UDK 334.728:351.759.4/.5
DOI 10.7251/ZREMP1601187T

DRUŠTVENI ZNAČAJ KORPORATIVNE BEZBEDNOSTI

THE SOCIAL IMPORTANCE OF CORPORATE SECURITY

Duško Tomić, Marlema Milićević

Sažetak

„Bolest počinje sa osetljivim stanjem tela koje može biti izazvano naslednim faktorima ili nezdravim ponašanjem – krizna žarišta u korporacijama se javljaju u sektorima gde je loše upravljanje. Faza inkubacije nastupa kada se patogeni elementi namnože i nastane – zanemarivanje na izgled bezazlenih problema. Kada dostignu izvestan prag, patogeni elementi savlađuju odbrambeni sistem tela i čine da se pacijent oseća bolesnim – eskalacija krize. Bolest se ispolji i bitka za oporavak ili preživljavanje može da počne."

Isto je tako i u korporacijama, zanemarivanje problema u administraciji ili tehničkom obezbeđenju korporacije i danas u XXI veku kao glavni problem zaštita podataka, slaba zaštita servera u korporacijama omogućavaju sajber napade na istu – akcije koje se preduzimaju kako bi se stekla informaciona superiornost kao podrška poslovnim strategijama korporacije – korak ispred. Bitka za konkurenciju uvek traje.

Neke korporacije pate od izopačenja racionalnog plana. Savremene korporacije u zapadnom društvu pristupaju racionalno-naučnom pristupu upravljanja. Njihov racionalni sistem razmišljanja svodi se na izračunavanje rizika i iscrtavanje mogućih puteva neuspeha razvijanjem procedura za detektovanje abnormalnih obrazaca koji ipak u velikoj meri vode ka neuspehu i krizama. Zašto se to dešava? Nemoguće je predvideti kakva će kriza nastupiti.

Racionalno -naučni pristup vodi ka lažnom osećaju sigurnosti, opisivanjem svih tih mogućih uzroka kriza, iscrtavanjem puteva neuspeha i dodeljivanjem kvatifikovanog faktora rizika svakom scenariju. Ako nastupi žarište – rizik koji je jako mali postaje prihvatljiv i zanemaruje se, jer ljudi su skloni da zaborave da rizici - ma kako mali – zaista se mogu ostvariti. „Normalizacija rizika" često dovodi do shvatanja koje se sve češće sreće: „to se neće ovde dogoditi", a kada kriza nastupi, svi ostanu zapanjeni.

Ključne reči: Korporacija, bezbednost, konkurencija, rizik
JEL klasifikacija: *M14*

Abstract:

"The disease begins with a delicate state of the body that may be caused by hereditary factors or unhealthy behaviors – trouble spots in corporations occur in sectors with poor management. The incubation phase occurs when pathogens multiply and dwell – the neglection of seemingly harmless problems. When they reach a certain threshold, the pathogens defeat the defense system of the body and make the patient feel sick – the escalation of the crisis. The disease is manifested and the battle for the survival or recovery can begin."

It is the same in corporations, ignoring problems in the administration or technical security, and especially nowadays in the XXI century when the main problem is data protection, the weak

protection of servers in corporations allow cyber attacks on the data protection – actions that are undertaken in order to gain information superiority in support of business strategies of corporation – one step ahead. The battle for the competitive advantage continues.
Some corporations suffer from the degeneration of a rational plan. Modern corporations in Western society share the rational-scientific approach to management. Their rational system of thinking boils down to calculate the risks and possible ways of rendering the failure of developing procedures to detect abnormal patterns still largely lead to failure and crises. Why is this happening? It is impossible to predict what sort of crisis will occur.
The rational-scientific approach leads to a false sense of security, describing all the possible causes of the crises, plotting the routes of failure and assigning quantified risk factors to each scenario. If there is a hotspot – the risk that is very small becomes acceptable and ignored, because people tend to forget that the risks – however small – may actually come true. "The normalization of risk" often leads to understanding that "it is not going to happen here", but when a crisis occurs, all remain stunned.
Key words: corporation, safety, competition, risk
JEL classification: *M14*

Korporativna bezbednost

Pojmovno određivanje korporativne bezbednosti

Korporativna bezbednost u XXI veku predstavlja pravi izazov za top-menadžere. Da bi savremena korporacija bila bezbedna i poslovala u savremenim uslovima nije dovoljno samo odsustvo nečeg ili nekog oblika ugrožavanja, već i njena sposobnost da se adaptira na novonastale uslove i da funkcioniše pod pritiskom.

Funkcionisanje korporacije se više ne može posmatrati izolovano – u čistom obliku, jer dolaskom globalizacije osim novih trendova dolaze i novi rizici i pretnje – izazovi.

Danas se korporativna bezbednost posmatra kao uslov opstanka i održivog funkcionisanja sistema jedne korporacije.

Korporativna bezbednost predstavlja deo bezbednosne strukture koja je utemeljena na društvenim ciljevima koji koordiniraju poslovne aktivnosti privrednih subjekata i regulišu njihovo društvenoodgovorno ponašanje u skladu sa propisanim zakonima.[1]

Istorijski prikaz

U feudalnim društvima, društvena zajednica je bila u obavezi da svoje građane zaštiti od kriminala. U to vreme zločini su se rešavali prikupljanjem informacija od građana (svedoka) da bi na kraju počinilac bio uhvaćen. Glavni problem u srednjem veku je taj što su se takvi sistemi više bavili statusom pojedinca u društvenoj zajednici, nego samim činjenicama. Tako da možemo zaključiti da je u većini slučajeva rešavanje zločina u srednjem veku bilo nepravedno (neprofesionalno), jer su strukture koje su rešavale zločine više bile usmerene na status pojedinca nego na istinite činjenice.

Do kraja 13. veka temelji zakonske vladavine su bili postavljeni, 1215. godine engleski kralj Džon izdao je Veliki zakonik (Manga Carta), koji je predviđao propisani zakonski postupak za pojedinca. I kod nas imamo, takođe, kada je Car Dušan uveo Dušanov zakonik.

Sve više je u visokim slojevima društva naglašena potreba za sigurnošću – zaštita lica i imovine. Njima su tu bezbednosnu zaštitu pružale carske, kraljevske vojske. Bilo da ih nazivamo vitezovi ili samuraji njihov zadatak je bio isti - da štite ono najvažnije.

1 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski

U 17. veku s razvojem trgovinskih preduzeća u Zapadnoj Evropi i Americi rastao je i kapital i države su se širile. Razvoj i širenje države rezultira porastom populacije a sa tim dolazi i do porasta kriminala i nasilja sa čim državna policija nije mogla sasvim da se izbori. Ovakva negativna situacija pogodovala je razvoju privatnih bezbednosnih struktura – privatne policije s ciljem zaštite privatne imovine.

Svaka promena u međunarodnim odnosima ima uticaj na bezbednost korporacija. Države se udružuju radi zajedničkih interesa bilo da su ekonomski, strateški ili bezbednosni. Kada dođe do promene interesa u međunarodnim odnosima, sa njima se menjaju i bezbednosni odnosi.

Početak XX veka donosi veliki pomak u razvoju državne i privatne bezbednosti.

U periodu Hladnog rata (strateško udruživanje – bipolarni svet) svet je bio polarizovan na dva suprotstavljena vojnopolitička bloka Varšavski ugovor (sa Rusijom – tadašnja SSSR na čelu) i Atlantski pakt – NATO (sa SAD na čelu).

Sam taj period je izazivao veliku potrebu za tajnošću. Obezbeđenje (državni i privatni sektor) je bilo fokusirano na zaštitu informacija. Neprekidna trka u naoružanju rezultirala je stalnim pretnjama za spoljnu bezbednost. Pošto su potrebe sistema naoružanja Hladnog rata i drugih rukovodstava postajale sofisticiranije, tako je rastao i traženi nivo zaštite lica i imovine. U tom periodu je ustanovljeno da je informacija osnovna valuta moći, potreba za metodama zaštite informacija na svakom polju bila je izražena pa i na polju bezbednosti u korporacijama. Korporacije koje su podržavale državne odbrambene i ofanzivne potrebe, poznate kao industrijske odbrane[2], njihovo obezbeđenje se vrlo brzo širilo i razvijalo s ciljem zaštite imovine, informacija koje su bile deo i državnog nacionalnog aparata (npr. poverljivi ugovori).

Krajem 70-ih godina dolazi do političkih, ekonomskih, socijalnih promena, koje su doprinele porastu kriminalnih stopa. Povećanje kriminalnih stopa doprinelo je ekspanziji privatnog obezbeđenja. Bezbednosna kontrola u korporacijama se razvijala i usavršavala zbog velike potrebe za pouzdanom radnom snagom. Drugi svetski rat je stvorio ogroman broj ljudi sa znanjem iz bezbednosti, sprovođenja zakona, istražnim iskustvom, a sa svim tim i mogućnost njihovog zapošljavanja u privatnom sektoru. Kao dodatak ugovorima u upravljanju korporacijama, s ciljem zaštite imovine bila je izričito spomenuta i bezbednosna kontrola. Bezbednosna kontrola u to vreme zasnivala se na pretresu radnika u korporacijama da bi se izbegle krađe alata i slično.

Što se tiče bezbednosti posle Hladnog rata, sve do 1999. godine između Evropske unije i Rusije je vladala politika zanemarivanja. Zato što su još uvek bile geografski daleko. Prisutne su od tada pretnje za unutrašnju bezbednost u bivšim socijalističkim republikama gde postoje tzv. *nacionalne pukotine* (Bosna, Ukrajina), politika gotovo da nije ni postojala, ali se NATO profilisao kao garant bezbednosti.

Krajem 90-ih godina sa završetkom Hladnog rata postalo je vrlo jasno da ne nastupa period blagostanja. Stopa kriminala se povećava, a zločini - konflikti postaju sve više kompleksniji. Opasnost po bezbednost korporacija je upravo ta globalizacija, ne generalno globalizacija, ali sa povećanom globalnom konkurentnošću potreba za informacijama o poslovanju konkurentnih korporacija, da bi se bilo korak ispred, postala je epidemična.

Danas, u eri III tehnološke revolucije osim razvoja tehnologije drastično se povećavaju i sajber napadi na korporacije s ciljem krađe informacija od važnosti ili sabotaže određenih

2 Korporativna bezbednost, doc. dr Miroslav M. Milutinović

delatnosti koji su od bitnog interesa za korporaciju. Zbog toga dolazi do razvoja i usavršavanja korporativnog sektora bezbednosti.

Sektor korporativne bezbednosti je od krucijalnog značaja za jednu korporaciju, jer on štiti od potencijalnih oblika ugrožavanja vitalnih struktura korporacije i uspostavlja osnovu za donošenje kvalitativnih i kvantitativnih upravljačkih odluka. Obezbeđuje top-menadžmentu pristup poverljivim informacijama i garantuje njihovu sigurnost kroz procese i procedure koji sprečavaju njihovo odlivanje iz korporacije[3].

Odnos korporativne i privatne bezbednosti

Opstanak i održivi razvoj države kao političke zajednice koja služi vladajućoj klasi za održavanje njene ekonomske i političke vlasti uspostavlja se makrobezbednosnim sistemom koji sačinjavaju brojni višenivoovski mikrobezbednosni sistemi.

Savremena država je suočena sa raznovrsnim problemima. Sa ciljem zaštite vitalnih nacionalnih vrednosti i očuvanja unutrašnjeg mira (sprečavanje anarhije) sa jedne strane i odbrane od spoljnog ugrožavanja sa druge strane ona razvija monopol upotrebe legitimne sile[4].

Privatna bezbednost je činilac sistema nacionalne bezbednosti i putem zakonskih odredbi je određena njena uloga, delokrug rada i nadležnosti. Prema nekim analitičarima, na razvoj sektora privatne bezbednosti bitno su uticala dva momenta.

Prvi momenat je trend privatizacije koji je prisutan od 80-ih godina u zemljama Zapadne Evrope i Severne Amerike.

Drugi momenat je kao posledica okončavanja Hladnog rata višak vojnog, obaveštajnog i policijskog osoblja koje je potražilo posao u privatnom sektoru bezbednosti koji u to vreme postaje aktuelan.

Postoji jako bitna razlika između privatne (*private security*) i korporativne bezbednosti (*corporate security*). Zato što privatna bezbednost predstavlja specifičan podsistem u odnosu na sistem nacionalne bezbednosti države.

Privatni sektor možemo podeliti na privatni sektor bezbednosti - poslovi privatnog obezbeđenja lica, poslovanja i imovine (vitalne nacionalne infrastrukture, postrojenja i naftovoda, zaštita humanitarnih radnika i zaštita konvoja, detektivska istražna delatnost).

Privatni sektor obuhvata i poslove privatnih vojnih kompanija i mnoge druge na komercijalnoj osnovi realizovane poslove bezbednosti[5] (plaćenici - predstavljaju vojnike koje unajmljuju strane države ili pobunjenički pokreti da bi doprineli vođenju oružanog konflikta, direktnim ili indirektnim angažovanjem u sukobu, putem treninga, logistike, konsaltinga ili prikupljanja podataka – oni to rade izvan nadležnosti oružanih snaga i države kojoj pripadaju, privatizovane kaznene ustanove).

Privatna bezbednosna kompanija je jasno strukturirana i hijerarhijski definisana registrovana korporativna asocijacija. Pruža usluge bezbednosnog karaktera, takmičeći se sa drugim takvim firmama za dobijanje poslova na tržištu.[6]

Privatizacija vojne industrije, podstaknuta revolucionarnim talasom privatizacije svih oblasti života, omogućila je privatnim firmama da postanu potencijalni provajderi bezbe-

3 Korporativna bezbednost, Dragan Trivan
4 Nacionalni sistem bezbednosti, prof. dr Duško Tomić, prof. dr Milan Mijalkovski, Predrag Marić
5 Korporativna bezbednost, Dragan Trivan
6 Petrović, Predrag, Unijat, Jelena, Milošević, Marko (2010), Komentari na Nacrt zakona o privatnom obezbeđenju i Nacrt zakona o detektivskim poslovima

dnosnih i vojnih usluga. U uslovima posle Hladnog rata dolazi do rasprodaje oružja i vojne opreme i viška vojnog osoblja, a uporedo sa neoliberalnom privatizacijom korporacije su brzo uvidele šansu u mogućnostima koje je vlada, privatizacijom određenih državnih sektora, nudila.

Države su podstaknute talasom privatizacije želele da smanje vojne troškove i da određeni deo prenesu na privatni sektor. Rezultat toga bio je da su svetske sile – tradicionalni akteri u regionalnim i međudržavnim konfliktima za vreme Hladnog rata – smanjile svoje angažovanje u rešavanju konflikata. Privatne vojne kompanije su u tome brzo uvidele veliku šansu i popunile taj vakuum - automatski su apsorbovale višak vojnog osoblja i opreme. Ubrzo su počele da nude širok spektar vojnih i bezbednosnih usluga različitim zainteresovanim klijentima.

Nakon završetka Hladnog rata, drugi veliki talas rasta privatnih vojnih i bezbednosnih kompanija nastupio je posle intervencija u Avganistanu i Iraku.

Privatni sektor u zapadnim zemljama je nastupio kao posledica zahteva da državne institucije efikasnije obavljaju svoj posao. Međutim, u Srbiji je do toga došlo zbog sasvim drugog razloga. Zbog potpunog kolapsa države u jednom momentu i njene nemogućnosti da obavlja osnovne funkcije. U periodu između 1990. i 2000. godine Srbija je doživela ogroman pad industrijske proizvodnje, veliko smanjenje izvoza, hroničnu nezaposlenost, a siva ekonomija je zamenila regularno tržište.

Takođe, Srbiju je zadesio i ogroman pad u oblasti vladavine prava i efikasnosti institucija zaduženih da građanima osiguraju bezbednost. Tokom devedesetih godina dolazi do ukidanja Zakona o društvenoj samozaštiti 1993. godine. Taj zakon je propisivao zadatke i odgovornosti privrednih subjekata u sistemu bezbednosti. Firme koje su do tada poslovale u okviru društvenih preduzeća nastavile su po inerciji da slede odredbe ovog zakona. Problem je nastao zato što se ukidanjem društvene samozaštite pojavila praznina u sektoru bezbednosti koju državni akteri nisu popunili, pa je u taj **prostor došao** privatni kapital. Delujući po zahtevima tržišta, a u odsustvu zakonske regulative, ovaj sektor se nije integrisao u bezbednosni sistem Srbije.

Nakon promene vlasti 5. oktobra 2000. godine u privatnom bezbednosnom aparatu učinjeni su značajni pokušaji da se njihova delatnost usavrši. Većina firmi doživela je svoj procvat ulaskom stranih preduzeća na srpsko tržište krajem XX veka. Najznačajniji klijenti u Srbiji postale su strane banke.

Porast privatnog sektora bezbednosti od početka demokratizacije predstavlja prelazak viška vojnog i policijskog osoblja u privatne bezbednosne kompanije usled smanjivanja brojnog stanja vojske i policije. Vojska Srbije nema evidenciju o tome koliko je njenih bivših pripadnika zaposleno u firmama ovog tipa. Uvideći veliku zainteresovanost osnovala je program prekvalifikacije za poslove u privatnim bezbednosnim kompanijama[7]. Najviše napora ka usavršavanju i razvijanju privatnog sektora bezbednosti učinilo je Udruženje za fizičko tehničko obezbeđenje osnovano pri Privrednoj komori Srbije (PKS) 2005. godine.

Sadržaj i osnovna obeležja korporativne bezbednosti

Danas u XXI veku bezbednost korporacija je ugroženija nego ikad. Korporativna bezbednost u savremenim uslovima postala je strateška funkcija poslovnih subjekata. Drasti-

7 Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?, mr Sonja Stojanović, Centar za civilno-vojne odnose, Beograd 2008

čan porast broja organizacija – grupa, pojedinaca koji imaju interes da ugroze opstanak i održivi razvoj jedne korporacije ili su plaćeni za takvo nešto od strane druge korporacije (subjekt opasnosti) koja korporaciju – koja je žrtva u ovom slučaju doživljava kao konkurentnu pretnju. Delovanje destruktivnih organizacija ili pojedinaca osim želje za konkurentnom prednošću napadi mogu biti zbog nekih drugih pobuda: religioznog, ekonomskog, političkog, ideološkog tipa.

To su razne vrste opasnosti - napada koje mogu biti internog ili eksternog karaktera. Mogu da se ispolje iznenada ili nakon nekog određenog vremena, nanoseći korporaciji veliku štetu u sistemu funkcionisanja (reputacija kompanije, razotkrivanje strategije poslovanja i analiza konkurencije, a ovo može da rezultira opadanjem morala i motivisanosti zaposlenih kao i njihovo poverenje u instituciju u kojoj rade). Opasnost po održivost jedne korporacije mogu biti i drastično nepovoljni vremenski uslovi.

Direktni izvori opasnosti po bezbednost korporacija mogu biti:

- Tehničko-tehnološki akcidenti;
- Elementarne nepogode;
- Krivična dela kojima se nanosi šteta poslovnom subjektu (diverzije, sabotaže, terorizam, uništenje/oštećenje sredstava za proizvodnju proizvoda);
- Krivična dela klasičnog kriminaliteta;
- Krivična dela privrednog kriminaliteta – koja vrše zaposleni u sprezi sa poslovnim partnerima (zloupotreba službenog položaja, korupcija, mito, pronevera, pljačka, ugovaranje ili poslovanje na štetu kompanije);
- Krivična dela izazivanja opšte opasnosti i krivična dela protiv zdravlja ljudi i životne sredine;
- Krivična dela upotrebom informatičkih tehnologija – sajber kriminal;
- Saobraćajne nesreće i nezgode;
- Odlivanje poverljivih podataka;
- Prekršaji (nesavesno poslovanje, kršenje radne discipline, prekoračenje ili uzurpiranje nadležnosti i ovlašćenja);
- Socijalni i drugi konflikti unutar korporacije.[8]

Kriterijumi nosioca opasnosti vitalnim vrednostima korporacije sa jedne strane su sve ugrožavajuće delatnosti koje subjekti opasnosti svesno preduzimaju da bi pribavili ličnu korist ili pak svojim nehatnim delovanjem izazivaju štetu, a sa druge su prirodne sile (izvori opasnosti) – elementarne nepogode.

Subjekti opasnosti protiv sistema vrednosti korporacije mogu da budu internog i eksternog tipa.

U interni tip spadaju: članovi kompanije/ njeni zaposleni – pojedinci i ogranizovane grupe uključujući i top-menadžment koji svojim činjenjem ili nečinjenjem ugrožava bezbednost;

U eksterni tip spadaju: pojedinci/kolektiviteti iz okruženja kompanije koji u saradnji sa pojedincima/organizovanim grupama unutar kompanije deluju protiv bezbednosti korporacije.

Motivi za delovanje na štetu korporacije mogu biti beskonačni, počevši od sukoba između zaposlenih – rivalstva, nesklada ili nesrazmera finansijskih i statusnih želja; destruk-

8 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski

tivno ponašanje – zavisnost od alkohola, narkotika; kleptomanija; dugovi, bolest; odranije ispoljena sklonost ka kriminalnim radnjama.

Odnos spoljnih i unutrašnjih oblika ugrožavanja korporacije približno je 80% : 20%, s tim što visina štete po korporaciju je obrnuta, veća šteta je kada zaposleni učestvuju u konfliktu.[9]

Jedan od opasnijih oblika korporacijskog kriminala jeste akt koji je rezultat donošenja odluka od strane onih koji zauzimaju uticajne (menadžerske, izvršne) pozicije u kompaniji. Ove uticajne strukture koje su deo korporativnog aparata i čiji je zadatak da donose zakonite odluke, zasnovane na pravilima poslovanja sa ciljem ostvarenja dobiti korporacije, povlače sasvim suprotne poteze. Reč je o visokokvalifikovanim profilima koji svojim svesnim planiranim delovanjem direktno ili indirektno vrše nezakonite aktivnosti da bi pribavili ličnu imovinsku korist. Profili učinioca ovakvih krivičnih dela vrlo često koriste svoj položaj (status) da bi izbegli krivičnu odgovornost – sankciju, a subjekti nacionalne bezbednosti im često povlađuju.

Ovakav vid kriminala se češće dešava u zemljama trećeg sveta gde postoje pukotine u nacionalnim strukturama bezbednosti.[10]

Oformljavanjem sektora za kontrolu bezbednosno-korporativne kontrole u korporacijama na regionalnom nivou. Koje će da rade nezavisno i da budu deo državnog aparata. Cilj im je razotkrivanje ovakvih kriminalnih grupa, delatnosti. Verujem da bi to značajno doprinelo smanjenju ovakvih nezakonitih aktivnosti koje osim štete po korporaciju nanose i štetu državi.

Opasnost po održivo funkcionisanje sistema korporacije osim čovekovog činjenja/nečinjenja mogu da prouzrokuju i elementarne nepogode. U njih spadaju: zemljotresi, poplave, bujice, olujni vetrovi, lavine, suše, šumski požari, jaki uporni mrazevi, epidemije, epizootije.[11]

Prirodne i čovekove opasnosti po bezbednost korporacija se ispoljavaju svakodnevno. Međutim, kada se na prostoru ili u okolini desi neka nepredviđena krizna ili vanredna situacija, povećava se ranjivost korporacija na potencijalne hazarde.[12] Usavršavanjem bezbednosnog menadžmenta, korporacije uče kako da se adaptiraju na novonastale neprijatne uslove funkcionisanja kroz:

Prvenstveno podizanje svesti radnika, zaposlenih, članova, osoblja o potencijalnim pretnjama – nosiocima ugrožavajućih delatnosti; adekvatnu obuku istih za delovanje u slučaju vanredne situacije. Sektor korporativne bezbednosti ne oslanjajući se isključivo samo na racionalno-naučni princip savladavanja teškoća priprema sve i na ono što se možda nikad neće desiti.

Zato Evropska unija predlaže implementaciju integralne bezbednosti u korporacijama.

Takva vrsta bezbednosti obuhvata poslove obezbeđenja (*security*) i poslove zaštite (*safety*). Na osnovu iskustva dobre prakse smatra se da povezivanje ovakvih poslova od strane jedinstvenog menadžera bezbednosti doprinosi delotvornijoj organizaciji, koordinaciji i kontroli datih poslova, a samim tim i racionalizaciji i unapređenju celokupnog poslovanja.[13]

9 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski
10 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski
11 Epidemije kod životinja
12 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski
13 Korporativna bezbednost, Dragan Trivan

Na osnovu svih mogućih potencijalnih opasnosti sa kojima smo se upoznali možemo zaključiti da rad menadžera bezbednosti u korporaciji nije jednostavan. Njegov zadatak obuhvata poslove kao što su prikupljanje informacija, bezbednosnih procena i procena rizika, informatičke zaštite, kriznog menadžmenta, zaštite od požara, eksplozija i havarija, zaštite bezbednosti i zdravlja na radu.

Integralna bezbednost u korporacijama

U borbi za opstanak na tržištu, najuspešnije korporacije, banke i druge finansijske organizacije (uglavnom veće, a često i multinacionalne) sa prostora Zapadnog Balkana, shvataju da je bezbednost od vitalnog značaja za njihovo normalno funkcionisanje. Zbog toga ulažu sve napore na blagovremenu identifikaciju i procenu pretnji u vezi s poslovanjem, na proaktivno/reaktivno delovanje i upravljanje rizicima, kao i na efikasniju i širu implementaciju odbrambenih mehanizama. Uviđaju da je korporativna bezbednost krucijalni segment za normalno funkcionisanje korporacije.

Sigurno je da je jedna od posledica ekonomske krize i recesije upravo zanemarivanje sektora za korporativnu bezbednost, što je prisutno kod većine kompanija zemalja Zapadnog Balkana.[14]

Različiti podaci ukazuju na to da većinu rukovodećeg sastava: zaposlenih u korporativnom sektoru bezbednosti i u privatnim kompanijama za obezbeđenje još uvek čine bivši pripadnici vojnih i policijskih struktura koji su se pojavili u periodu posle Hladnog rata.[15] Takvi profili ljudi ne poseduju šire znanje i posebne veštine koje su danas neophodne da bi se rad na ovim bezbednosnim poslovima potpuno uskladio sa principima i ciljevima poslovanja korporacije.

Korporacija se zasniva na privatnom vlasništvu. Danas je to najkompleksniji organizacioni model poslovnog sistema. Korporacija predstavlja društvo kapitala koje do sredstava za osnivanje i poslovanje dolazi izdavanjem deonica.[16]

Korporacije su pod velikim uticajem okruženja u kojem rade, jer one iz okruženja nabavljaju (crpe) resurse. Resursi su aktiva, kao što su ljudi, informacije, mašine, veštine, sirovine i finansijski kapital. Sistem korporativne bezbednosti u korporacijama, prema smernicama Evropske unije, može se definisati kao integralna bezbednost. Takav sistem bezbednosti sadrži brojne podsisteme koji su od vitalnog značaja za njeno normalno funkcionisanje. Jer da bi ona normalno – optimalno funkcionisala sektori bezbednosti moraju da budu prisutni u svim funkcijama njenog delovanja.

Korporativni bezbednosni menadžment je upravljačka delatnost pojedinih članova i mikrobezbednosnog sistema korporacije. Kroz nju (upravljačka delatnost) menadžeri štite sistem vrednosti kompanije od svih oblika samougrožavanja i ugrožavanja (agresije) u uslovima realnog okruženja.

Uloga – zadatak bezbednosnog menadžera jeste da prepozna, odvraća, sprečava, suzbija i kažnjava svakog subjekta opasnosti koji je usmeren na izazivanje štetnih promena u sistemu vrednosti kompanije.

Bezbednosni menadžer u korporaciji ostvaruje svoje zadatke primenom dva međusobno isprepletena modela operativnog delovanja:

14 Korporativna bezbednost u uslovima krize, Dragan Trivan
15 Odnosi se na zemlje Jugoistočne Evrope, prvenstveno na zemlje Zapadnog Balkana
16 Korporativna bezbednost, Dragan Trivan

1. *Preventivni* – odvraća nosioce od preduzimanja ugrožavajućih delatnosti i sprečava njihovu realizaciju;
2. *Represivni* – kažnjavanje učinioca ugrožavajućih delatnosti na pravno dozvoljen način i saniranje posledica.

Porast svesti o bezbednosti i potencijalnim hazardima nesumnjivo ukazuje vlasnicima kapitala i top-menadžerima da je razvoj i usavršavanje bezbednosnih kadrova u korporaciji bazičan preduslov za njeno optimalno funkcionisanje.

Pošto je korporativna bezbednost podeljena na mikrobezbednosne sektore svaki od njih ima zadatak da:

1. Analizira aktuelne rizike;
2. Precizira nadležnosti;
3. Strogo vodi računa o organizaciji i ispravnosti uređaja fizičko-tehničkog obezbeđenja svih objekata koji su u sklopu kompanije;
4. Primenjuje i podstiče na mere zaštite vezane za bezbednost i zdravlje, zaštitu životne sredine, zaštitu od požara, eksplozija;
5. Mere zaštite poslovanja koorporacije od korupcije, zloupotrebe, pronevera, prevara;
6. Preciziranje zaštite poslovne i službene tajne;
7. Konkretizovanje mera u odnosu na kontrolu kretanja i boravka stranih lica u objektima i prostoru;
8. Organizaciju i funkcionisanje informacionih sistema u obezbeđenju lica i imovine i poslovanja koorporacije pogotovo zaštita informacija;
9. Harmonizaciju normativnih akata u svim segmentima bezbednosti sa nacionalnim propisima;
10. Ocenu stepena ugroženosti lica koja u koorporaciji rade na poslovima zaštite njihovih vitalnih vrednosti.[17]

Menadžer korporativne bezbednosti je lice koje je osposobljeno i ovlašćeno da planira, organizuje, sprovodi strategiju i koordinira i kontroliše rad profitne organizacije (firma, preduzeće, kompanija, korporacija, trust, banka). Menadžer bezbednosti ima brojne nadležnosti i snosi veliku odgovornost za bezbedan rad kako bi organizaciono poslovanje bilo optimalno uspešno. On to ostvaruje kroz osmišljavanje i implementaciju integrisanih sistema obezbeđenja na svim poljima.

Prema smernicama Evropske unije u sastavu integrisanog sistema bezbednosti u korporacijama treba da bude:

1. Organizaciona jedinica za korporativnu bezbednost:

- rukovodilac organizacione jedinice;
- menadžer za informacionu bezbednost;
- specijalista za poslove bezbednosti;
- specijalista za poslove obezbeđenja ličnosti;
- specijalista za odbrambene pripreme.

2. Organizaciona jedinica za zaštitu na radu, zaštitu od požara, zaštitu životne sredine:

- rukovodilac organizacione jedinice
- specijalista za zaštitu na radu i zaštitu od požara

17 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski

- specijalista za zaštitu životne sredine. 18

Zaštita resursa kritične infrastrukture

Pojam kritična infrastruktura (*Critical Infrastructure*) postaje aktuelan neposredno nakon terorističkih napada 11. septembra 2001. godine u SAD. Nakon takvog scenarija kritična infrastruktura postaje bitan deo nacionalne bezbednosti svake države.

SAD kritičnu infrastrukturu i resurse definišu kao neophodne (krucijalne) elemente (sektore) za svakodnevno funkcionisanje političkih, ekonomskih, društvenih i kulturnih sistema jedne države. Pod pojmom kritična infrastruktura smatraju se sva prirodna i materijalna dobra, imovina, tehnički sistemi, komunikacije, poslovne delatnosti i službe koje su od posebnog (bitnog) značaja za državu. To predstavlja da bilo kakvo oštećenje, uništenje ili prekid tih resursa se automatski odražava na nacionalnu bezbednost, ekonomiju, vitalne društvene funkcije, zdravlje, stanovništvo i javni poredak države. Okviri krivičnih infrastruktura nisu u svim zemljama isto definisani, prvenstveno zbog različitih političkih prilika i geografskih lokacija.

KANADA	VELIKA BRITANIJA	SAD	NEMAČKA	NORVEŠKA	ŠVAJCARSKA
ENERGIJA (objekti električne i nuklearne energije, prirodni plin i nafta, proizvodni i transportni sistemi)	**ENERGIJA**	**ENERGIJA**	**ENERGIJA** (električna, nafta i plin)	**ENERGIJA I OBJEKTI**	**OBJEKTI I SLUŽBE**
KOMUNIKACIJE	**TELEKOMUNIK.**	**INFORMACIJE I TELEKOMUNIK.**	**TELEKOMUNIK. I INFORMACIONA INFRASTRUKTURA**	**SNABDEVANjE NAFTOM I PLINOM**	**TELEKOMUNIK.**
SERVISI (finansije, distribucija hrane, javno zdravstvo)	**ZDRAVSTVENE SLUŽBE**	**JAVNO ZDRAVSTVO**	**JAVNO ZDRAVSTVO** (uključujući i snabdevanje pitkom vodom i hranom)	**TELEKOMUNIK.**	**DISTRIBUCIJA INFORMACIJA**

Tabela – Neke od kritičnih infrastruktura različitih zemalja[19]

U poslednjih nekoliko godina došlo je do usavršavanja strategija za zaštitu kritičnih infrastruktura. Te strategije su usmerene ka efikasnom i preventivnom delovanju u slučaju negativnih scenarija (terorističkih napada, prirodnih katastrofa većih razmera).

U okviru Direktive Saveta Evrope 2008/114/ES određeni sektori za koje je potrebno definisati kritičnu infrastrukturu su:

18 Bezbednosni menadžment, prof. dr Duško Tomić, prof. dr Milan Mijalkovski

19 Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope 2008/114/ES, Mirko Škero Bezbedno-informativna agencija, Vladimir Ateljević, Vlada Republike Srbije, Kancelarija za evropske integracije

Sektor	Podsektor	Kritična infrastruktura
Energija	1. Električna energija	Infrastruktura i objekti neophodni za proizvodnju i prenos električne energije
	2. Nafta	Proizvodnja nafte i rafinisanje
	3. Gas	Proizvodnja gasa i rafinisanje
Transport	4. Drumski transport 5. Železnički transport 6. Vazdušni transport 7. Transport unutrašnjim plovnim putevima 8. Prevoz okeanom i morima	

Kritične infrastrukture su povezane na različitim nivoima i „kvar" na jednom elementu može da izazove prelivanje na ostale elemente – domino efekat. Kritične infrastrukture u okviru jedne države predstavljaju složene podsisteme između kojih postoji velika međuzavisnost.

Npr. Velika povezanost i međuzavisnost vlada između informacionih i komunikacionih sistema i elemenata nacionalne infrastrukture: transport, proizvodnja i distribucija električne energije i drugih energenata, bankarsko poslovanje, javno zdravstvo, državna i lokalna uprava, vodosnabdevanje, mediji, nauka, vaspitanje, obrazovanje, službe hitne pomoći. To nesumnjivo ukazuje na to da informacioni i komunikacioni sektor ima poziciju centralne infrastrukture, a takvi sistemi i procesi predstavljaju privlačne mete terorističkih napada. U slučaju prekida telekomunikacionog sistema treba uzeti kao prioritet i ostale elemente koji su u tesnoj vezi sa tim sektorom, jer meta napada ne mora da bude uvek i sektor koji je napadnut.

Ovakvi sistemi danas su najčešće meta mlađih generacija terorista. Razlog za drastično povećanje terorističkih operativnih sposobnosti je lako dostupna sofisticirana tehnologija i pomagala kao što su: vrhunska računarska i komunikacijska oprema; sredstva za kvalitetno kriptovanje poruka; tehnički sistemi za detekciju kretanja, prisluškivanje, noćno osmatranje; oružja za privremeno onesposobljavanje i iznuđivanje tajnih informacija i podataka; mašine i alati za izradu oružja; serveri i informacioni sistemi za raznovrsne podatke, uključujući i satelitske snimke koji su lako dostupni na internetu.

Zbog ovakih operativnih sposobnosti resursi kritičnih infrastruktura potencijalno su ugroženi i od sabotaža i hakerskih napada. Informacija svoju valutu ne menja, danas hakeri vrlo lako mogu da upadnu u servere kritičnih infrastruktura da nanesu štetu u funkcionisanju ili da dođu sa lakoćom do većeg broja ključnih podataka. Sabotaža unutrašnjeg informacionog sistema ima mnogo veću posledicu od postavljanja eksploziva u postrojenjima. Ključni nosioci ovakvih delatnosti mogu biti od terorističkih organizacija, grupa organizovanog kriminala i hakerskih mreža.

Evropska pravna regulativa u oblasti kritičnih infrastruktura

Savet Evrope je 24. juna 2004. godine zatražio od Komisije da pripremi strategiju zaštite kritične infrastrukture. Komisija je 20. oktobra 2004. godine usvojila dokument koji se odnosi na terorizam kao potencijalnu opasnost „**Zaštita kritične infrastrukture u borbi protiv terorizma**" koji predlaže šta bi poboljšalo evropsku prevenciju, spremnost i odgovor na teroristički napad koji pogađa kritičnu infrastrukturu.

Savet je usvojio i **Evropski program za zaštitu kritične infrastrukture** (EPZKI/EPCIP) i saglasio se oko aranžmana Komisije za **Informacionu mrežu za upozoravanje o kritičnoj infrastrukturi** (IMUKI/CIWIN).

U novembru 2005. godine Komisija je usvojila Zeleni papir o Evropskom programu za zaštitu kritične infrastrukture (EPZKI/EPCIP).

Na ovaj način EU definiše Evropsku kritičnu infrastrukturu kao infrastrukturu koja se sastoji od fizičkih resursa, službi, uređaja, informacione tehnologije, sigurnosti mreža i infrastrukture, bezbednosne, ekonomske ili socijalne dobrobiti.

Odnos Republike Srbije prema zaštiti resursa kritične infrastrukture

Ključna infrastruktura u Srbiji su preduzeća u oblasti energetike, vodoprivrede, poštanskih usluga, telekomunikacija, železnice, zdravstvene ustanove, aerodromi, rečne luke, vodovodi, škole, fakulteti, autobuske stanice.

Republika Srbija čini značajne napore u stvaranju integrisanog sistema zaštite i spasavanja, koji bi se primenio u uslovima ugrožavanja kritičnih nacionalnih resursa. Država je donošenjem Zakona o vanrednim situacijama 2009. godine odlučila da Ministarstvo unutrašnjih poslova bude nadležno za izradu procene ugroženosti od elementarnih nepogoda i drugih nesreća. U čl. 46 tog zakona propisuje se da se procenom ugroženosti identifikuju izvori mogućeg ugrožavanja, predvide posledice, i koje su mere - zadaci neophodni radi zaštite i spasavanja.

Procena ugroženosti sadrži naročito:

1. Karakteristike teritorije, kritična postrojenja, kritična mesta i prostore sa gledišta ugroženosti od elementarnih nepogoda i drugih nesreća, sa eventualnim prekograničnim efektima udesa;
2. povredljivost teritorije od elementarnih nepogoda i drugih nesreća;
3. analizu mogućih posledica od elementarnih i drugih nesreća;
4. potrebe i mogućnosti za zaštitu ljudi, materijalnih dobara i životne sredine od posledica elementarnih i drugih nesreća[20].

Donošenjem „Strategije razvoja informacionog društva u Republici Srbiji do 2020", se definiše: „Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme".

U okviru „Strategije nacionalne bezbednosti Republike Srbije", pojam „kritična infrastruktura" se ne spominje direktno, ali se ukazuje na probleme ekonomskog razvoja Republike Srbije usled višegodišnjih sankcija i uništenja vitalnih objekata privredne i saobraćajne infrastrukture, energetsku međuzavisnost i osetljivost infrastrukture za proizvodnju i

20 Zakon o vanrednim situacijama, SL. RS 2009

transport energenata, visokotehnološki kriminal i ugrožavanje informacionih i telekomunikacionih sistema.[21]

Vlada Republike Srbije je 2002. godine podnela Narodnoj skupštini Nacrt zakona o fizičko-tehničkom obezbeđenju objekata. Ovim zakonom se predlaže da objekti od strateškog značaja za Republiku Srbiju i njene građane, ili koji predstavljaju povećanu opasnost za život i zdravlje ljudi, moraju imati fizičko - tehničko obezbeđenje. Kao obavezno obezbeđeni objekti navode se:

1. Objekti za proizvodnju, preradu, distribuciju i skladištenje nafte, naftnih derivata i gasa;
2. Objekti za proizvodnju, preradu, distribuciju i skladištenje vode;
3. Objekti za proizvodnju i distribuciju električne energije;
4. Objekti u kojima se proizvode, koriste ili skladište radioaktivne i druge opasne i štetne materije;
5. Objekti od značaja za saobraćaj u svim vrstama saobraćaja;
6. Objekti u kojima se drže stvari od izuzetnog značaja za nauku, kulturu i umetnost;
7. Objekti u kojima se okuplja veliki broj ljudi i drugi objekti za koje Vlada utvrdi da se obavezno obezbeđuju.[22]

Zaključak

Postojanje i implementacija sistema korporativne bezbednosti štiti kompaniju od potencijalnih ugrožavajućih delatnosti. Primenom savremenih metoda, tehnologija i principa menadžeri bezbednosti bolje razumeju prepreke sa kojima se susreću. S tim oni razvijaju efikasnije strategije za preventivno i represivno delovanje u kriznim i vanrednim situacijama. Porastom svesti o bezbednosti vlasnici kapitala i top-menadžeri shvataju da razvojem – usavršavanjem korporativne bezbednosti obezbeđuju sebi sigurniji put ka ostvarenju finansijskih i strateških ciljeva.

Krizne i vanredne situacije su deo svakodnevnog života, sa razvojem društva povećavaju se njihovi izvori, oblici javljanja, a nespremnost rezultira gubicima ljudskih života i velikom materijalnom štetom.

Zbog kompleksnosti vanrednih i kriznih situacija države su razvile metode sa kojima se prepoznaju indikatori ranjivosti infrastruktura, definišu mere za smanjenje rizika, osmišljavaju planovi za oporavak od kriznih i vanrednih situacija, podstiče na razvoj senzibiliteta kod javnih i privatnih operatera u pogledu problema zaštite kritične infrastrukture, metode koje podstiču na međunarodnu saradnju.

Evropska unija da bi zaštitila svoju kritičnu infrastrukturu je primenila niz direktiva, zakona i strategija i uredba koje im omogućavaju da preventivno i represivno deluju kada nastupi kriza ili vanredna situacija ili eventualno da spreče njen nastanak.

Republika Srbija bi u toku procesa pridruživanja EU trebalo da usvoji Zakon o kritičnim infrastrukturama koji će biti usklađen sa elementima Direktive 2008/114/ES. Na taj način bi se regulisala značajna oblast koja do danas nije adekvatno regulisana.

21 Strategija Nacionalne bezbednosti RS 2009

22 Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope 2008/114/ES, Mirko Škero, Bezbedno-informativna agencija, Vladimir Ateljević, Vlada Republike Srbije, Kancelarija za evropske integracije

Literatura:

1. Tomić D., Mijalkovski M., *Bezbednosni menadžment*, Fakultet za inžinjerski menadžment, 2015, Beograd
2. Trivan D., *Korporativna bezbednost*, Protekta 2014, Beograd
3. Škero M., Ateljević V., *Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope* 2008/114/ES, Kancelarija za evropske integracije, 2014, Beograd
4. Jakovljević V., Gačić J., *Zaštita kritičnih infrastruktura u kriznim situacijama,* Fakultet bezbednosti 2013, Beograd
5. Tomić D., Mijalkovski M., Marić P., *Nacionalni sistem bezbednosti*, PI PRESS 2012, Pirot
6. Stojanović S., *Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?,* Centar za civilno--vojne odnose, Beograd, 2008
7. Anđelković S., Savković M., *Značaj i uloga privatne bezbednosti u sistemu nacionalne bezbednosti,* Fakultet političkih nauka, 2012, Beograd