom stručnom i zakonodavnom djelatnošću.

Djelatnost Zavoda u zakonodavnom i stručnom dijelu uključuje i područje autorskog prava i srodnih prava. Osim zakonodavne i stručne djelatnosti te postupaka priznanja prava, važan dio djelovanja Zavoda predstavlja informacijska i servisna djelatnost iz područja intelektualnog vlasništva, te suradnja s ostalim institucijama za provedbu prava intelektualnog vlasništva i potporu inovacijskoj djelatnosti, kao i suradnja s gospodarskim i znanstvenoistraživačkim entitetima[34]

3.1.4. Privatna zaštita

U današnjici postoji sve više vlasnika poduzeća koji se trude da što bolje i potpunije zaštite svoju imovinu i svoje poduzeće. Trenutno je na snazi Zakon o privatnoj zaštiti koji

[33] Zlatović D., Intelektualno vlasništvo i marketing, Zagreb, 2010., str. 59.
[34] Ibid., str. 61.

uređuje način obavljanja djelatnosti privatne zaštite i propisuje uvjete i način rada za njeno obavljanje. S obzirom na to da građanima jamči određenu razinu zaštite od protupravnih radnja (zaštita života i tjelesnog integriteta, zaštitu imovine i sl.), privatna zaštita je dopuna poslovima sigurnosti što ih obavljaju nadležna tijela državne vlasti. Pravni subjekti koji obavljaju poslove privatne zaštite ne smiju u svome radu primjenjivati operativne metode i sredstva slične onima koje primjenjuje Ministarstvo unutarnjih poslova i druga tijela državne uprave. Sukladno Zakonu, tjelesnu zaštitu osoba i imovine, kao posao, obavlja zaštitar osobnom nazočnošću i zaštitnom aktivnošću, bez prevladavajuće uporabe tehničkih sredstava i naprava.[35] Tehnička zaštita, pak znači stvaranje tehničkih uvjeta za sprečavanje protupravnih radnja usmjerenih spram štićene osobe ili imovine.

Djelatnost privatne zaštite obavlja se tjelesnom i tehničkom zaštitom, odnosno kombiniranjem jednog i drugog zaštitnog oblika. Privatnu zaštitu mogu obavljati samo pravne osobe koje su za to registrirane u nadležnome trgovačkom sudu (osim tajnih društava), s tim da obrtnici bez ograničenja mogu obavljati poslove tehničke zaštite, a poslove tjelesne zaštite samo za vlastite potrebe.[36]

Poslovi koji se najčešće pojavljuju u djelatnosti privatne zaštite su:

1. osiguranje mirnih prosvjeda i javnih okupljanja
2. osiguranje stambenih i poslovnih prostora
3. neposrednu tjelesnu zaštitu osoba (tjelohranitelj)
4. zaštitu prirodnih dobara i okoliša
5. osiguranje i pratnju novca, vrijednosnih papira i dragocjenosti.[37]

Zakon je kategorizirao poslove privatne zaštite, ovisno o njihovoj složenosti i ovlastima osoba što ih te poslove obavljaju, u tri skupine: čuvari, zaštitari i zaštitari tehničari.

Zaštita imovine u smislu kontrole i nadzora pristupa najkarakterističniji je segment privatne zaštite koji se koristi u korporativnoj sigurnosti. Nadzor pristupa se najčešće izvodi kombinacijom nekoliko elementa tehničke zaštite i to sustavima protuprovale, sustavima kontrole pristupa te sustavima video nadzora. Integralna sigurnost koja je naziv za integraciju

[35] NN broj: 68/03, 31/10, 139/10
[36] NN broj: 68/03, 31/10, 139/10
[37] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 315.

navedenih sustava najčešća je pogreška prilikom uspostave korporativne sigurnosti. Ovisno o djelatnosti kojom se poduzeće bavi razine zaštite mogu varirati od slabe (nikakve) do naprednih sustava s biometrijskim prepoznavanjem. Za pojedine segmente odnosno poslovnog okruženja postoje strogi propisi s razinama zaštite koja ovise o mnogo parametara. Najbitnija stvar vezana uz sustave privatne zaštite je kvalitetan elaborat prosudbe ugroženosti s preporučenim mjerama zaštite. Pravilnikom o uvjetima i načinu provedbe tehničke zaštite jasno je određeno za koje objekte se prosudba ugroženosti mora raditi. Pretežno se to odnosi na novčarske institucije, kladionice, mjenjačnice odnosno za najrizičniju skupinu poslovnih subjekata koji imaju tijekom radnog vremena velik priliv i odljev financijskih sredstava odnosno gotovine. Elaborat posudbe ugroženosti može ukazati na potencijalne kritične točke i na koji način ih štititi. Trenutna praksa u Republici Hrvatskoj je da se pozicije detektora, kamera i ostalih elemenat tehničke zaštite određuju na licu mjesta odnosno na objektu koji se štiti. Propušta se prilika dubinske analize o kaznenim djelima koja su već bila na lokaciji ili u neposrednoj okolici te o načinu njhovog izvršenja. Tjelesna zaštita objekata propisana je za objekte visokog rizika (npr. banke). Sve više poduzeća angažira čuvarsku službu na ulazu u objekt kao preventivu mjeru. Bitne stvari koje trebamo razlikovati po pitanju tjelesne zaštite su ovlasti čuvara u odnosu na ovlasti zaštitara.

Ovlasti čuvara i zaštitara su središnji i najosjetljiviji dio zakona o privatnoj zaštiti, s obzirom da primjena ovlasti uvijek donekle ograničuje prava i slobode osoba prema kojima ih se primjenjuje. Ovlasti su u zakonu točno nabrojane, prema težini zadiranja u prava osoba prema kojima ih se primjenjuje, odnosno težini štetnih posljedica kakve primjenom ovlasti mogu nastati (od provjere identiteta do uporabe vatrenog oružja). Primjena je ovlasti čuvara i zaštitara, u pravilu ograničena na štićene objekte i prostore. Tako se još jednom jasno ističe razlika privatne zaštite, te ovlasti zaštitara, na jednoj i zaštite kakvu građanima jamči država posredstvom svoga represivnog aparata (policije) i policijskih ovlasti s druge strane. Primjena ovlasti mora biti razmjerna potrebi zbog koje se poduzima. Primjena ovlasti ne smije izazvati veće štetne posljedice od onih koje bi nastupile da čuvari i zaštitari nisu primijenili ovlasti.[38]

Poslovi privatne zaštite mogu se obavljati isključivo na temelju pisanog ugovora pravnih osoba registriranih za obavljanje poslova privatne zaštite osoba i imovine naručitelja. Zakon jasno definira prostor obavljanja poslova privatne zaštite: samo unutar štićenog objekta i oko štićene osobe, do granica prostora za čije su čuvanje zaduženi zaštitari i čuvari.

[38] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 318.

3.2. Zaštita

Segment zaštite koji je naveden kao zasebna cjelina spada u kategoriju koja se naziva sigurnost (eng. safety) . Sustav zaštite utječe na sustav korporativne sigurnosti u segmentu zakonske regulative koje se svaki poslodavac mora pridržavati. Kako bi se shvatila kompleksnost navedenog područja, navest će samo neke brojke kao primjer[39]:

- Zaštitu na radu uređuju 3 zakona i 4 izmjene i dopune zakona, 41 pravilnik i 15 izmjena i dopuna pravilnika,1 naputak i 1 uredba
- Zaštita od požara je regulirana jednim zakon, 33 pravilnikom i 6 izmjenama i dopunama pravilnika
- Zaštitu i spašavanje regulira 9 zakona i 25 izmjena i dopuna zakona, 25 pravilnika i 24 izmjene i dopune pravilnika, 13 uredbi, 1 plan, 1 metodologija
- Zaštita okoliša i održivo gospodarenje otpadom je uređena sa četiri zakona i tri izmjene i dopune zakona, 40 pravilnika i 17 izmjena i dopuna pravilnika, 32 uredbe, 11 odluka, 4 naputka, 7 planova, jednom strategijom

Kada se napravi rekapitulacija segmenta zaštite, dobije se ukupno 322 dokumenta.

Stručnost i osposobljenost djelatnika koji se bave poslovima po navedenim segmentima je osnovni preduvjet za kvalitetno rješavanje zadataka iz pojedinih područja. Segment zaštite za razliku od ostalih navedenih područja ima stroge i učestale inspekcijske nadzore. U većini slučajeva poslodavci za područja zaštite na radu, zaštite od požara i zaštite okoliša koriste usluge vanjskih tvrtki specijaliziranih za određena područja. Ovaj način je poslovanja je većini idealno rješenje jer se netko drugi brine o "suvišnim" papirima, no tu nastaje drugi problem, koji je vidljuv na primjeru zaštite na radu. Za izradu procjene rizika za neko radno mjesto vanjskoj tvrtki se moraju dostaviti opis radnog mjesta, tehničke i fizikalne uvjete rada, nabrojati s kojim je sve opasnostima djelatnik okružen. Uz to, otrebno je dostaviti i opće liječničko uvjerenje o zdravstvenoj sposobnosti djelatnika. Dakle, osim što se daju nekome poslovni podaci o radnom procesu u npr. proizvodnji, daju se i osobni podaci djelatnika koji se temeljem zakona o zaštiti osobnih podataka ne bi trebali biti baš tako distribuirati. Naravno, postoji ugovor o zaštiti i tajnosti podataka, ali kada su podaci već izvan tvrtke teško je dokazati od kuda su zapravo došli. U svakoj procjeni rizika mora se raditi i ispitivanje

[39] http://www.pravnadatoteka.hr/hrv/index.asp, 20.ožujka.2019.

radnog okoliša na kojem svaki djelatnik radi. Nadalje ispitivanje strojeva i opreme za rad je također sastavni dio procjene rizika gdje svaki uređaj koji se ispituje mora biti označen: proizvođačem, oznakom, serijskim brojem. Navedeni podaci su potrebni za izradu pravilnika o radu na siguran način.

Na osnovi prikupljenih podataka lako se može složiti poslovni proces proizvodnje nečega. A detalji o materijalu i tehnologiji mogu se saznati i drugim putem. Naj kompleksniji segment je potencijalno najveća rupa za curenje informacija. Stoga segment zaštite treba biti pod segmentom korporativne sigurnosti u smislu protoka i distribucije informacija

3.2.1. Zaštita na radu

Zaštita na radu je skup tehničkih, zdravstvenih, pravnih, socijalnih i drugih mjera i aktivnosti kojima je svrha spriječiti i otkloniti opasnosti i štetnosti koje mogu ugroziti zdravlje i život osoba na radu. Ozljede na radu i profesionalne bolesti nanose štetu radniku, njegovoj obitelji, ali i poslodavcu i cjelokupnoj društvenoj zajednici. Iz tog razloga zaštita na radu provodi se kao organizirana djelatnost sa svrhom osiguranja uvjeta rada u kojima neće postojati opasnosti za zdravlje i život, odnosno uvjete u kojima će te opasnosti biti smanjene na najmanju moguću mjeru.[40]

U današnje vrijeme još uvijek postoje poslodavci koji zaštitu na radu ne percipiraju kao sastavni dio poduzeća i izvođenja procesa rada te dugoročno ulaganje, već to smatraju dodatnim troškom. S druge strane ipak se postupno povećava broj poslodavaca koji su potpuno svjesni važnosti zaštite sigurnosti i zdravlja na radu, unatoč troškovima koji nastaju zbog poboljšanja radnog okruţenja.

Zaštita na radu sastavni je dio organizacije rada i izvođenja radnog procesa, koja se ostvaruje obavljanjem poslova zaštite na radu i primjenom propisanih, ugovorenih i priznatih pravila zaštite na radu, te naređenih mjera i uputa poslodavca.

Zakon o zaštiti na radu je temeljni propis koji u hrvatskom zakonodavstvu uređuje prava, obveze i odgovornosti u vezi zaštite na radu. Prava, obveze i odgovornosti u vezi zaštite na radu uređuju se izravno i neizravno propisima radnog zakonodavstva, propisima mirovinskog osiguranja, propisima zdravstvenog osiguranja i zdravstvene zaštite te tehničkim i drugim propisima kojima se štite sigurnost i zdravlje osoba na radu.

[40] Puljić N., Zaštita na radu, Zagreb 2006., str.6

Poslodavac je odgovoran za organizaciju i provedbu zaštite na radu u svim radnim procesima i dijelovima poduzeća. Odgovornost poslodavca ne može se umanjiti niti isključiti neovisno o tome je li organiziranje provedbe zaštite na radu ustrojio na način da je odredio radnika za obavljanje aktivnosti zaštite na radu ili je ugovorio suradnju s pravnom osobom ovlaštenom za obavljanje poslova zaštite na radu. Primjena pravila zaštite na radu i mjera zdravstvene zaštite ne smije predstavljati nikakve troškove za zaposlenike, a svako traženje poslodavca da radnik sudjeluje u troškovima provođenja zaštite na radu je prekršaj. Poslodavac odgovara radniku za štetu uzrokovanu ozljedom na radu, profesionalnom bolešću ili bolešću vezanom uz rad po načelu objektivne odgovornosti, na koju utječu propisane obveze zaposlenika u području sigurnosti i zdravlja na radu. Uz iznimku poslodavac se može osloboditi odgovornosti prema općim propisima obveznog prava, ako je riječ o događajima nastalih zbog nepredvidivih okolnosti na koje poslodavac nije mogao utjecati.[41]

Poslodavac je obvezan inspektoru rada na njegov zahtjev dati obavijest i podatke koji su mu potrebni u obavljanju nadzora. Za vrijeme obavljanja nadzora poslodavac je dužan inspektoru rada dati na uvid potrebne isprave i omogućiti utvrđivanje činjenica, koje su mu potrebne radi donošenja ocijene je li postupano u skladu s propisima o zaštiti na radu. Poslodavac ima obvezu izvijestiti inspekciju rada o svakoj smrtnoj, težoj ili skupnoj ozljedi i to odmah po nastanku događaja, a u roku od 48 sati od nastanka događaja dužan je inspekciji rada dostaviti propisano pisano izvješće.

Zakon o zaštiti na radu obvezuje poslodavca na čuvanje određene dokumentacije, vođenje odgovarajućih evidencija, vođenje knjiga nadzora i podnošenje odgovarajućih izvješća. Te obveze odnose se na sva mjesta rada poslodavca. Način vođenja evidencija iz područja zaštite na radu, sadržaj i način vođenja knjige nadzora i način podnošenja izvješća propisani su Pravilnikom o evidenciji, ispravama, izvještajima i knjizi nadzora iz područja zaštite na radu.[42]

Inspekcijski nadzor nad provedbom Zakona o zaštiti na radu i propisa donesenih na temelju zakona obavljaju inspektori rada Državnog inspektorata. U provedbi inspekcijskog nadzora u području zaštite na radu inspektor rada ovlašten je u skladu s utvrđenim činjeničnim stanjem donijeti slijedeća rješenja:

- rješenje o privremenoj zabrani korištenja sredstava rada, prostora ili instalacija

[41] Ibid., str.6.
[42] NN broj: 52/84

- rješenje o zabrani određenog načina postupanja

- rješenje kojim naređuje poslodavcu da zaposlenika privremeno udalji s obavljanja poslova, u slučajevima kada utvrdi da su izravno ugroženi život ili zdravlje zaposlenika ili drugih osoba[43]

U slučaju da inspektor utvrdi da postoje nedostaci u primjeni propisa zaštite na radu, ali da oni kao takvi ne utječu štetno na život i zdravlje zaposlenika i drugih osoba u prostoru, te da se oni mogu otkloniti u roku od trideset dana, izdat će rješenje o otklanjanju nedostataka

Do inspekcijskog nadzora može doći na temelju prijave pravnih ili fizičkih osoba, na temelju naloga rukovodeće strukture unutar Državnog inspektorata ili postupanjem inspektora prema planu rada.[44]

3.2.2. Zaštita od požara

Svaka tvrtka koja želi preventivnu zaštitu od požara će posvetiti veliku važnost organizacijskim i tehničkim mjerama i radnjama usmjerenim na uklanjanje opasnosti od nastanka požara, rano otkrivanje požara i njegovo učinkovito gašenje. Sustav zaštite od požara obuhvaća planiranje zaštite od požara, provođenje mjera zaštite od požara, financiranje zaštite te osposobljavanje za obavljanje poslova zaštite od požara. Glavni cilj je zaštititi život, zdravlje i sigurnost ljudi, te sigurnost materijalnih dobara, okoliša i prirode od požara, uz prihvatljiv požarni rizik. Sustav zaštite od požara u Republici Hrvatskoj uređen je Zakonom o zaštiti od požara,[45] a zaštita od požara zakonom je utvrđena kao djelatnost od posebnog interesa za Republiku Hrvatsku. Zaštitu od požara provode fizičke i pravne osobe utvrđene zakonom o zaštiti od požara i pravne osobe i udruge koje obavljaju vatrogasnu djelatnost.

Svaka fizička i pravna osoba mora djelovati na način kojim se požar ne može izazvati i mora provoditi mjere zaštite od požara utvrđene Zakonom o zaštiti od požara i propisima donesenim na temelju tog zakona. Također je svaka osoba odgovorna za neprovođenje mjera zaštite od požara, izazivanje poţara i sve posljedice koje bi iz toga mogle nastati. Svatko ima pravo, ali i obvezu biti upoznat s opasnostima od požara na mjestu gdje radi ili boravi. Odluku o planu i programu te načinu upoznavanja s opasnostima od požara donose pravne osobe na

[43] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str.300.
[44] Puljić N., Sigurnost i zaštita zdravlja na radu, Zagreb, 2009., str. 203.
[45] NN broj: 92/10

svom vlasništvu. Kako bi se pravovremeno i učinkovito osigurala zaštita od požara pravne osobe organiziraju osposobljavanje zaposlenika za provedbu preventivnih mjera zaštite od požara, gašenje požara i spašavanje ljudi i imovine ugroženih požarom. Djelatnici službe za zaštitu od požara moraju imati odgovarajuće obrazovanje, ovisno o poslovima koje obavljaju i položen stručni ispit u području zaštite od požara. Program, uvjeti i način polaganja propisani su Pravilnikom i stručnim ispitima u području zaštite od požara.[46] Fizičke i pravne osobe osiguravaju financijska sredstva za provedbu zaštite od požara prema vlastitim planovima.

3.2.3. Zaštita okoliša

Svaka ljudska djelatnost u većoj ili manjoj mjeri utječe na okoliš, pri čemu zagađivači nisu samo velike multinacionalne kompanije, već i srednja i mala poduzeća različitim aktivnostima znatno utječu na štetno djelovanje okoliša. Svako poduzeće može smanjiti svoj negativan utjecaj na okoliš na način da smanji ispuštanje štetnih tvari, smanjenje količine proizvedenog otpada i racionalnije korištenje skupih i neobnovljivih resursa. S obzirom na porast svijesti o važnosti smanjenja i kontroliranja utjecaja na okoliš, kao i činjenicu da uspostavljanje sustava upravljanja zaštitom okoliša postalo sastavni dio društveno odgovornog poslovanja, nužno je upoznati se s važećom zakonskom regulativom ovog područja.

Zakon o zaštiti okoliša uređuje između ostalog načela zaštite okoliša i održivog razvoja, zaštitu sastavnica okoliša i zaštitu okoliša od utjecaja opterećenja, subjekte zaštite okoliša, dokumente održivog razvoja i zaštite okoliša, instrumente zaštite okoliša, odgovornost za štetu i druga pitanja od značaja za zaštitu okoliša.

Subjekti zaštite okoliša održavaju razvoj i zaštitu okoliša, u Republici Hrvatskoj to su:

- Hrvatski sabor
- Vlada Republike Hrvatske
- Ministarstva i druga nadležna tijela državne uprave
- Županije i Grad Zagreb, te ostali gradovi i općine
- Agencija za zaštitu okoliša

[46] NN broj 40/94, 55/94 i 89/01

- Fond za zaštitu okoliša i energetsku učinkovitost
- Pravne osobe s javnim ovlastima
- Pravne i fizičke osobe odgovorne za onečišćavanje okoliša
- Druge pravne i fizičke osobe koje obavljaju gospodarsku djelatnost
- Udruge civilnog društva koje djeluju na području zaštite okoliša
- Građani kao pojedinci, njihove skupine, udruge i organizacije[47]

Informacijski sustav zaštite okoliša uspostavljen je sa svrhom cjelovitog upravljanja zaštitom okoliša, te u svrhu izrade i praćenja provedbe dokumenata održivog razvoja i zaštite okoliša. On sadrži podatke i informacije o stanju okoliša, opterećenjima i utjecajima na okoliš, te odgovorima društva. Nadležno upravno tijelo u županiji vodi registar onečišćavanja okoliša.[48] Registar je skup podataka o izvorima, vrsti, količini, načinu i mjestu ispuštanja, prijenosa i odlaganja onečišćujućih tvari i otpada u okoliš. Tijelo javne vlasti dužno je osigurati pristup informacijama o okolišu koje posjeduje u skladu sa Zakonom o zaštiti okoliša, uz odgovarajuću primjenu posebnih propisa kojima se uređuje pravo javnosti na pristup informacijama.

Poduzeće koje obavlja djelatnost koja predstavlja rizik za okoliš i za ljudsko zdravlje, odgovara za štetu u okolišu i prijeteću opasnost od štete, osim ako dokaže da opasna djelatnost nije bila uzrok štete u okolišu. Poduzeće za prouzročenu štetu odgovara po načelu objektivne odgovornosti (uzročnosti). Poduzeće je dužno u utvrđenom roku izraditi sanacijski program za uklanjanje štete u okolišu koja je nastala zbog prekoračenja graničnih vrijednosti emisija u skladu s posebnim propisom. Operater tvrtke obvezan je osiguranjem kod osiguravatelja u skladu sa zakonom osigurati raspoloživa sredstva za naknadu štete koja bi mogla biti nanesena okolišu, odnosno za otklanjanje prijeteće opasnosti od štete.[49]

Inspekcijski nadzor nad primjenom Zakona o zaštiti okoliša i propisa donesenih na temelju zakona provode državni službenici ministarstva nadležnog za zaštitu okoliša. Inspekcijski nadzor u području okoliša provode i druge inspekcije nadležne prema posebnim propisima za nadzor pojedinih sastavnica okoliša i zaštite od utjecaja opterećenja na okoliš.

[47] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str.324.
[48] Ibid., str. 325.
[49] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str.326.

U inspekcijskom nadzoru inspektor nadzire osobe koje su obavezne provoditi mjere i aktivnosti zaštite okoliša, te ispunjavanje i način rada nadziranih osoba, obavlja izravan uvid u opće i pojedinačne akte, te poduzima mjere određene Zakonom i propisima donesenim na temelju Zakona o zaštiti okoliša.

U provedbi inspekcijskog nadzora inspektor može na licu mjesta zatvoriti prostorije i pristup prostoru u kojima nadzirana osoba obavlja određenu djelatnost i onemogućiti joj korištenje postrojenja i opreme pečaćenjem.[50]

3.3. Struktura odjela korporativne sigurnosti

Struktura odjela korporativne sigurnosti ovisi o veličini poduzeća. Kako bi se odredio ukupni broj djelatnika, važno je znati kako ih rasporediti na odgovarajuća radna mjesta. Osnovna stvar svakog odjela za korporativnu sigurnost je voditelj takvog odjela (eng. CSO = Chief Security Officer). U hijerarhijskoj strukturi tvrtke voditelj odjela za korporativnu sigurnost odgovara direktno upravi društva. On mora imati ovlasti za implementaciju, provedbu i nadzor nad svim segmentima sigurnosti društva. Isto tako mora imati ovlasti za provedbu direktnog nadzora poslovnih procesa bez mogućnosti direktne promjene u njima. Također bitna stvar je da uz opravdani razlog može privremeno udaljiti djelatnika s radnog mjesta i zatražiti/započeti internu ili vanjsku istragu o sumnjivim aktivnostima za koje smatra da su prijetnja tvrtki. Razloge svojih postupaka mora pismeno obrazložiti i navesti indicije ili predočiti dokaze na osnovi kojih je nešto učinio.[51] U svijetu je praksa da voditelj odjela korporativne sigurnosti donosi planove i procedure zaštite osoba (uprave) i objekata u kojima se odvijaju poslovni procesi. Voditelj odjela za sigurnost definira i nadzire sve razine fizičke i tehničke zaštite osoba i objekta sukladno pozitivnim zakonskim propisima i ovlastima.

Druga obavezna osoba u strukturi odjela za korporativnu sigurnost je voditelj odjela (pododjela) za informacijsku sigurnost (eng. CISO = Chief Information Security Officer). Osnovna zadaća voditelja za informacijsku sigurnost je donošenje, implementacija i nadzor nad pristupom i distribucijom poslovnih informacija. Voditelj odjela za informacijsku sigurnosti u suradnji s voditeljem odjela za sigurnost te upravom nekog društva dužan je

[50] Ibid, str. 326.
[51] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str.226.

odrediti: razine pristupa podacima, tko i pod kojim uvjetima im može pristupiti te na koji način se oni distribuiraju.[52]

Osoba zadužena za zaštitu na radu (ovisno o veličini poslovnog subjekta i zakonskim propisima određuje se i njegova stručnost koja može biti stručnjak zaštite na radu ili Specijalist zaštite na radu). Svrha internog stručnjaka ili specijalista zaštite na radu osim segmenta posla vezanog uz vođenje zaštite na radu bi bila i zaštita pristupa podacima trećim osobama što sam naveo u segmentu zaštite. Ako se gledaju ekonomski uvijeti, ista osoba tehnički bi mogla i obavljati poslove vezane uz zaštitu okoliša zbog povezanosti zakonskih područja.

Sljedeća osoba od važnosti je osoba za zaštitu od požara. Djelatnik mora imati položen državni stručni ispit za zaštitu od požara (sukladno broju ljudi i namjeni objekta stupanj osposobljavanja je definiran zakonom i pripadjućim pravilnikom). Također bi ista osoba mogla biti zadužena za poslove zaštite i spašavanja.

Zakon o zaštiti osobnih podataka propisuje da poslodavac mora imati osobu imenovanu kao voditelja zbirke osobnih podataka. Djelatnik koji bi obavljao poslove voditelja zbirke bi mogao biti pravne struke koji bi osim poslova voditelja zbirke osobnih podatak mogao biti pravna pomoć odjelu po pitanju promjena zakonskih obveza za navedena područja.

Za oodjel korporativne sigurnosti minimalno je potrebno 5 stručnih i kvalificiranih djelatnika.

4. IDENTIFIKACIJA KRITIČNIH TOČAKA

Osnovna točka za uspostavu korporativne sigurnosti u nekom poduzeću je određivanje objekta kojeg trebamo štititi. Osobno smatram da je za sva poduzeća najbitnija stvar za štićenje - podatak. Svako poduzeće ima različite tipove podataka, neki se odnose na osobne podatke klijenata i njihove navike zatim podaci o cijenama nekih usluga ili robe na tržištu te zadnji i u segmentima proizvodnje najbitniji podatci su specifikacije materijala za određene proizvode te način njihove izrade odnosno proizvodnje.

[52] Ibid., str.226.

Prvi primjer su trgovine gdje većina trgovačkih centara putem raznih kartica za sakupljanje bodova, ostvarivanje popusta stvara točnu sliku o navikama svojih kupaca i na osnovi tih podataka može im ponuditi točno određenu stvar. Gubitak takve baze podataka značio bi tržišnu prednost nekom drugom tko bi do takvih podataka došao.

Drugi primjer su financijske ustanove gdje kroz financijske transakcije svojih klijenata, npr. banke, mogu ponuditi dodatne usluge i financijski obvezati klijente da ne promjene banku. Isto tako mogu im ponuditi različite pogodnosti da ih zadrže što možemo vidjeti u obliku poklona, kupona s popustima kod njihovih poslovnih partnera.

Treći primjer su proizvođači kojima su bitni podatci tehnologija proizvodnje, sastav materijala, nabavne cijene gubitak takvih podataka jednak je gubitku tržišne pozicije.

Dakle zajednička štićena stvar za sve vidove poslovanja je podatak. S podatcima upravljaju ljudi i računala na kojima su pohranjeni. Što znači da korporativnu sigurnost nekog poduzeća mogu ugroziti dva slučaja:

- ljudska pogreška nastala neznanjem, propustom, namjerom

- tehnički kvar nastao prirodnom nepogodom, neznanjem, propustom i namjerno[53]

Dubljom analizom se može objasniti svaka od navedenih pogrešaka i kvarova, kako nastaju, kako iste možemo spriječiti te koje su posljedice ako ih ignoriramo. Bitna stvar je da na sve incidentne situacije treba reagirati i istražiti koji su pravi uzroci.

4.1. Ljudska pogreška

Ljudska pogreška, kao što je već navedeno, dolazi neznanjem, propustom (nemarom) ili namjerno. Sva tri načina imaju jednaku težinu jer rezultat curenja podataka na bilo koji od navedenih načina može imati ozbiljne posljedice za poslodavca. Kategoriziranje težine ljudske pogreške je dosta nezahvalno jer šteta je počinjena. Bitni su odnosi u kojima je do pogreške došlo.

[53] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011., str. 327.

Informiranost i upoznavanje djelatnika s pravilima i posljedicama ako dođe do "curenja" informacija mora biti primarni cilj odjela za korporativnu sigurnost. Ako se slijede pripremni koraci i ako se jasno definira svrha, doseg, pravila za korištenje te poznavanje mogućih sankcija, može se smatrati da do neznanja ne može doći. Bitna stvar je da su djelatnici upoznati sa obvezama po pitanju pravilnika te da se dobije od njih pisana izjava da su upoznati s pravilnicima, da su im objašnjeni i da su upoznati s posljedicama nepridržavanja. Ako sve to postoji, onda se bilo kakav propust ne može pravdati kao neznanje. Ključna stvar je informiranost djelatnika.[54]

Pogreška učinjena propustom (nemarom) je najčešći oblik ljudske pogreške. U najsređenijim sustavima dogodi se da korisnik zaboravi na što je upozoren. U svrhu smanjenja ovakvog tipa pogrešaka bitno je kontinuirana komunikacija između odjela za informacijsku sigurnost i djelatnika. Dobar primjer komunikacije između odjela za korporativnu sigurnost i djelatnika poduzeća je kada jednom mjesečno djelatnici na svoj mail dobiju kratki sažetak u vidu podsjetnika što je bitno iz domene korporativne sigurnosti, čega se moraju prisjetiti i kako postupati. Uz mail je uključena opcija da su mail primili i pročitali. Tako se način kontinuirano podsjeća djelatnike na njihove obveze i ne može doći do propusta odnosno nemara

Namjerno učinjena pogreška je najteži oblik pogreške. Bitna stvar za utvrditi kod ovakvih pogrešaka je kako i zašto je do nje došlo. Je li se moglo to spriječiti, je li odjel za informacijsku sigurnost mogao nešto učiniti da se to spriječi. Ako je došlo do zloupotrebe ovlasti i prava, odnosno korisnik s višom razinom pristupa je iskoristio tu mogućnost da dođe do podataka za pribavljanje sebi ili nekom drugom materijalne ili bilo kakve koristi. U tom slučaju govorimo o kaznenom djelu. Bitna stvar za razlikovanje je li pogrešku učinio djelatnik ili administrator sustava. Za sva prava i razine pristupa koje definira uprava za sve djelatnike bitno je da nakon što se ovlasti dodjele potrebno je i provjeriti da li su prava primijenjena na korisnike sa točno određenim razinama pristupa ili je došlo do propusta sa strane odjela za informacijsku sigurnost.[55] Zbog ovakvih slučajeva bitno je kvalitetno odrediti razine pristupa za sve korisnike. Ni jedan korisnik osim najviše razine uprave ne bi smio imati pristup do svih poslovnih dokumenata u tu zabranu uključeni su i voditelj odjela korporativne sigurnosti te voditelj odjela informacijske sigurnosti.

[54] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 327.
[55] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 327.

4.2. Tehnički kvar

Tehnički najčešće nastaje: prirodnom nepogodom, neznanjem, propustom (nemarom) ili namjerno. Mogućnost tehničke pogreške svodi se na minimum, međutim uvijek postoji rizik da nešto pođe po zlu.

4.2.1. Tehnički kvarovi nastali prirodnom nepogodom

Kako bi se pripremilo na ovu vrstu kvarova, moraju se imati resursi koji omogućavaju relativno brzi nastavak poslovanja na istoj ili nekoj drugoj lokaciji. Prirodne nepogode se ne mogu predvidjeti, a pogotovo njihov razmjer i trajanje. Ono što bi svaka tvrtka kojoj je ključan faktor vremena uspostave ponovne funkcionalnosti i operativnosti trebala imati je kvalitetna sustav pohrane kritičnih podataka. Postoji nekoliko pravila po pitanju smještaja računala - servera na kojima se nalazi pričuvna kopija podataka.[56] Ako je moguće smještaj centralnog i računala za pohranu podataka ne bi smio biti u podrumu ili prizemlju objekta. Smještajem centralne opreme na više katove eliminiramo mogućnost da poplava ili iznenadna velika količina oborinskih voda ugrozi rad opreme. No tu dolazi do jednog previda. Servere i opremu smjestimo na više katove ali sustav besprekidnog akumulatorskog napajanja ili agregat ostavimo u podrumu ili prizemlju. Uslijed prodora vode može doći do naponskog uništenja opreme. Ako je moguće barem besprekidno akumulatorsko napajanje staviti na istu etažu gdje se nalazi i centralni sustav. Ako poduzeće raspolaže sa više lokacija idealno mjesto za smještaj pričuvnog podatkovnog centra bi bio na drugoj tektonskoj ploči, čime bi se izbjeglo oštećenje podataka uslijed potresa. Kvalitetne veze između lokacija ključne su za uspostavu funkcionalnosti u kratkom vremenskom roku.

4.2.2. Tehnički kvarovi nastali propustom (nemarom)

Propust ili nemar kao tehnički kvar najviše se odražava na odjel informacijske sigurnosti i informatički odjel tvrtke. Sve operativne sustave i korisničke aplikacije prema preporukama proizvođača (autor) potrebno ih je ažurirati. Naj češće se problemi javljaju kada se operativni sustavi na ažuriraju sa sigurnosnim zakrpama koje utječu na njihovu ranjivost. Svi sustavi koji imaju poslovnu svrhu moraju se redovito održavati i nadograđivati. Do propusta može doći i

[56] Ibid., str.328.

pogreškom djelatnika. To se odnosi na korespondenciju elektroničkom poštom kada zbog nemara i ignoriranja sigurnosnih politika djelatnici upotrebljavaju računalni sustav tvrtke za osobne potrebe u jednom slučaju i u drugom slučaju koji je u zadnje vrijeme sve češći ciljanim virusnim napadom na tvrtke od kojih se traži otkupnina za povrat podataka.[57] Zadnje navedeni slučajevi se u velikoj većini slučajeva ne mogu predvidjeti jer sustavi zaštite računalnih sustava ne prepoznaju napad kao takav odnosno tek nakon što virus zarazi računalo dobiju informaciju što se događa. Zbog toga je bitna kvalitetna tehnička podrška sustavima korporativne sigurnosti.

4.2.3. Tehnički kvarovi nastali namjerno

Tehnički kvarovi koji su nastali namjerno predstavljaju tešku povredu radnih obveza. Najčešći krivci za ovakve kvarove su administratori sustava i djelatnici s višim razinama pristupa. Administratori sustava u većini slučajeva ostavljaju si "stražnji" ulaz za pristup podacima. Najčešća opravdanja su brzi pristup podacima na zahtjev pojedinog djelatnika, voditelja ili direktora. Naknadnom analizom se onda može utvrditi kako nisu poštivane mjere zaštite pristupa podacima.[58] U svakom poduzeću bez obzira na djelatnost se pronađe neki "haker" koji gleda što postoji u računalnom okruženju i kako se može doći do nekih podataka. Najtraženiji podaci su podaci o plaćama djelatnika, administratorske šifre za ulazak u druge sustave, privatni podaci o djelatnicima. Druga skupina koja izaziva namjerne tehničke kvarove najčešće spada u grupu srednjeg menadžmenta koji nemaju velike ovlasti, ali ipak imaju moć da se s njihovih prijenosnih računala skinu sigurnosne mjere iz nekih izmišljenih razloga. Rezultati su poražavajući, prijenosna računala spojena na internet bez segmenta zaštite najčešće pokupe nekakav virus i nakon što se spoje na računalnu mrežu u poduzeću prošire virus na ostale sustave.

Pravila informacijske sigurnosti po tehničkim pitanjima moraju se poštivati na svim razinama bez izuzetaka. Svaki izuzetak potencijalna je prijetnja sustavu i kao takva može nanijeti veliku štetu. Iako se korisnici sustava teško privikavaju na nova ograničenja i zabrane ona se moraju dosljedno provoditi samo tako možemo reći da imamo siguran sustav poslovanja.

[57] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Zagreb, 2011. str. 330.
[58] Ibid., str.330.

5. ZAKLJUČAK

Od trenutka stvaranja sustava korporativne sigurnosti, preko njegovog razvoja, primjene i održavanja potrebno je učiti korisnike kako se ponašati u računalnom okruženju, koje su vrijednosti posla te da štiteći poslovno okruženj zapravo se štiti radno mjesto i egzistencija. U sustavima korporativne sigurnosti nema mjesta popuštanju pod pritiscima i nema iznimki. Pravila propisana sustavom nisu napisana da ih se krši već da ih se striktno pridržava. Egzistencija poduzeća ovisi o pravilima korporativne sigurnosti. Svaki propust ili nepredviđeni događaj može oslabiti ili uništiti poziciju tvrtke na tržištu. Svaki podatak koji napusti tvrtku mora imati razlog zašto ga je napustio i tko je to odobrio.

Sama korporativna sigurnost ponekad sadrži rizik da postane teret, a ne koristan instrument. U najgorem se slučaju može ostvariti kao trošak u proračunu tvrtke koji ne doprinosi operativnoj dobiti tvrtke. Zbog toga se postavlja razumno pitanje: zašto bi tvrtka trebala i dalje razvijati korporativnu sigurnost, a ne prihvatiti trenutnu razinu? Korporacije imaju različite potrebe za korporativnom sigurnošću, a ključno je postaviti ciljanu razinu kako bi se stvorio uspješan sustav upravljanja sigurnošću. Tvrtke koje odlučuju biti zadovoljne s trenutnom situacijom ne postupaju ispravno i riskiraju cjelokupno poslovanje i egzistenciju. Srećom, danas se sve više povećava broj poduzeća koja su potpuno svjesna važnosti osiguravanja rada na siguran način za zaposlenika i poslodavca, a to postižu primjenom mjera i radnji iz područja zaštite na radu, zaštite od požara, zaštite okoliša i ostalih područja koja su obrađena u radu.

Ono na što bi sva poduzeća trebala obratiti pažnju je da nije dovoljno samo uspostaviti sustav korporativne sigurnosti, već uz puno stručnosti se treba dalje nadograđivati i prilagođavati novim tehnologijama i vremenima koja dolaze. Sustav nije moguće realizirati preko noći, već je potrebna uska suradnja Uprave i odjela za korporativnu sigurnost da se zaštite sve vrijednosti koje je neko poduzeće stvorilo ili ga tek stvara.

POPIS LITERATURE

Knjige:

- Bilandžić M., Poslovno-obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb, 2008.

- Ivandić Vidović, Karlović L, Ostojić A., Korporativna sigurnost, U.H.M.S, Zagreb, 2011.

- Javorović B., Bilandžić, M., Poslovne informacije i business intelligence, Golden marketing -Tehnička knjiga, Zagreb, 2007.

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

- Mintas-Hodak Lj., Pravno okruženje poslovanja, Mate d.o.o., Zagreb, 2010.

- Puljić N., Sigurnost i zaštita zdravlja na radu, Poslovni zbornik, Zagreb, 2009.

- Veić P., Nađ I., Zakon o privatnoj zaštiti s komentarom, Nalada Žagar, Rijeka, 2005.

- Zlatović D., Intelektualno vlasništvo i marketing, INMAG, Zagreb, 2010.

Internet izvori:

- Advisera, dostupno na https://advisera.com/27001academy/hr/sto-je-iso-27001/

- Digitalna komora, dostupno na https://digitalnakomora.hr/hr

- EUR-Lex, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/

- Ministarstvo unutarnjih poslova, dostupno na http://www.mup.hr/1063.aspx,

- Pravna datoteka, dostupno na: http://www.pravnadatoteka.hr/hrv/index.asp

- Poslovni.hr, dostupno na: http://www.data-link.hr/uploads/poslovnihr-11-22-03.pdf