Univerzitetna založba
Univerze v Mariboru

INTEGRALNA KORPORATIVNA VARNOST

PRAKTIKUM

Miha DVOJMOČ

Univerza v Mariboru

Fakulteta za varnostne vede

Integralna korporativna varnost

Praktikum

Avtor

Miha Dvojmoč

April 2024

Naslov / *Title*: **Integralna korporativna varnost** / *Integral Corporate Security*

Podnaslov / *Subtitle*: **Praktikum** / *Practicum*

Avtor / *Author*: Miha Dvojmoč
(Univerza v Mariboru, Fakulteta za varnostne vede)

Recenzija / *Review*: Branko Lobnikar
(Univerza v Mariboru, Fakulteta za varnostne vede)

Dragan Trivan
(Univerzitet Union – Nikola Tesla, Fakultet za poslovne studije i pravo)

Lektoriranje / *Language editing*: Andreja Breznik

Barbara Erjavec
(Univerza v Mariboru, Fakulteta za varnostne vede)

Tehnična urednika / *Technical editors*: Marina Bajić
(Univerza v Mariboru, Univerzitetna založba)

Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka / *Cover designer*: Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Grafične priloge / *Graphic material*: Viri so lastni, razen če ni navedeno drugače.
Dvojmoč (avtor), 2024

Grtafika na ovitku / *Cover graphics*: White and black glass walled building, avtor: Maximalfocus, unsplash.com, 2020

Založnik / *Published by*: **Univerza v Mariboru**
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj / *Issued by*: **Univerza v Mariboru**
Fakulteta za varnostne vede
Kotnikova ulica 8, 1000 Ljubljana, Slovenija
https://www.fvv.um.si/, fvv@um.si

Izdaja / *Edition*: Prva izdaja

Izdano / *Published at*: Maribor, april 2024

Vrsta publikacije / *Publication type*: E-knjiga

Dostopno na / *Available at*: https://press.um.si/index.php/ump/catalog/book/869

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

005.934(0.034.2)

DVOJMOČ, Miha
Integralna korporativna varnost [Elektronski vir] : praktikum / avtor Miha Dvojmoč. - 1. izd. - E-knjiga. - Maribor : Univerza v Mariboru, Univerzitetna založba, 2024

Način dostopa (URL): https://press.um.si/index.php/ump/catalog/book/869
ISBN 978-961-286-850-5 (PDF)
doi: 10.18690/um.fvv.3.2024
COBISS.SI-ID 191817987

ISBN 978-961-286-850-5 (pdf)

DOI https://doi.org/10.18690/um.fvv.3.2024

Cena / *Price*: Brezplačni izvod

Odgovorna oseba založnika / *For publisher*: prof. dr. Zdravko Kačič,
rektor Univerze v Mariboru

Citiranje / *Attribution*: Dvojmoč, M. (2024). *Integralna korporativna varnost: praktikum.* Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.fvv.3.2024

Univerzitetna založba
Univerze v Mariboru

Kazalo

Univerzitetna založba
Univerze v Mariboru

1 Predgovor

Na podlagi poučevanja in priprav vaj pri predmetu »Integralna korporativna varnost« na Fakulteti za varnostne vede Univerze v Mariboru ter letih raziskovanja je nastal praktikum, ki je zbirka vsebinsko zaokroženih poglavij, sledijo jim teoretična vprašanja, ki omogočajo poglobljeno razmišljanje in tudi samo razumevanje vsebine. Pri odgovarjanju na vprašanja je predvidena uporaba že pridobljenega znanja in logičnega razmišljanja ter tudi lastnega mišljenja, ki je s pomočjo praktikuma še nadgrajeno.

Praktikum je razdeljen na tri glavne dele: 1. del predstavlja Osnove korporativne varnosti, 2. del Specifična področja korporativne varnosti, 3. del pa obravnava Posebne teme v korporativni varnosti. Vseh poglavij praktikuma je dvanajst, pri čemer je vsako poglavje razdeljeno na podpoglavja, ki obravnavajo določene teme. Nekatere teme so bolj poglobljene in obsežne, saj je njihovo razumevanje zelo pomembno. Vprašanja so zastavljena po koncu vsakega poglavja z namenom, da se vsebinsko zaokroži pridobljeno znanje. Bralec s tem svoje znanje utrdi in obnovi, nekatera vprašanja pa ga spodbudijo k lastnemu razmišljanju in temu, da tudi sam poišče nekatere informacije, ki v besedilu mogoče niso dostopne ali v celoti razložene.

Cilj praktikuma je skozi celotno besedilo bralce seznaniti z osnovnimi pojmi in elementi korporativne varnosti, njenim zgodovinskim pregledom ter drugimi informacijami, kot so: kaj je analiza tveganj in kako se opravi, kaj je načrtovanje korporativne varnosti in varnostnih ukrepov, kaj to sploh pomeni ter tudi specifičnih področij, kot so fizična, tehnična, informacijska in finančna varnost skupaj z varovanjem zaposlenih in objektov.

V delu »Posebne teme v korporativni varnosti« so predstavljeni poslovna skrivnost, zaščita intelektualne lastnine, menedžment varovanja in njegove odgovornosti, krizni menedžment ter načini reševanja sporov v organizaciji. Cilj praktikuma je skozi celotno besedilo bralce seznaniti z integralno korporativno varnostjo, kar na splošno pomeni z vsem, kar korporativno varnost tvori in kar je na tem področju pomembno za vzpostavitev varnosti. Z razumevanjem vsebine celotnega praktikuma postane razumevanje korporativne varnosti lažje. Poleg tega pa odgovarjanje na vprašanja bralca spodbuja k lastnemu mišljenju, ki se nadgrajuje z vsakim poglavjem posebej.

Univerzitetna založba
Univerze v Mariboru

2 Uvod v korporativno varnost

Varnost je ena izmed pomembnejših prvin obstoja in razvoja človeštva. Dejavnost, katere cilj je v organizacijah zagotoviti varnost, se imenuje korporativna varnost. Dvojmoč (2021) jo označuje kot celostno varnost, katere cilj je odprava neželenih situacij v organizacijah. Čeprav sam razvoj korporativne varnosti sega v 1990. leta, se o njej ne govori in se ji ne posveča dovolj pozornosti (Dvojmoč, 2017a).

2.1 Pomen korporativne varnosti

Če želi organizacija delovati uspešno, se mora zavedati vseh morebitnih nevarnosti in dejstva, da je celovito obvladovanje tveganj in neprekinjenega poslovanja nujni dejavnik za uspešno in neprekinjeno poslovanje (Gerginova, 2018).

Prav tako mora imeti organizacija za uspešno in nemoteno delovanje vzpostavljen sistem korporativne varnosti. Integralna korporativna varnost skrbi za zagotavljanje varnosti v organizacijah in je opredeljena kot zaščita premoženja in poslovnih procesov v sami organizaciji, pri čemer so njeni ukrepi preventivni in tudi kurativni. Kot je zapisal Button (2014), je področje zasebnega varovanja in zasebne varnosti v zadnjih tridesetih letih postalo veliko bolj zanimivo za proučevanje in raziskovanje. Kljub temu pa področje integralne korporativne varnosti ostaja še dokaj nedotaknjeno oziroma mu je namenjeno veliko manj raziskovalnega prostora. Pri tem je treba opozoriti na dejstvo, da je področje integralne korporativne varnosti zelo pomembno za organizacije, njihovo uspešnost in ljudi, ki so v njih zaposleni (Dvojmoč, 2017a).

V najširšem pomenu besede je korporativna varnost dejavnost, ki identificira in izvaja ukrepe za obvladovanje tveganj v organizaciji. Vloga korporativne varnosti je zaščita organizacij, njene tehnologije, zaposlenih, tehničnih virov in vseh podatkov ter informacij strank tako pred notranjimi kot tudi zunanjimi grožnjami. Pomembno je, da izvajanje korporativne varnosti deluje v skladu z delovanjem celotne organizacije in njenih poslovnih procesov. To ima pomembno vlogo pri doseganju organizacijskih ciljev organizacije brez strahu pred nastankom tako finančne kot tudi materialne škode (Dvojmoč, 2019).

Po svoji definiciji je korporativna varnost integrirana in vsebuje izvajanje več različnih funkcij, ki jih je treba sinhronizirati (Vršec in Vršec, 2015). Dvojmoč (2017a) poudarja, da morajo organizacije sprejeti celosten pristop k zagotavljanju varnosti, kamor spada identifikacija tveganj, uvedba varnostnih ukrepov, usposabljanje zaposlenih, redno preverjanje in posodabljanje ter spremljanje morebitnih varnostnih incidentov. Na podlagi tega je vzpostavljen integriran sistem korporativne varnosti v organizaciji, ki identificira njena tveganja in oblikuje mehanizme za njihovo preprečevanje. Poleg tega bi morala tudi vsaka gospodarska družba oz. organizacija vzpostaviti ustrezno varnostno funkcijo na podlagi veljavne zakonodaje. Ta funkcija bi urejala in zagotavljala varstvo pred naravnimi in drugimi nesrečami, zaščito ter reševanje, varstvo okolja, požarno varnost, varnost in zdravje pri delu, varstvo osebnih in tajnih podatkov, varovanje poslovnih skrivnosti ter varovanje intelektualne lastnine (Dvojmoč, 2017a).

Integralno korporativno varnost sestavlja šest pravnih procesov. O vseh šestih procesih bomo podrobneje spregovorili v nadaljevanju, kjer bo vsak proces tudi bolj poglobljeno predstavljen. Omenjeni procesi so:

- pravno zagotavljanje zakonitega in nemotenega poslovanja,
- pravno zagotavljanje varnostnega »know-howa«, specifičnega za organizacijo
- pravna zaščita tehnologij in informacijskega sistema (varnost IT),
- pravna zaščita stvarnopravnih pravic in pravic intelektualne lastnine,
- pravno zagotavljanje zasebne varnosti,
- pravno zagotavljanje varnega delovnega mesta (Dvojmoč, 2020).

Pomembno je, da se organizacije pripravijo na varnostna tveganja, ki jih lahko doletijo. To naredijo s pomočjo varnostnih strategij, pri katerih morajo upoštevati varnostne standarde, ki so določeni z državnimi in mednarodnimi predpisi. Prav tako ima osebje organizacije ključno vlogo pri korporativni varnosti, kar pomeni, da mora imeti strokovno

znanje, kar vključuje poznavanje pojmov javne in zasebne varnosti, preprečevanje kaznivih dejanj, preprečevanje izgub, upravljanje z varnostnimi tveganji in podobno (Cassidy, 2021).

Zavedati se je treba tudi, da je odgovornost korporativne varnosti tudi skrb za to, da vsak udeleženec oziroma zaposleni v organizaciji opravlja svoje delo in s tem vlogo v varnostnem sistemu. Korporativna varnost je tako odgovorna za koordinacijo celotnega varnostnega sistema organizacije, kar vključuje sodelovanje z varnostnimi menedžerji oz. varnostno ekipo in z vsemi drugimi dejavnostmi v podjetju, ki skrbijo in se nanašajo na varnost, neprekinjeno poslovanje, obvladovanje tveganj in zaščito. Glede na to lahko povzamemo, da korporativna varnost sestoji iz tehničnega in fizičnega varovanja, informacijske varnosti, neprekinjenega poslovanja, analiziranja tveganj in njihovo ocenjevanje, načrtovanja in nadzora nad varnostnimi ukrepi ter preprečevanja mogočih incidentov. S tem je njen cilj premagovanje varnostnih tveganj in preživetje ter ostati v koraku s konkurenco ali pred njo (Cabric, 2015).

Dvojmoč (2021) korporativno varnost izenači tudi s terminom celostna varnost, katere cilj je odpraviti nezaželene situacije v organizaciji, kar so, kot že omenjeno, tveganja in grožnje, ki pretijo organizaciji. Te se odpravijo z zagotavljanjem varnega delovnega okolja, varovanjem ljudi, osebnih podatkov, fizičnim in tehničnim varovanjem, obveščevalnimi in protiobveščevalnimi ukrepi, zagotavljanjem nemotenega in zakonitega poslovanja ter drugimi ukrepi, ki so potrebni za poslovanje in delovanje organizacije.

2.2 Cilji korporativne varnosti

Korporativna varnost skrbi za ohranitev reda, spoštovanje zakonov in internih predpisov ter varnost ljudi in premoženja v organizaciji (Gostič, 2014).

Cilj korporativnega varnostnega sistema je zagotovitev notranje varnosti podjetja, kar se doseže z uporabo različnih ukrepov, ki se uveljavljajo na pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ravneh. Ukrepi morajo biti skladni s spoštovanjem zakonov in internih zapisov ter z zagotavljanjem varnosti ljudi in premoženja v podjetju (Dvojmoč, 2017a).

Kot je bilo že omenjeno, je korporativna varnost ključnega pomena za vzpostavitev celotnega sistema varnosti v organizacijah, kar vključuje različna področja. Cilj je zagotoviti fizično in tehnično varnost v organizaciji, katerima se pridružuje tudi informacijska varnost. Z analizo tveganj se naredi tudi ocenitev le-teh, na podlagi česar se

pripravita načrt in nadzor nad varnostnimi ukrepi, s katerimi se preprečujejo incidenti (Cabric, 2015). Pri tem je treba omeniti tudi neprekinjeno poslovanje organizacije, ki je prav tako del korporativne varnosti. Ta zagotavlja podporo organizaciji v primerih varnostnih incidentov in nepričakovanih sprememb v delovanju organizacije. Cilj neprekinjenega poslovanja je zagotovitev, da tudi v primeru incidentov in pojava tveganj organizacija še vedno lahko deluje ter posluje neprekinjeno in sproti obvladuje nastalo situacijo (Will in Brauweiler, 2020).

Seveda pa tudi vzpostavljen sistem korporativne varnosti ne bi bil mogoč brez izkušenih in izobraženih zaposlenih, ki so temelj delovanja in poslovanja vsake organizacije. Predvsem s tega vidika je pomembno in nujno, da organizacije svoje zaposlene izobražujejo in usposabljajo ter vzpostavijo skladen varnostni koncept in uvedejo sodobno varnostno tehnologijo. Cilj tega je uspešno in učinkovito preprečevanje tveganj ter konkurenčna prednost, kar organizaciji pomaga tudi pri splošnem ugledu (Urbach in Ahlemann, 2019). Bistveni cilj varnostnega menedžmenta je predvsem izboljšanje učinkovitosti poslovanja, preprečevanje prevar in zaščita same organizacije. Zraven prištevamo tudi dvig varnostne kulture pri zaposlenih in uvajanje novih strategij, tehnologij in metod za preprečevanje nevarnosti (Kovačič in Podvršič, 2014).

Cilj korporativne varnosti v organizacijah je tako razviti preventivne ukrepe, ki odpravljajo vsa tveganja, zmanjšati grožnje na najmanjšo mogočo mero, razviti načrt poslovanja v času krize, povečati konkurenčnost, produktivnost, izboljšati tehnologije in uvesti ukrepe, kadar pride do pojava varnostnih tveganj (Gerginova, 2016).

2.3 Zgodovinski pregled razvoja področja korporativne varnosti

Korporativna varnost oziroma ideja zanjo se je najprej pojavila na mednarodni ravni, in sicer v 1990. letih, ko se je prvič pojavila oziroma razvila ideja o oblikovanju korporativnega varnostnega mehanizma, katerega cilj sta bila sodelovanje svetovnih sil na azijsko-pacifiškem delu in preprečevanje medsebojnih konfliktov (Dvojmoč, 2019). Mehanizem je pomagal reševati določene varnostne cilje in zmanjšati napetosti v interakcijah med državami. Tako imenovani korporativni pristop je spodbujal države, da se osredotočijo na varnostno problematiko znotraj težav in iščejo kompromise pri varnostnih problematikah izven državnih meja (Dvojmoč, 2017a).

Po terorističnem napadu v New Yorku leta 2001 je korporativna varnost dobila pomembnejšo vlogo (Cavanagh, 2005). Narasla je ozaveščenost o korporativni varnosti, saj so si podjetja začela prizadevati za varnostno politiko, ki bi jim omogočila čim višjo

stopnjo varnosti. Prav tako so začeli uporabljati več varnostnih tehničnih sredstev, kot so varnostne kamere, alarmi in podobno. Zaposlovati so začeli korporativne varnostne menedžerje, katerih naloga je bila, da varnostno politiko podjetja dvignejo na višjo raven. Pri tem so imela manjša podjetja več težav kot večja, saj niso imela dovolj sredstev, s katerimi bi si lahko priskrbela nadgradnjo varnostnega sistema (Cavanagh, 2005).

V Sloveniji zakoni in drugi predpisi urejajo posamezne oblike zaščite v organizaciji. To so predvsem predpisi s področij, kot so zaščita premoženja, ekologija, logistika, varnost pri delu, industrijska lastnina, obramba, požarna varnost, ergonomija in druga področja varovanja. Sam razvoj korporativne varnosti lahko pojasnimo z zakoni, ki so nastajali in bili sprejeti čez leta in imajo vpliv oziroma so potrebni pri sistemu integralne korporativne varnosti (Dvojmoč, 2017a). Eden izmed teh zakonov je »Zakon o industrijski lastnini (ZIL-1)« (2001), ki ureja skoraj celotno področje le-te. Zraven spadajo sodno varstvo patentov, geografske označbe, znamke, modeli, trajanje in pridobitev. Ena izmed najpomembnejših funkcij pravic industrijske lastnine je konkurenčna funkcija. Naslednji zakon je »Zakon o zasebnem varovanju in obveznem organiziranju službe varovanja (ZZVO)«, ki je bil sprejet leta 1994. Zasebno varovanje je pomembno predvsem zaradi tega, ker dopolnjuje varstvo, ki je zagotovljeno z nacionalnovarnostnim sistemom. Pri tem je pomembno, da imajo izvajalci znanje tudi o potrošnikih oz. o njihovih potrebah. Doseči je treba učinkovito doseganje ciljev, kar pomeni minimalizacijo stroškov in maksimilizacijo rezultatov za organizacijo (Modic, Lobnikar in Dvojmoč, 2014). Korporativna varnost in njeno zagotavljanje potrebuje različne vrste vložkov, pri čemer se je treba zavedati, da so ti investicija in ne le nepotreben strošek za organizacijo. Leta 2003 je bil sprejet »Zakon o zasebnem varovanju (ZZasV)«, ki je bil leta 2011 nadgrajen (»ZZasV-1«, 2011). Leta 1994 je bil sprejet tudi »Zakon o detektivski dejavnosti (ZDD)«, ki je prinesel konec državnega monopola na področju varnosti. Zakon je bil z nekaterimi spremembami nadgrajen in sprejet leta 2011 (»ZDD-1«, 2011).

Leta 2001 je bil sprejet Zakon o tajnih podatkih (»Zakon o tajnih podatkih (ZTP)«, 2001), saj je vlada določila, da mora biti varovanje teh podatkov urejeno z zakonom. Po tem zakonu so se morali ravnati določeni državni organi, organi lokalnih skupnosti ter njihovi posamezniki in tudi nekateri drugi. Tajni podatki so podatki, ki so strateško pomembni za poslovanje in delovanje organizacije ter za njene poslovne partnerje. Z zakonom je bilo določeno, da morajo imeti vsi zaposleni, ki s temi podatki poslujejo, izdana dovoljenja za dostop. Z Zakonom o varstvu osebnih podatkov (»Zakon o varstvu osebnih podatkov (ZVOP-1)«, 2007) so določeni pogoji za zbiranje, obdelovanje in nadzor osebnih podatkov, poleg tega pa tudi namen uporabe ter varstvo teh podatkov (Dvojmoč, 2017a).

Predlog Zakona o kritični infrastrukturi je bil oblikovan leta 2016, njegov namen pa je bil predvsem določitev kritične infrastrukture v Republiki Sloveniji in načrtovanje ter urejanje njene zaščite, pristojnosti in odgovornosti organov ter organizacij. Zaščita kritične infrastrukture obsega dejavnosti, ki prispevajo k njenemu neprekinjenemu delovanju (Dvojmoč, 2017a). »Zakon o kritični infrastrukturi (ZKI)« je bil sprejet leta 2017 in je pomemben del nacionalne varnosti, saj bi nedelovanje kritične infrastrukture imelo resne posledice na celotno državo.

Poleg vseh omenjenih zakonov, ki so pomemben del in prispevajo k zagotavljanju integralne korporativne varnosti, moramo upoštevati tudi zakonodajo nekaterih drugih področij, kot so informacijska varnost, zavarovalništvo, bančni sistemi, varnost in zdravje pri delu ter še mnoga druga (Dvojmoč, 2017a).

Sam razvoj korporativne varnosti organizacij lahko razdelimo na pet faz (Walby in Lippert, 2014). Prva faza je poimenovana zelena barka in ponazarja nizek položaj delavcev, ki so včasih skrbeli za varnost podjetij. Ti delavci oziroma varnostno osebje so bili slabo cenjeni, prav tako pa je bilo slabo cenjeno tudi njihovo delo. Poleg tega na razpolago niso imeli dobrih tehničnih sredstev, s katerimi bi lahko zagotavljali varnost v organizacijah. Druga faza je imenovana fizična varnost in predstavlja fazo, v kateri se je korporativna varnost osredotočala na preprečevanje izgub. V tej fazi je varnostno osebje tako na vstopnih kot tudi na izstopnih točkah povečalo svoje kontrole. Naslednja, tretja faza, se imenuje korporativna varnost in predstavlja fazo, s katero so podjetja sprejela večplasten pristop k varnosti. Podjetja so v tej fazi v svoj splošni poslovni načrt vključila korporativno varnost. Četrta faza se imenuje popolna zaščita premoženja, v kateri sta vsaka stvar in vsak posameznik v organizaciji ovrednotena kot sredstvo ali tveganje. Zaradi tega se interesi v tej fazi usklajujejo z interesi varnostne politike. V zadnji, peti fazi, se korporativna varnost vključi v javne in vladne organe, ki želijo tudi na državni ravni doseči četrto fazo oziroma popolno zaščito premoženja (Walby in Lippert, 2014).

2.4 Trenutni izzivi v korporativni varnosti

Izziv, ki je v zadnjih letih pokazal, kako zelo pomembno je nemoteno delovanje organizacij, je predvsem kriza oz. pandemija covida-19. Zagotavljanje varnosti v kriznih situacijah predstavlja kompleksen izziv za organizacije in se ga je treba lotiti sistematično ter skladno z regulativo. V takšnih situacijah je nujna vzpostavitev kriznega vodenja. S tem se vzpostavi krizna ekipa, ki vodi vse dejavnosti v času krize, opredeli vse nevarnosti in tveganja ter predaja navodila in smernice drugim v organizaciji (Čeč, 2020).

Z razvojem tehnologije in postopki digitalizacije tako v javnem kot tudi v zasebnem sektorju se je povečala pomembnost korporativne varnosti. S pojavom novih tehnologij se pojavljajo tudi nove oblike groženj, ki bi lahko ogrozile delovanje oziroma poslovanje organizacij. Kibernetska varnost je pomembna komponenta korporativne varnosti, saj zaščiti organizacijo, njene tehnologije, zaposlene, tehnične vire in podatke pred grožnjami. Pri tem gre tudi za preprečevanje dostopov do informacij in informacijskih sistemov (Dvojmoč, 2017a). Organizacije so vedno bolj odvisne od digitalnih sistemov, zato je pomembno, da se razvije korporativna varnost, ki bi preprečila naključne in zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost in zaupnost shranjenih podatkov (Markelj in Završnik, 2016).

Informacijski sistemi predstavljajo nevarnost tudi zaradi sprememb in rotacije papirnega dela v elektronsko obliko ter podatkovne zbirke. Čeprav je ta način učinkovitejši in lažji, pa je ravno zaradi večje povezljivosti ter lažjega dostopa sistem zelo ranljiv (ISACA, 2023).

Korporativna varnost je osredotočena predvsem na zagotavljanje varnosti svojih strank, objektov in sistemov. Zaradi tehnološkega napredka in vse več elektronskega poslovanja so podatki postali najpomembnejše sredstvo vsake organizacije (Fakiha, 2021). Izziv organizacijam predstavlja samo varovanje podatkov, saj jim njihovo uhajanje lahko povzroči velike izgube, kraje, okužbe sistemov in škodi ugledu celotne organizacije (Mukharjee, 2019).

Izziv predstavljajo tudi podjetja, ki jih je država določila kot kritično infrastrukturo. Prekinitev njihovega delovanja ali celo njihovo uničenje bi močno vplivalo na nacionalno varnost, gospodarstvo in druge družbene funkcije ter imelo tudi resne posledice nanje. Poleg tega bi vplivalo tudi na zdravje, varnost, blaginjo in zaščito ljudi. Te organizacije so na primer bolnišnice, telekomunikacijska podjetja, energetska podjetja, promet (letalski, železniški in pomorski), banke in podobno (Sotlar in Dvojmoč, 2021).

Prav tako se nenehno spreminja globalno varnostno okolje, in sicer se pojavljajo nove oblike varnostnih tveganj, ki imajo negativni vpliv na poslovanje in s tem tudi na varnost zaposlenih ter premoženje samo. Globalizacija na splošno je prinesla tako pozitivne kot tudi negativne stvari. Med negativne lahko prištejemo varnostne izzive, organizirano kriminaliteto, terorizem, kibernetske napade, deviantnosti zaposlenih in odtujitve ključnih poslovnih organizacij podjetja (Čaleta, 2017).

Odgovorite na vprašanja

Kako bi z lastnimi besedami zapisali, kaj je integralna korporativna varnost?

Kako lahko organizacija deluje uspešno? Pojasnite.

Naštejte 6 pravnih procesov integralne korporativne varnosti.

Kako je opredeljena integralna korporativna varnost?

Kaj je odgovornost korporativne varnosti in kako bi jo opisali s svojimi besedami?

Katere funkcije izvaja korporativna varnost?

Kaj je cilj korporativne varnosti? Pojasnite.

Kdaj se je korporativna varnost začela razvijati? Kateri dogodek je poskrbel za to, da je postala vidnejša?

Opišite razvoj korporativne varnosti v Sloveniji.

Ali se vam zdi, da je korporativna varnost v Sloveniji dovolj razvita? Razmislite in pojasnite.

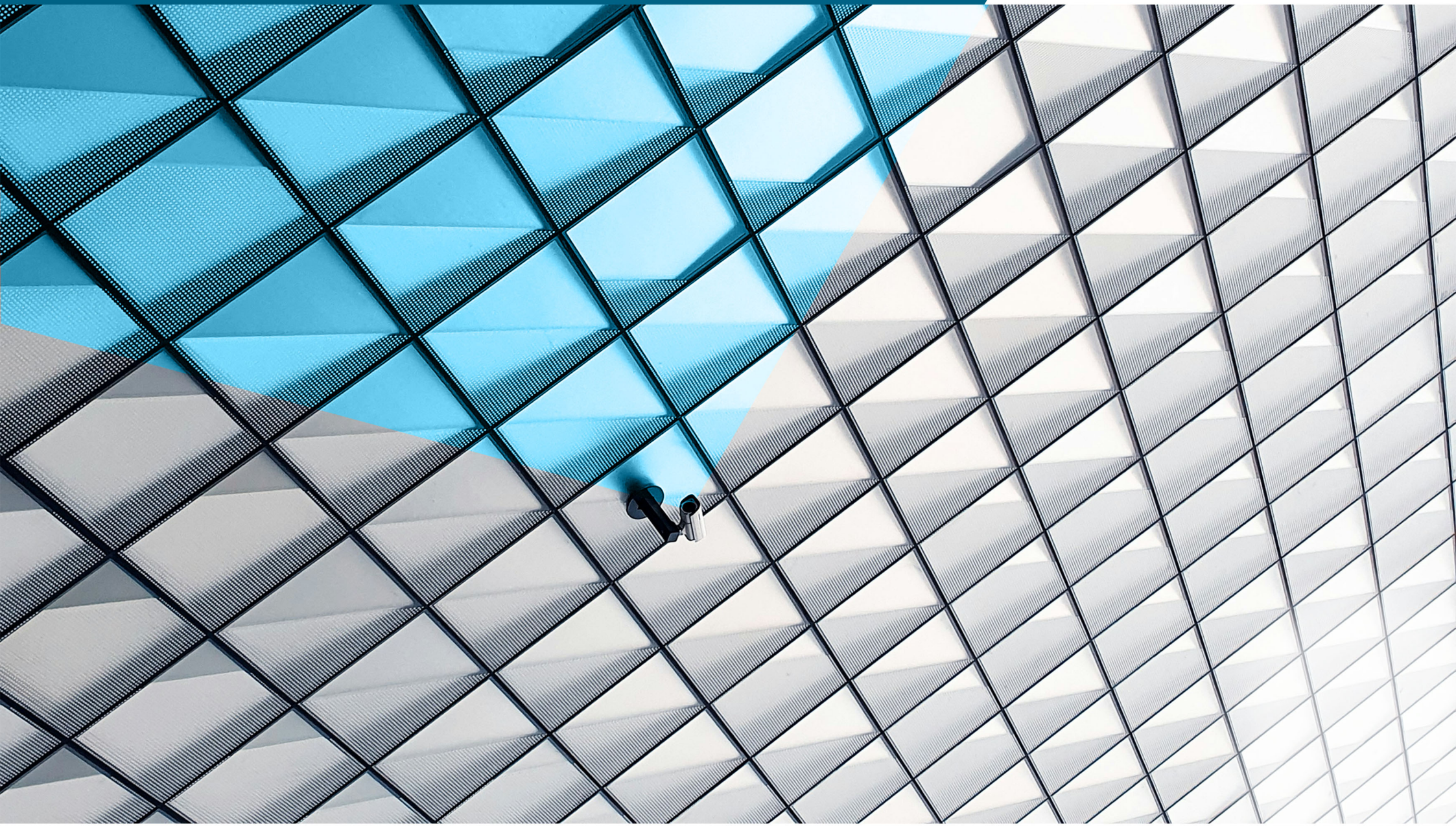
Na katerih 5 faz je razdeljen razvoj korporativne varnosti? Naštejte in opišite faze.

Kateri so po vašem mnenju trenutni izzivi v korporativni varnosti?

Kako je epidemija covida-19 vplivala na korporativno varnost?

ZAPISKI

DEL I



OSNOVE KORPORATIVNE VARNOSTI

Univerzitetna založba
Univerze v Mariboru

3 Definicija korporativne varnosti

Definicij, kaj korporativna varnost pravzaprav je, je toliko, kot je avtorjev, saj jo vsak opredeljuje nekoliko drugače. Vseeno pa je Trivan (2013) na podlagi nekaterih definicij razvil svojo in določil, da korporativna varnost predstavlja prisotnost in/ali odsotnost nevarnosti za poslovne sisteme. Določenih je tudi več ključnih elementov korporativne varnosti, kamor spadajo na primer fizično in tehnično varovanje, informacijska varnost, neprekinjeno poslovanje, krizno upravljanje in drugo (Cabric, 2015). Pomembno vlogo ima tudi varnostni menedžer, ki mora biti dobro usposobljen in tudi izkušen (Kumar, 2014).

3.1 Ključni elementi in definicije korporativne varnosti

Korporativna varnost je dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v organizaciji. S tem predstavlja eno od osnovnih funkcij za samo delovanje le-te. Vpliva na organizacijo in na njeno uspešnost in s tem tudi na ljudi ter njihovo vedenje (Čaleta, 2018). Korporativna varnost zajema pravne, funkcionalne, organizacijske, tehnične in kadrovske ukrepe, spoštovanje zakonov, internih predpisov ter varnosti ljudi in samega premoženja v podjetju (Gostič, 2008). Zelo pomembno je, da organizacija na vodstvene položaje oziroma v ekipo postavi strokovnjake za varnost, saj je to ključno za upravljanje vseh prej omenjenih ukrepov (Ludbey, 2016). Omeniti je treba tudi dejstvo, da morajo organizacije oziroma varnostni menedžerji dobro poznati tveganja, saj na ta način lahko sprejmejo boljše odločitve in ukrepe, povezane z le-temi. To jim prinese optimalno uporabo virov in obvladovana

tveganja (Kandžič, 2021). Poleg tega je tudi sodelovanje drugih oddelkov z oddelkom korporativne varnosti izrednega pomena, saj je povezanost med njimi temelj za lažje reševanje nastalih kriznih situacij in soočanje s tveganji ter boj proti grožnjam. Ločevanje med oddelki ima lahko zelo slab, negativen vpliv na organizacijo in na njeno obvladovanje tveganj, v nekaterih primerih pa lahko predstavlja celo oviro ali grožnjo (Schneller idr., 2022).

Trivan (2013) je povzel nekaj definicij in določil, da korporativna varnost predstavlja prisotnost in/ali odsotnost namernih, malomarnih ali naključno nastalih nevarnosti na poslovne sisteme s področij organizirane kriminalitete, korupcije, poslovnih tajnosti, informacijske varnosti, fizične in tehnične varnosti ter varnosti in zdravja zaposlenih pri delu. Na podlagi tega je korporativna varnost strateška funkcija podjetja s ciljem doseganja varnega poslovnega uspeha. Vsebuje tudi odpravo vseh tveganj in nevarnosti, ki bi lahko vplivale na poslovne dejavnosti in doseganje poslovnih ciljev, zmanjšanje groženj na najmanjšo mogočo raven, vzdrževanje delovanja pod kriznimi pogoji ter vrnitev k normalnemu delovanju. Oseba, ki je običajno zadolžena za korporativno varnost v podjetju, je korporativni varnostni menedžer. Njegove naloge so določitev ciljev, načrtovanje, organizacija, izdajanje navodil, nadzor, usklajevanje in odgovornost za varne operativne razmere v podjetju. Upravljanje varnosti se nanaša na varovanje zaposlenih in premoženja (Trivan, 2013).

V teoriji in praksi se definicije korporativne varnosti precej razlikujejo. Po mnenju Walbya in Lipperta (2014) se korporativna varnost pojavlja kot primarna oblika varnosti 21. stoletja. Avtorja navajata tudi, da je korporativna varnost zagotavljanje varnosti, ki si prizadeva za doseganje organizacijskih ciljev organizacije (Dvojmoč, 2017a). Gerginova (2016) je korporativno varnost opredelila kot zaščito lastnine in poslovnih procesov, s katero bi se lahko preprečile in zmanjšale materialne izgube in bi se poskrbelo za varnostne interese lastnikov, zaščitilo dobiček ter premoženje pred različnimi nevarnostmi. Avtorica tudi meni, da obstaja velika razlika med pojmom korporativna varnost s praktičnega in teoretičnega vidika.

Cubbage in Brooks (2012) menita, da je naloga korporativne varnosti odkrivanje goljufij in kaznivih dejanj ter preučevanje konkretnih kriznih primerov organizacije, ki bi se jih morali strokovnjaki zavedati in zagotoviti učinkovito zaščito ljudi in sredstev. Markelj in Završnik (2016) poudarjata, da je korporativna varnost sistem za zagotavljanje notranje varnosti podjetij in obsega vrsto ukrepov. Avtorja prav tako menita, da je namen korporativne varnosti identificirati in izvesti vse potrebne sistemske ukrepe za

obvladovanje varnostnih tveganj v posamezni organizaciji ter predstavlja eno od funkcij korporacije (Dvojmoč, 2017a).

Ne glede na vse definicije o korporativni varnosti je Gerginova (2016) izpostavila, da vseeno primanjkuje natančna opredelitev pojma. Opredelitev korporativne varnosti po mnenju Walbyja in Lipperta (2014) predstavlja izziv, s čimer se strinja tudi Dvojmoč (2017a).

Ključni elementi korporativne varnosti so:

- fizično in tehnično varovanje ljudi in premoženj,
- varnost blagovnih znamk in ugleda podjetja,
- informacijska varnost,
- upravljanje oz. menedžment varnosti,
- preiskovanje, odkrivanje in preprečevanje kriminalitete,
- preiskave,
- upravljanje nefinančnih tveganj,
- neprekinjeno poslovanje in obnovitev po incidentu,
- krizno upravljanje. (Cabric, 2015)

Fizična varnost je minimalna človeška vrednota, kar pomeni, da je tudi človekova pravica (Chan, 2014). Pod fizično varovanje spadajo ljudje, oprema in grajeno okolje za nadzor določenih dostopnih točk znotraj organizacije (Brooks, 2010). Fizična varnost je opredeljena tudi kot varnost, ki poskrbi za preživetje (Rumelili, 2015). »ZZVO« (1994) je v Sloveniji prvič opredelil fizično varovanje, ki je bilo opredeljeno kot varovanje oseb in premoženja pred uničenjem, poškodovanjem, tatvino in drugimi oblikami škodljivega delovanja (Christián in Sotlar, 2018).

Glavni cilj fizičnega varovanja je varovanje ljudi in premoženja na nekem varovanem območju ali objektu (Varnost Ljubljana, 2020). Fizično varovanje vključuje tudi inženirske naprave v nekem določenem okolju, ki so zasnovane z namenom zmanjšanja groženj z nadziranjem gibanja (Coole in Brooks, 2021). Zahteva visoko stopnjo profesionalnosti, izurjenosti in popolno predanost, izvajajo pa ga specialisti, ki so za to usposobljeni (Policija, n. d. a).

Sistemi tehničnega varovanja predstavljajo različna tehnična sredstva in mehanske naprave, ki nudijo protivlomno varovanje, kontroliranje vstopnih ter izstopnih točk, pregledovanje oseb, prevoznih sredstev, prtljage in podobno (»ZZasV-1«, 2011).

Cilj uvajanja ukrepov fizičnega in tehničnega varovanja je predvsem preprečiti fizični dostop do informacijske tehnologije in gradiva; nepooblaščeno spreminjanje podatkov in informacij; izgubo, poškodovanje ali zlorabo informacijskih sistemov; prekinitev poslovnih procesov ter motenje v poslovnih prostorih (Hajtnik, 2020).

Dva ključna elementa korporativne varnosti oziroma podjetja sta tudi varnost in kakovost.

Varnost je ena izmed najpomembnejših dobrin v življenju vsakega posameznika. Pojem varnosti lahko obravnavamo kot osnovno človekovo pravico in hkrati temeljno dolžnost družbe in na podlagi tega lahko govorimo o globalni varnosti, varnosti na ravni države ter varnosti vsakega posameznika. Varnost nam ni dana sama po sebi, ampak si jo morajo posameznik, skupina oziroma vsa populacija zagotoviti sami (Golob, 2013).

Baldwin (2001) je med prvimi sistematično opredelil sedem glavnih vrst vprašanj:

1. Varnost za koga?
2. Varnost za katere vrednote?
3. Koliko varnosti?
4. Varnost pred katerimi grožnjami?
5. Varnost s katerimi sredstvi?
6. Varnost s kakšnimi stroški?
7. Varnost v katerem časovnem obdobju?

Varnost v podjetju se kaže na drugih poslovnih funkcijah podjetja, kot so proizvodno-tehnična, logistična, tržna, finančna, računovodska funkcija, kadrovska, informacijska in upravljavsko-poslovna funkcija. Formalne podlage zagotavljanja varnosti so zakonska določila iz različnih področij (zaščite premoženja, varstva pri delu, požarnega varstva, ekologije in podobno) ter standardi kakovosti (razni standardi ISO, najnovejši ISO 28000) (Dvojmoč, 2020).

Kakovost pa je kompleksna in večdisciplinarna veličina, ki jo moramo obravnavati z več vidikov. Je stopnja, v kateri skupek svojstvenih karakteristik izpolnjuje vnaprej znane zahteve.

Kakovost in varnost morata skupaj prispevati k čim boljšim poslovnim izidom podjetja.

3.2 Vloge in odgovornosti v korporativni varnosti

Vse gospodarske družbe in druge organizacije morajo na podlagi veljavne zakonodaje vzpostaviti ustrezno varnostno funkcijo oziroma varnostno delovanje, ki ureja in zagotavlja varstvo pred naravnimi in drugimi nesrečami, zaščito in reševanje (civilno zaščito), varstvo okolja, varstvo pred požari, varnost in zdravje pri delu, varstvo osebnih in tajnih podatkov, varovanje intelektualne in industrijske lastnine ter varovanje poslovnih skrivnosti (Dvojmoč, 2017a). V vsaki organizaciji je treba organizirati tudi fizično varovanje z varnostniki in varovanje s tehničnimi sredstvi – tehnično varovanje območij, osebja, premoženja, kapitala in dokumentacije, kar se organizira na podlagi lastne presoje in ocene ranljivosti, ogroženosti in varnostnih tveganj. Za določena področja morajo biti imenovane tudi odgovorne osebe, ki morajo biti tudi redno usposobljene (Dvojmoč, 2019). Imenovanje krovne odgovorne osebe je smiselno za izvajanje varnostne politike in za upravljanje varnostnega sistema. Ta oseba je varnostni menedžer, ki skrbi za ustrezen celostni potek varovanja (Gostič, 2008). V nekaterih organizacijah je oddelek korporativne varnosti tudi ločen od drugih z namenom zagotavljanja nemotenega poslovanja, varnostni menedžer pa je vodja oddelka.

Varnostni menedžerji so vodilni v varnostnih strukturah in sprejemajo odločitve, na podlagi katerih se potem oblikujejo varnostni ukrepi in imajo s tem pomembno vlogo v vsakdanjem delu organizacij (Reinfelder idr., 2019). Dejstvo je, da je vloga varnostnega menedžerja večja, če je varnostnih tveganj več, zaradi česar mora imeti posameznik tudi ustrezna znanja z različnih področij, kot so področje varnosti, kazenski pregon, informacijska varnost in podobno (Arion, 2010).

Strokovnjak za korporativno varnost mora biti dobro usposobljen, kar pomeni, da razume varnostna tveganja, s katerimi se spopada podjetje, in je sposoben izvesti notranjo revizijo varnostnih tveganj z namenom, da se varnostna funkcija podjetja ohrani. Usposobljen mora biti tudi za izvajanje notranje revizije standardov ISO z namenom, da se varnostne funkcije podjetja uskladijo s poslovnimi cilji in se vzdržujejo najvišji standardi kakovosti z najboljšimi svetovnimi varnostnimi praksami (Kumar, 2014). Poleg tega mora tudi dobro poznati celotno organizacijo, njen način poslovanja, strategije neprekinjenega poslovanja, kdo so njeni konkurenti in njen dobiček. Pomembno je, da ima dobre sposobnosti komunikacije, da zna voditi velike projekte in druge pri tem, da zna ustvarjati strategije ter razdeliti posameznike v ustrezne skupine. Pri svojem delu mora nenehno delovati v skladu z zakonodajo in drugimi predpisi (Arion, 2010). Veliko organizacij ima že vnaprej določena tudi interna pravila obnašanja, ki varnostnim menedžerjem pomagajo pri njihovih odločitvah v primeru etičnih dilem in moralnih konfliktov (Dvojmoč, 2017a).

Omenimo lahko tudi, da je potrebnih pet izpolnjenih komponent, da za neko organizacijo lahko rečemo, da je uspešna in učinkovita. Prva predstavlja nadarjen kader, kamor spadajo dobre selekcijske metode in vodstvene komponente. Druga je motivirano osebje, ki je neposredno povezano s samo uspešnostjo organizacije. Pod tretjo spada dobra menedžerska ekipa, ki je odgovorna za vodenje organizacije. Četrta komponenta predstavlja učinkovito strategijo za prehitevanje konkurence in je odvisna od raziskovanja ter poznavanja trendov v določeni industriji. Peta komponenta pa je sposobnost menedžerja, kamor spada njegovo spremljanje ravni nadarjenosti osebja in zaposlenih, ravni njihove motivacije, uspešnosti menedžerske ekipe ter učinkovitost strategije. Vseh teh pet komponent mora varnostni menedžer upoštevati v organizaciji, saj to vodi do njene uspešnosti in učinkovitosti (Hogan in Kaiser, 2005). Dober varnostni menedžer mora imeti poleg vseh že naštetih lastnosti tudi dobro razvit razum, logiko in čustveno inteligenco, kar mu pomaga pri vsakodnevnih opravilih in obveznostih. Na tak način se lažje spopada s stresnimi situacijami, spodbuja svoje zaposlene, navezuje stike in tudi komunicira (Sapiński idr., 2020).

3.3 Pristopi h korporativni varnosti

Varnost podjetja temelji predvsem na zagotovitvi sprememb v procesu upravljanja, s čimer se skozi procese podjetju zagotavlja sprejemanje tveganja na obvladljivo raven (Čaleta, 2011). Integralno korporativno varnost sestavlja šest glavnih procesov, in sicer:

- pravno zagotavljanje zakonitega in nemotenega poslovanja,
- pravno zagotavjanje varnostnega »know-howa«, specifičnega za organizacijo,
- pravno in fizično zaščito tehnologij in informacijskega sistema (IT varnost),
- pravno zaščito stvarnopravnih pravic in pravic intelektualne lastnine,
- zagotavljanje dejavnosti zasebne varnosti (security), kar določa uredba Vlade,
- zagotavljanje dejavnosti varnega delovnega mesta (safety). (Dvojmoč, 2020)

Prvi proces je pravno zagotavljanje zakonitega in nemotenega poslovanja, ki je za večino organizacij ključnega pomena. Z mehanizmi korporativne varnosti se ga zagotovi s pravno ureditvijo varnostnih vprašanj v zvezi s korporacijskim upravljanjem, pravno ureditvijo zaščite poslovnih skrivnosti in pravno ureditvijo protikorupcijskih procesov ter integritete zaposlenih. Drugi proces je pravno zagotavljanje »know-howa«, specifičnega za organizacijo, ki zajema preiskovanje in odkrivanje protipravnih dejanj v organizaciji, preiskovanje in odkrivanje preslepitev in prevar v škodo organizacije ter obveščevalno (OSINT) in kontraobveščevalno dejavnost. Pod tretji proces spada pravna zaščita tehnologij in informacijskega sistema (IT varnost) skupaj s kibernetsko varnostjo, ki je

zaradi razvoja tehnologij in groženj izredno pomembna. Zajema organizacijsko informacijsko varnost s pripravo in sprejemom ustreznih notranjih aktov, tehnično informacijsko varnost s pripravo in sprejemom ustreznih notranjih aktov ter spremljanje in nadzor nad izvajanjem navedenih pravil. Za organizacije je poudarek predvsem na zagotavljanju varnosti vseh podatkov in informacij, bodisi o zaposlenih ali o strankah. To se zagotovi, kot že omenjeno, z notranjimi akti in tudi z rednim preverjanjem nadzora nad mehanizmi, ki zagotavljajo kibernetsko varnost. Četrti proces predstavlja pravno zaščito stvarnopravnih pravic in pravic intelektualne lastnine ter zajema pravno varovanje lastninske pravice in drugih stvarnih pravic organizacije, pravno zaščito patentov, blagovnih znamk, modelov in porekla proizvodov ter pravno zaščito materialnih avtorskih pravic organizacije. Ta proces je pomemben predvsem z vidika delovanja sistemov v organizaciji, ki morajo v vseh situacijah delovati brezhibno, pri čemer je pomembno zagotoviti tudi, da ti niso izpostavljeni grožnjam, ki so lahko fizične ali virtualne. Peti proces je pravno zagotavljanje zasebne varnosti, pod katero spadajo pravna ureditev varovanja premoženja organizacije (»ZZasV-1«, 2011), pravna ureditev nadzora nad zunanjimi in notranjimi ogrožanji (»ZZasV-1«, 2011; »ZDD-1«, 2011) in pravna ureditev varnostnega načrtovanja. Zasebnovarnostna podjetja so odgovorna za varovanje premoženja v veliko organizacijah in tudi za zagotavljanje varnosti vseh zaposlenih, obiskovalcev in strank. Če pride do zunanjih ali notranjih groženj, k varnosti pripomorejo tudi detektivi, v primeru varnostnega načrtovanja pa tudi Civilna zaščita. Zadnji, šesti proces, je pravno zagotavljanje varnega delovnega mesta, in sicer pravna ureditev varovanja oseb ter osebnih podatkov, pravna ureditev varovanja okolja in pravna ureditev varnosti in zdravja na delovnem mestu. To je predvsem pomembno pri zagotavljanju varnosti zaposlenih, ki je izrednega pomena v organizacijah in zato tudi eden ključnih dejavnikov korporativne varnosti (Dvojmoč, 2020).

Vršec (2014) je prav tako opredelil procese, ki jih uvrščamo v sistem korporativne varnosti, izhajajoč iz integralnega varnostnega sistema, ki zajema vsa področja varnosti. Sistem upravljanja zajema naslednje procese:

- proces upravljanja zaščite in reševanja ter varstva okolja,
- proces upravljanja integriranega fizičnega in tehničnega varovanja,
- proces upravljanja varnosti in zdravja pri delu ter varstva pred požari in eksplozijami,
- proces upravljanja varstva podatkov in poslovnih skrivnosti,
- proces upravljanja varovanja informacij in elektronskih komunikacij,
- proces upravljanja zaščite blagovnih znamk, konkurenčnih prednosti in ugleda,
- proces upravljanja varnostne dokumentacije,

- proces upravljanja načrta varovanja in vzpostavljenega varnostnega režima,
- proces upravljanja varnostno-nadzornega centra – upravljanje izrednih dogodkov,
- proces upravljanja, vodenja in usposabljanja varnostnega osebja.

Poleg omenjenih procesov funkcija korporativne varnosti zajema tudi ukrepe za preprečevanje korupcije in drugih kriminalnih ravnanj. (Vršec, 2014)

Odgovorite na vprašanja

Katere ukrepe zajema korporativna varnost?

Kako je Trivan (2013) povzel, kaj je korporativna varnost? Opredelite s svojimi besedami.

Kaj je naloga korporativne varnosti?

Kateri so ključni elementi korporativne varnosti?

Na kratko opredelite zgoraj naštete elemente korporativne varnosti.

Kako bi opredelili pojem varnosti s svojimi besedami?

Kako se varnost kaže v podjetju?

Kaj je kakovost?

Zakaj je pomembno, da gospodarske družbe vzpostavijo ustrezno varnostno funkcijo oziroma varnostno delovanje?

Kaj mora biti organizirano/določeno v sami organizaciji?

Kdo je strokovnjak za korporativno varnost?

Katerih pet komponent mora biti izpolnjenih, da je organizacija uspešna in učinkovita?

Naštejte, katerih 6 procesov sestavlja integralno korporativno varnost.

Na kratko pojasnite vseh 6 zgoraj omenjenih procesov.

Katere procese zajema sistem upravljanja?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

4 Analiza tveganj

Za korporativno varnost je zelo pomembna tudi analiza tveganj, s katero se na podlagi določenih postopkov ocenijo možni škodljivi učinki le-teh (Molak, 1997). Z analizo tveganj se opravi tudi ocena tveganj, ki predstavlja postopek, pri katerem se ugotavljajo nevarnosti in dejavniki tveganja, ki bi lahko ogrozili delovanje organizacije, določijo pa se tudi načini za odpravo teh nevarnosti. Ocena tveganj je pomembna zaradi različnih razlogov in predvsem zaradi dejstva, da pripomore k celoviti korporativni varnosti organizacije (Infocenter, 2023). Poznamo pa tudi več pristopov, na podlagi katerih lahko organizacije ocenijo tveganja (Stevenson, 2022). Za varnost organizacije je potrebna tudi analiza SWOT, ki oceni prednosti, pomanjkljivosti, nevarnosti in priložnosti le-te. S pomočjo analize se določijo področja, ki so močnejša, in področja, ki so šibkejša ter predstavljajo priložnosti in grožnje.

4.1 Identifikacija in ocena tveganj

Tveganje lahko opredelimo kot prepoznano ali pa neprepoznano aktualno stanje, v katerem lahko zaradi ogroženosti in ranljivosti predmeta ogroženosti in negotovosti škodnega dogodka nastanejo škodne posledice. Strokovnjaki tveganja delijo na osebna, premoženjska in operativna tveganja (Golob, 2013). Prav tako je tveganje vsaka grožnja, ki ima vpliv na organizacijo in ima pogosto negativen vpliv na njeno delovanje, zaradi česar je njeno poslovanje moteno ali pa ima organizacija zaradi tega tudi denarno izgubo (Abdullah idr., 2017).

Tveganje je neizogibna sestavina sveta. Živimo v verjetnostno-deterministčnem svetu in tveganje je nujna razsežnost človeških dejavnosti. Ne moremo izbirati med tveganjem in netveganjem, ampak samo med različnimi stopnjami in vrstami tveganja. Tudi opustitev dejanja je tveganje (Kirn, 1995). Tveganje pomeni možnost dogodka, ki je drugačen od predvidenega, in izhaja iz nestabilnosti ter negotovosti prihodnjih dogodkov. Uspešno upravljanje s tveganji izhaja iz dobrega predvidevanja verjetnosti škodnega dogodka in obvladovanja odstopanj. Tveganja niso nov pojem v družbeni praksi, njihova obravnava obstaja že dolgo, v zadnjem obdobju pa se vse bolj uporablja znanstveni pristop, v katerem so tveganja kvantificirano ovrednotena in podprta z raznimi modeli ter analitičnimi orodji. Sam koncept tveganja ima tri elemente, in sicer:

- zaznavanje, da se nekaj lahko zgodi;
- verjetnost, da se nekaj dogaja in
- posledica, če se zgodi.

Ocena tveganja je izraz, ki se uporablja za opis celotnega postopka ali metode, pri kateri se ugotavlja, katere so nevarnosti in dejavniki tveganja, ki bi lahko povzročili škodo (ugotavljanje nevarnosti); analizira in oceni tveganje, ki je povezano z nevarnostjo (analiza tveganja in ocena tveganja), ter določi ustrezne načine za odpravo nevarnosti (obvladovanje tveganja) (Infocenter, 2023). Primarno vlogo ima ocena tveganja v panogah in na področjih, kritičnih za varnost. Sooča se z vrsto splošnih izzivov, ki so delno povezani s tehnološkim napredkom in naraščajočimi potrebami (Paltrinieri idr., 2019).

Z analizo tveganja se ocenijo možni škodljivi učinki. Ta vključuje:

- identifikacijo nevarnosti,
- določitev razmerja med koncentracijo tveganja in škodljivo posledico,
- analizo izpostavljenosti, ki vključuje kdo, koliko in na kakšen način je izpostavljen tveganju;
- karakterizacijo tveganja, ki naredi izračune z jasno navedenimi vsemi predpostavkami;
- obveščanje o tveganju. (Molak, 1997)

Oceno tveganja je treba opraviti pred uvedbo novih procesov ali dejavnosti; pred uvedbo sprememb v obstoječe procese ali dejavnosti in po tem, ko so ugotovljene nevarnosti (Infocenter, 2023). Dolžnost za opravljeno oceno tveganja je v rokah delodajalca, ki mora to opraviti sam ali pa za to najeti zunanjega sodelavca, ki oceno tveganja opravi v celoti.

Po opravljeni oceni mora delodajalec o rezultatih obvestiti pristojne posameznike, če že ne sodelujejo pri sami oceni (British Safety Council, 2023).

Dobro načrtovanje je bistveno za učinkovito izvedbo ocene tveganja. Pri tem je treba upoštevati štiri elemente, in sicer obseg, vire, vpletenost osebja in zakonske določbe. Prvi element je obseg, ki pomeni, da je treba določiti obseg pri samem načrtovanju ocene tveganja. To nam pomaga ugotoviti, kateri viri so potrebni. Drugi element so viri, kar pomeni, da je treba določiti vrsto usposabljanja, orodij, opreme in drugih sredstev, ki jih organizacija potrebuje za učinkovito izvedbo ocene tveganja. Določiti se morajo tudi ukrepi analize tveganja, ki bodo uporabljeni, pri tem pa je pomembno vedeti, zakaj so izbrani ukrepi res primerni. Naslednji element je vpletenost osebja, kamor štejemo osebje, ki je vključeno v načrtovanje in izvajanje ocene tveganja. To so lahko menedžerji, nadzorniki, delavci ali dobavitelji. Z določitvijo osebja lažje prepoznamo tudi dodatne vire, ki nam lahko pomagajo izboljšati učinkovitost ocene tveganja. Zadnji element so zakonske določbe. Pri celotnem oblikovanju ocene tveganja je nujno upoštevati zakone, predpise in notranje pravilnike, saj lahko neupoštevanje le-teh povzroči denarne kazni in druge prekrške, ki bi lahko ogrozili delovanje celotne organizacije (Andales, 2023).

Z vidika poslovanja organizacije tveganje ni le posledica porazdelitve negotovih dogodkov v prihodnosti, temveč je tudi posledica nepopolnih ali nekakovostnih informacij, ki jih organizacija uporablja za sprejemanje poslovnih odločitev. Ocenjevanje tveganja v organizaciji zahteva tudi razmislek o zaznavi tveganja, ki je izrazito subjektivna kategorija. Zaznava tveganja poteka na individualni osnovi, rezultati ocenjevanja pa so običajno skupinski. Obravnava tveganj omogoča organizaciji izkoristiti priložnost, če ta pri upravljanju tveganj določene dogodke prepozna in izkoristi kot priložnosti. Je dejavnost, ki se ukvarja z identificiranjem nenormalnih situacij, ki bi lahko imele negativne posledice na poslovanje in finančno stanje organizacije, ter z izbiro ukrepov za zmanjšanje oziroma odpravo škode, ki bi jo povzročili ti pojavi (Molak, 1997).

Pri zaznavi tveganja izhajamo iz osnovne predpostavke, da poslovno okolje organizacije ni stalno in predvidljivo. Brez tveganja bi bilo vse vnaprej jasno in tako bi bili vsi dogodki v poslovnem okolju odvisni le od sosledja vzrokov in posledic. Pri zaznavi tveganja pa se je treba zavedati, da se to ocenjuje v razmerju do neke koristi.

Ocenjevanje tveganja zahteva presojo vrednostne narave sveta in zmožnost inteligentnega razmišljanja o malo verjetnih, toda pomembnih dogodkih. Tveganjem, povezanimi z različnimi dogodki, praviloma pripisujemo verjetnostno naravo in jih ocenjujemo kot bolj ali manj verjetne ter v skladu s tem tudi sprejemamo določene poslovne odločitve.

Rezultati raziskav psiholoških eksperimentov kažejo, da posamezniki niso ravno najboljši ocenjevalci verjetnosti in da sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo. Njihove izbire velikokrat ne ustrezajo osnovnim zahtevam doslednosti in skladnosti. Pri teh kršitvah se pogosto uporabljajo posebne hevristike, s katerimi se težave s presojo resničnosti poenostavijo (Kirn, 1995).

Dejavniki, ki vplivajo na zaznavanje in ovrednotenje tveganja, so številni, nekateri so posameznikom bolj, nekateri pa manj sprejemljivi. Bolj sprejemljivi so naslednji: prostovoljni, naravni, pod nadzorom, se nanašajo na druge, so nujni, so čutno zaznavni, se nanašajo na samooceno in podobni. Med manj sprejemljive dejavnike spadajo naslednji: neprostovoljni, človeški, so zunaj nadzora, imajo takojšnji učinek, se nanašajo na nas, niso nujni, so precenjeni, so nerazumljeni, neznani in podobno.

Ocena tveganja je pomembna zaradi številnih razlogov, saj pomaga pri: ustvarjanju zavedanja o nevarnostih in tveganjih; ugotavljanju, kdo bi lahko bil ogrožen; ugotavljanju, ali so obstoječi ukrepi ustrezni; določitvi razvrščanja nevarnosti; izpolnjevanju zakonskih zahtev in podobno. Cilj ocene tveganja pa je oceniti nevarnosti in jih odpraviti oziroma zmanjšati raven njihovega tveganja z različnimi ukrepi. S tem se zagotovi in ustvari varnejše in zdravo delovno okolje (Infocenter, 2023).

V zvezi z zaznavanjem sta prisotna na eni strani podcenjevanje in na drugi strani precenjevanje tveganja. Običajno posamezniki podcenjujejo tveganja za znana ogrožanja in za tista, ki jih lahko kontrolirajo, precenjujejo pa tveganja za neznana ogrožanja in za tista, ki so zunaj zmožnosti človekove kontrole.

Za oceno tveganja je treba pripraviti tudi določeno dokumentacijo. Sama raven dokumentacije je odvisna od stopnje tveganja, zakonskih zahtev in zahtev morebitnih veljavnih sistemov upravljanja. Prav tako mora biti iz dokumentacije razvidno, da je bil izveden dober pregled nevarnosti, da so bila določena tveganja za nevarnosti, izvedeni nadzorni ukrepi, primerni za tveganje, in pregledane vse nevarnosti na delovnem mestu (Infocenter, 2023).

4.2 Metode analize tveganj v korporativni varnosti

Analiza tveganja zagotavlja strukturiran pristop za ocenjevanje negotovosti, kar povečuje prilagodljivost organizacije in dolgoročni uspeh. Z analizo tveganj organizacije predvidijo in zmanjšajo učinek škodljivih posledic; ocenijo potencialna tveganja; načrtujejo odzive na

različne situacije; ugotovijo vpliv sprememb v delovnem okolju ter razporedijo vire, kot so čas, denar in zaposleni, tja, kjer so najbolj potrebni (Yasar, 2023).

Organizacije lahko uporabijo več pristopov za ocenjevanje tveganj, in sicer kvantitativno metodo, kvalitativno metodo, polkvalitativno metodo, metodo na podlagi sredstev, metodo na podlagi ranljivosti in metodo na podlagi groženj. Vsaka metoda lahko oceni stopnjo tveganja organizacije (Stevenson, 2022).

- Kvantitativna metoda

Kvantitativne metode vnesejo v proces analitično strogost. Dobljeno oceno tveganja je nato mogoče predstaviti v finančnih izrazih, ki jih vodstvo in člani uprav zlahka razumejo. Analize stroškov in koristi omogočajo nosilcem odločanja, da določijo prednostne možnosti ublažitve. Vendar pa kvantitativna metoda morda ni ustrezna, saj nekatera sredstva ali tveganja niso preprosto merljiva.

Tudi kvantitativne metode so lahko precej zapletene. Poleg tega nekatere organizacije nimajo notranjega strokovnega znanja, ki ga zahtevajo kvantitativne ocene tveganja. Organizacije pogosto prevzamejo dodatne stroške, da privabijo tehnična in finančna znanja svetovalcev (Stevenson, 2022).

- Kvalitativna metoda

Če kvantitativne metode uporabljajo znanstveni pristop k oceni tveganja, imajo kvalitativne metode bolj novinarski pristop. Ocenjevalci se srečujejo z ljudmi v celotni organizaciji. Zaposleni delijo informacije o tem, kako oziroma ali bi lahko opravili svoje delo, če bi sistem prenehal delovati. Ocenjevalci uporabljajo ta vnos za kategorizacijo tveganj na grobih lestvicah, kot so visoko, srednje ali nizko. Kvalitativna ocena tveganja daje splošno sliko o tem, kako tveganja vplivajo na poslovanje organizacije. Kvalitativne metode so široko uporabljena sredstva za podjetja, da ocenijo in spremljajo vsakodnevna tveganja, s katerimi se le-ta soočajo (Horvath, 2023).

Poleg tega se kvalitativne metode štejejo za uspešnejše in učinkovitejše, saj informacije predstavljajo v širšem in bolj opisnem smislu. To je predvsem pomembno za podjetja in njihovo podatkovno analitiko, saj kvalitativni pristop omogoča globlje razumevanje dejavnikov tveganja in njihovega potencialnega vpliva na procese odločanja, ki temeljijo na podatkih. Sam postopek ima več prednosti, med katerimi so tudi ocenjevanje brez

orodij ali programske opreme, s čimer se prihranita čas in denar. Končna ocena tveganja pa je poleg tega tudi preprosta za branje, kar vodjem olajša delo (Michelle, 2023).

– Polkvantitativna metoda

Nekatere organizacije bodo združile prejšnje metode za ustvarjanje polkvantitativnih ocen tveganja. S tem pristopom bodo organizacije uporabile številčno lestvico, na primer 1–10 ali 1–100, za dodelitev številčne vrednosti tveganja. Tvegani elementi, ki so ocenjeni v spodnji tretjini, so razvrščeni kot nizko tveganje, srednja tretjina kot srednje tveganje in višja tretjina kot visoko tveganje (Stevenson, 2022). Pri polkvalitativni oceni tveganja so nekateri vidiki ocene tveganja kvantificirani z matematičnimi in statističnimi metodami, nekateri pa so ovrednoteni s subjektivnimi presojami in strokovnimi mnenji (Drata, 2023a).

Z mešanjem kvantitativnih in kvalitativnih metod se izognemo intenzivnim izračunom verjetnosti in vrednosti sredstev prve, hkrati pa ustvarimo več analitičnih ocen kot druge. Polkvantitativne metode so lahko bolj objektivne in zagotavljajo dobro osnovo za prednostno razvrščanje postavk tveganja. Uporabljajo se predvsem v primerih, ko so informacije, ki so na voljo za kvantitativno oceno tveganja, omejene ali nezanesljive (Drata, 2023a).

– Metoda na podlagi sredstev

Vsaka organizacija je edinstvena v svoji strukturi, vrstah informacij, ki jih obdeluje, in načinu delovanja in ravno zato mora biti pristop k varstvu podatkov unikaten. Pomembno je predvsem to, da postopki in ukrepi za varnost informacij ustrezajo grožnjam, s katerimi se organizacija sooča. Organizacije za ocenjevanje IT tveganja običajno uporabljajo pristop, ki temelji na sredstvih. Sredstva so sestavljena iz strojne in programske opreme ter omrežij, ki obdelujejo informacije organizacije. Ocena na podlagi sredstev običajno poteka v štirih korakih:

- Popis vseh sredstev.
- Ocena učinkovitosti obstoječih kontrol.
- Ugotovitev grožnje in ranljivosti vsakega sredstva.
- Ocenitev potencialnega vpliva vsakega tveganja. (Irwin, 2022)

Pristopi, ki temeljijo na sredstvih, so priljubljeni, ker se ujemajo s strukturo, delovanjem in kulturo oddelka IT. Tveganja in kontrole požarnega zidu je preprosto razumeti.

Vendar pristopi, ki temeljijo na sredstvih, ne morejo dati popolne ocene tveganja. Nekatera tveganja niso del informacijske infrastrukture. Politike, procesi in drugi »mehki« dejavniki lahko organizacijo izpostavijo tolikšni nevarnosti kot nepopravljen požarni zid (Stevenson, 2022).

– Metoda na podlagi ranljivosti

Metode, ki temeljijo na ranljivosti, širijo obseg ocen tveganja zunaj sredstev organizacije. Ranljivost je šibkost ali vrzel v obrambi organizacije, ki bi jo napadalec lahko izkoristil za pridobitev nepooblaščenega dostopa do občutljivih informacij ali motenje poslovanja. Ta proces oz. ocena tveganja na podlagi ranljivosti se začne s pregledom znanih slabosti in pomanjkljivosti znotraj organizacijskih sistemov ali okolij, v katerih ti sistemi delujejo. Prav tako je treba identificirati in razvrstiti tudi sredstva organizacije glede na njihovo vrednost, pomembnost in ranljivost glede na tveganja. Od tam ocenjevalci identificirajo možne grožnje, ki bi lahko izkoristile te ranljivosti, skupaj s potencialnimi posledicami izkoriščanja. Povezovanje ocen tveganja na podlagi ranljivosti s postopkom upravljanja ranljivosti organizacije dokazuje učinkovito obvladovanje tveganja in procese upravljanja ranljivosti (Drata, 2023b).

Čeprav ta pristop zajame več tveganj kot ocena, ki temelji izključno na sredstvih, temelji na znanih ranljivostih in morda ne zajame celotnega obsega groženj, s katerimi se sooča organizacija (Stevenson, 2022). Rezultati ocene tveganja na podlagi ranljivosti se lahko uporabijo za informiranje pri odločanju in usmerjanju razvoja načrta za obvladovanje tveganj (Drata, 2023b).

– Metoda na podlagi groženj

Metode, ki temeljijo na grožnjah, lahko zagotovijo popolnejšo oceno splošnega tveganja organizacije. Ta pristop ocenjuje pogoje, ki ustvarjajo tveganje. Revizija sredstev je del ocene, saj sredstva in njihove kontrole prispevajo k tem pogojem. Pristopi, ki temeljijo na grožnjah, gledajo onkraj fizične infrastrukture.

Z ocenjevanjem tehnik, ki jih na primer uporabljajo akterji groženj, lahko ocene ponovno razvrstijo možnosti ublažitve. Usposabljanje o kibernetski varnosti blaži napade socialnega inženiringa. Ocena na podlagi sredstev lahko daje prednost sistemskim kontrolam pred

usposabljanjem zaposlenih. Po drugi strani pa lahko ocena na podlagi groženj ugotovi, da povečanje pogostosti usposabljanja o kibernetski varnosti zmanjša tveganje ob nižji ceni (Stevenson, 2022).

Nobena izmed omenjenih metod ni popolna, saj ima vsaka svoje prednosti in slabosti. Dobro pa je, da se nobena med seboj ne izključuje. Izbira metode je odvisna predvsem od tega, kaj želimo doseči in tudi od same narave organizacije (Stevenson, 2022).

Analiza tveganj je pomemben del varnosti vseh organizacij in njihovega poslovanja. Tveganja lahko neposredno vplivajo na uspeh poslovanja in delovanja ter na samo organizacijo s tem, da povzročijo izgubo ugleda, prihodkov in podobno. Za zaščito organizacije in njenega poslovanja pred tveganji in grožnjami je pomembno ukrepati, še preden do tega sploh pride. Pri tem pa so za pomoč organizacijam na voljo tudi certificirani strokovnjaki za obvladovanje tveganj (Horvath, 2023).

4.3 Vrednotenje tveganj in prioritetizacija ukrepov

Zaradi kompleksnosti zaznave tveganj se zastavljajo vprašanja o merilih za njihovo upravljanje. V zvezi z ocenjevanjem in upravljanjem tveganja je opredeljenih deset osnovnih vprašanj, ki so naslednja:

- Kako določimo, koliko varno je dovolj varno?
- Kako dobri so baza znanja in metode ocenjevanja tveganja?
- Kako so ocene tveganja vključene v proces odločanja?
- Kako odločevalci obravnavajo negotovosti različnih tveganj in ogrožanj?
- Kako značilnosti institucij vplivajo na telesa, ki odločajo o tveganjih in ogrožanjih?
- Kateri dejavniki vplivajo na zaznave tveganj in koristi posameznikov?
- Kako so zaznave tveganj in koristi posameznikov vključene v javne politike?
- Kako družba obravnava tveganja, ki so nesprejemljiva za neki del družbe?
- Kako so normativne presoje (nepristranost, pravičnost) uravnotežene v procesu odločanja o tveganju?
- Katera so merila za primerjavo in ovrednotenje različnih politik upravljanja?

Iz zgoraj navedenega je razvidno, da pojem tveganja vsebuje vsaj tri bistvene elemente, in sicer neželene posledice, možnost pojavljanja ter sodbe o dejanskosti.

4.4 Analiza SWOT

Analiza SWOT oceni prednosti, slabosti, priložnosti in nevarnosti (grožnje), s katerimi se sooča podjetje oziroma organizacija. Pomaga ugotoviti, kje je organizacija močna in kje šibka, kateri zunanji dejavniki bi lahko pripomogli ali škodovali njenemu uspehu in katera področja poslovanja bodo morda zahtevala več pozornosti za rast. Je pomembno orodje za analizo varnosti in določitev načinov za njeno izboljšanje v prihodnosti (Thinkcurity, 2022).

S – Strengths (prednosti), W – Weaknesses (pomanjkljivosti, slabosti), O – Opportunities (priložnosti) in T – Threats (nevarnosti). Že po teh štirih besedah vidimo, da gre za analizo, ki analizira vse, kar se v organizaciji lahko izkoristi, da bo v njeno korist. Z analizo SWOT se prav tako zmanjša možnosti za neuspeh, saj nam pomaga, da ugotovimo, kaj organizaciji primanjkuje, in odpravimo nevarnosti, ki ji pretijo (Mind Tools Content Team, 2023).
Analiza SWOT se uporablja za oceno konkurenčnega položaja organizacije in tudi za razvoj strateškega načrtovanja. Poleg (zunanjih in notranjih) dejavnikov oceni tudi trenutni in prihodnji potencial. Kot je bilo že omenjeno, to pomaga ugotoviti, katere so prednosti in katere slabosti organizacije. Analiza predstavlja tudi tehniko za oceno uspešnosti, tveganja, konkurenčnosti in samega potenciala organizacije, kamor spada tudi njeno delo (Kenton, 2023).

Najprej je treba določiti, katere so prednosti in katere slabosti. To so notranji dejavniki, ki vplivajo na poslovanje organizacije. Slabosti so lahko pomanjkanje spletne prisotnosti ali pomanjkanje denarnih rezerv za kritje nepričakovanih stroškov. Nato se določijo še priložnosti in nevarnosti, ki predstavljajo zunanje dejavnike, ki vplivajo na organizacijo in njeno uspešnost. Primer priložnosti je na primer širitev na nove trge. Grožnja oziroma nevarnost pa bi lahko vključevala konkurente, ki ponujajo cenovno ugodnejše storitve (Thinkcurity, 2022).

Prednosti v analizi SWOT so ugodne notranje dejavnosti, procesi in vedenja podjetja, torej tisto, kar podjetje počne dobro. To so dejavniki, ki prispevajo k uspehu podjetja in njegove blagovne znamke. Slabosti so notranji dejavniki, ki zavirajo podjetje. Lahko so posledica kulture podjetja, pomanjkanja virov ali pomanjkanja procesov upravljanja. Prepoznavanje slabosti je bistvenega pomena za vsako analizo SWOT, saj omogoča, da se prepoznajo področja, na katerih so mogoče oziroma nujne izboljšave, s čimer se poveča poslovanje in pridobi nove stranke (Thinkcurity, 2022).

Priložnosti in nevarnosti/grožnje so zunanje – stvari se dogajajo zunaj vašega podjetja, na večjem trgu. Priložnosti so možnosti, da se zgodi nekaj pozitivnega, in prav tako prispevajo svoj del k uspehu. Običajno izhajajo iz situacij zunaj organizacije in zahtevajo pogled na to, kaj se lahko zgodi v prihodnosti. Pri priložnostih se moramo vprašati na način, kot sta: *Kako uspešni smo na trgu? Ali imamo na trgu nekaj, kar bo spodbudilo ljudi k nakupu?* in podobno. Lahko izkoristite priložnosti in se zaščitite pred nevarnostmi/grožnjami, ne morete pa jih spremeniti. Grožnje oziroma nevarnosti so slabosti vašega varnostnega podjetja. Na nevarnosti organizacije sami nimamo vpliva. Pri njih si lahko zastavimo vprašanja, kot sta: *Ali ima organizacija potencialne konkurente? Ali so opazne kakšne spremembe pri potrošnikih, ki bi lahko negativno vplivale na organizacijo?* in podobno (Parsons, 2021).

Analiza SWOT je lahko močno orodje za organizacijo oziroma podjetje. Pomaga prepoznati področja, na katerih je varnostno podjetje močno in na katerih šibko, ter tista, kjer se lahko v prihodnosti skrivajo priložnosti ali grožnje. Z rednim izvajanjem te vrste analize je večja verjetnost sledenja spremembam v panogi – in priprava nanje (Thinkcurity, 2022).

Za uspešno izvedeno analizo mora pri njej sodelovati skupina ljudi z različnih oddelkov v organizaciji. Pri tem gre za tako imenovani »brainstorming«, pri katerem vsak posameznik/zaposleni poda svoje ideje in mnenje. Na koncu se vse ideje združijo in razvrstijo v določene skupine. Pri tem gre lahko za omenjene prednosti, pomanjkljivosti, priložnosti ali nevarnosti (Kenton, 2023).

Najboljši čas za izvedbo analize SWOT je predvsem priporočljiv, ko v podjetju prihaja do sprememb. Z analizo se preveri trenutno stanje podjetja, na podlagi katerega lahko pride do izboljšav na različnih področjih. Prav tako analiza pokaže ključna področja, ki potrebujejo izboljšave in prilagoditve (Schooley, 2024). Priporočljiva je izvedba analize SWOT pred kakršnimikoli spremembami v organizaciji (Garmon Hummel, 2022), poleg tega pa tudi, kadar pride do različnih izzivov notranje narave v podjetju, prav tako pa tudi pred samo ustanovitvijo le-tega (Hilson, 2021).

4.5 Notranje grožnje

Notranje grožnje so zelo povezane s konceptom zlonamernih groženj, s katerimi se organizacije srečujejo s strani zaposlenih, nekdanjih zaposlenih, poslovnih partnerjev ali izvajalcev. Ti ljudje imajo dostop do notranjih informacij, povezanih s podatki podjetja, računalniškimi sistemi, varnostno prakso, zato bi morebitna goljufija, kraja ali sabotaža z njihove strani lebdela nad varnostjo organizacije (Georgescu, 2023).

Tveganja, ki prihajajo od zaposlenih, so predvsem nezapletena gesla, pošiljanje elektronske pošte na domače elektronske naslove, pošiljanje pošte napačnim osebam in podobno. Vse omenjeno predstavlja tveganja, saj domače omrežje ni pravilno zavarovano, geslo pa je lahko hitro zlorabljeno. Poleg tega se v današnjem času uporabljajo tudi mobilne naprave za dostopanje do podatkov in s tem tudi za delo, kar predstavlja še večje tveganje, predvsem če se naprava izgubi ali pa jo kdo ukrade (van Zadelhof, 2016).

Notranje grožnje se nanašajo na tveganje, ki ga predstavlja nekdo iz notranjosti podjetja, ki bi lahko izkoristil sisteme za krajo podatkov ali povzročil kakršno koli škodo.

- **Nepooblaščen dostop zaposlenih**

Zaradi različnih razlogov lahko zaposleni poskušajo pridobiti dostop do delov sistema, s katerimi običajno ne delajo. Prav tako lahko imajo ali pridobijo »skrbniške privilegije«, ki jim omogočajo opravljanje nadaljnjih skrbniških funkcij, kot je spreminjanje pravic dostopa drugih uporabnikov ali deaktiviranje orodij za varnost omrežja. Ta vprašanja so lahko ključna točka za nadaljnje napade (Georgescu, 2023).

- **Nenamerno razkritje podatkov**

Zlonamerno vedenje lahko privede do preprostih incidentov ali povzroči veliko škode, lahko pa tudi nesreče: naprave podjetja so lahko nekje pozabljene, kar lahko razkrije občutljive podatke, mape se lahko pomotoma izbrišejo ali podobno. Skupina posameznikov, ki nenamerno razkriva podatke, se imenuje brezskrbni zaposleni oz. neprevidne osebe. Ta kategorija vključuje posameznike, ki pri svojem delu delajo veliko napak in nanje niso pozorni ter tudi ne posvečajo velike pozornosti varnostnim praksam organizacije (Saxena idr., 2020).

- **Socialni inženiring**

Čeprav je socialni inženiring sam po sebi zunanja grožnja, lahko deluje le, če nekdo znotraj podjetja razkrije informacije. Da bi uspeli s svojim zlonamernim namenom, se lahko hekerji pretvarjajo, da so prijatelji ali druge zaupanja vredne osebe. Tako bodo zahtevali občutljive podatke ali celo ponudili nepričakovane nagrade (Georgescu, 2023).

– Nezakonite dejavnosti

Pomembno je vedeti, da je delodajalec odgovoren za skoraj vse, kar počnejo zaposleni, ko uporabljajo računalniško omrežje – razen če se lahko dokaže, da so bili pred tem sprejeti razumni ukrepi. Na žalost ni popolnoma nenavadno, da zaposleni prenašajo pornografijo ali prodajajo mamila in spolno žaljivo gradivo po e-pošti podjetja. Zraven lahko prištejemo tudi nenormalne dejavnosti, kot so dejavnost ob neobičajnem času (prijava v sistem pozno ponoči), velik obseg podatkovnega prometa (prenos prevelikega števila oz. obsega podatkov v omrežju) ter neobičajna ali nerutinska dejavnost (dostop do nenavadne baze). Osebe, ki izvajajo take vrste dejavnosti, so t. i. zlonamerni »insajderji«, ki namerno izrabljajo sistem, da bi pridobili podatke za finančno ali osebno korist. Druga skupina posameznikov so ogroženi notranji uporabniki, ki napadalcu nenamerno omogočijo dostop do omrežja in sistema (Saxena idr., 2020).

– Fizična kraja naprav podjetja

Zlasti danes, ko se politika dela od doma zaradi pandemije covida-19 še vedno povečuje, zaposleni svoje službene računalnike pogosto odnesejo iz pisarne. Tudi če nimajo zlonamernih namenov, lahko pride do kraje. Zato je pomembno zagotoviti, da zunanji uporabniki ne morejo dostopati do naprav in s tem podatkov podjetja, tudi če se te izgubijo ali so ukradene (Georgescu, 2023). Zaposleni naprave in druge fizične stvari v organizaciji ukradejo na različne načine. To so lahko kraja na način, da zaposleni stvari nosi, ko odide z delovnega mesta; ali shranjevanje v lastne škatle, nahrbtnike in podobno; skrivanje naprav in drugih stvari v vrečah za smeti, da se jih kasneje odnese; vrnitev na delo v poznih urah in podobno (Purpura, 2017).

Poleg tega so lahko trdi diski, ki vsebujejo občutljive informacije, ukradeni ali pa so podatki na njih preneseni na bliskovni pogon USB in nato izbrisani. Drugi poskusi sabotaže podjetja so lahko prikriti kot npr. požar, poplave, izpad električne energije in podobno (Georgescu, 2023).

Akterje notranjih groženj lahko razdelimo na več vrst. Prva skupina so zaposleni, ki predstavljajo največje tveganje za organizacije. Več kot ima podjetje zaposlenih, več groženj je mogočih. Naslednja skupina so izvajalci, ki prav tako kot zaposleni potrebujejo dostop do sistemov in podatkov organizacije, zato tudi oni predstavljajo grožnjo. Tretja skupina so poslovni partnerji, ki so najpogosteje zunanji poslovni partnerji in imajo dostop do sistemov in podatkov. Naslednji so ponudniki storitev, ki lahko z dostopom ali

nadzorom sistemov ali podatkov povzročijo škodo. Seveda je mogoča tudi okvara opreme, pri čemer sta pomembna predvsem redno vzdrževanje in zamenjava opreme (Reed, 2021). Ukrepi za preprečevanje notranjih groženj so tudi naslednji:

- pristopna kontrola,
- ključavnice in ključi, blagajne, trezorji in omare za dokumente,
- protivlomni alarmni sistemi in detektorji gibanja,
- televizija zaprtega kroga in
- varnostniki. (Dvojmoč, 2017a)

4.6 Zunanje grožnje

Zunanje varnostne grožnje vključujejo številne kategorije, ki izvirajo iz zunanjih zidov podjetja in jih sproži nekdo, ki ni povezan s podjetjem. Zunanje grožnje so lahko usmerjene tudi na posameznike. Vdori ali sheme za krajo gesel in spletne prevare, ki nas prepričajo, da voljno delimo poverilnice, so usmerjeni tako na osebne kot poslovne račune. Zunanja tveganja vključujejo tudi fizične grožnje, kot so posegi v napravo ali omrežje, katerih namen je motiti delovanje (Akasaka, 2023).

Zunanje grožnje kibernetske varnosti spadajo v tri osnovne kategorije:

- Zlonamerna programska oprema, kot je izsiljevalska programska oprema.
- Vdiranje, kot so napadi porazdeljene zavrnitvene storitve.
- Socialni inženiring, kot je lažno predstavljanje. (Akasaka, 2023)

Zlonamerna programska oprema je vrsta kodiranja, ki jo lahko zunanji napadalec uporabi za dostop do omrežja in shranjevanje informacij o organizaciji. Poznamo več različnih vrst zlonamerne programske opreme, pri čemer vsaka deluje na drugačen način. Grožnja, ki prav tako ni zanemarljiva, so tudi naravne nesreče, saj so izven dosega ljudi in ravno zato lahko predstavljajo največjo grožnjo. Tudi lažno predstavljanje je zunanja grožnja, ki se preko elektronske pošte infiltrira v samo organizacijo. Pri tem se oseba predstavlja kot nekdo drug, ko pristopa k podjetju ali razširi komunikacijo z njim. Napadalci znajo manipulirati z zaposlenimi in si tako zagotovijo dostop do zasebnega omrežja in tudi osebnih podatkov organizacije. Naslednja vrsta groženj so tudi kibernetski teroristi. Njihove dejavnosti pa vključujejo predvsem motnje ali zaustavitev poslovanja organizacije (Indeed, 2023b).

Druge zunanje grožnje so lahko še organizirane kriminalne združbe, ki so največkrat finančno motivirane; socialni inženiring, ki vključuje napadalce, ki zavajajo in manipulirajo z zaposlenimi v organizaciji, in ranljivosti v programski opremi, ki predstavlja težavo, saj lahko napadalci poznajo ranljivosti in jih izkoristijo za svoje napade (Indeed, 2023b).
Da bi se zmanjšala tveganja za varnost podatkov, bi morale organizacije izvajati proaktivne strategije spremljanja, ki so uporabljene za odkrivanje in odzivanje na incidente (Akasaka, 2023).

Ukrepi za preprečevanje zunanjih groženj so naslednji:

- varnost okoliša,
- ograje, okna in vrata,
- alarmni sistemi,
- televizija zaprtega kroga,
- osvetlitev objekta in okolice,
- kontrola parkirišč in vozil,
- varnostniki. (Dvojmoč, 2020)

4.7 Tehnološka tveganja

Tehnologija je povzročila številna varnostna tveganja, kot so lažno predstavljanje, socialni inženiring in pretvarjanje. Poznavanje teh tveganj je zelo pomembno pri izogibanju le-tem (Bdc, n. d.). Prislan in Bernik (2014) navajata, da tveganja na področju informacijske varnosti stalno naraščajo.

Tehnološka tveganja spadajo pod vrsto poslovnega tveganja, ki je opredeljeno kot možnost, da tehnološka napaka moti poslovanje. Brez ustreznih odzivov lahko vsako tehnološko tveganje povzroči finančne motnje, motnje ugleda, regulativne ali strateške motnje. Ključnega pomena je, da imajo organizacije učinkovito strategijo za obvladovanje tehnoloških tveganj, ki predvideva morebitne težave (RiskOptics, 2023).

Tukaj je seznam najpogostejših tehnoloških varnostnih tveganj, ki se jim je treba izogniti.

- Lažno predstavljanje je uporaba goljufivih e-poštnih sporočil ali telefonskih klicev za pridobivanje občutljivih informacij, kot so številke bančnih računov, podatki o kreditnih karticah ali gesla. Ta sporočila običajno vključujejo povezavo do nečesa, kar je videti kot zakonito spletno mesto, kjer je treba vnesti podatke o računu ali prenesti zlonamerno programsko opremo. Lažno predstavljanje je vrsta socialnega

inženiringa, ki je napad, ki uporablja lažno predstavljanje za pridobivanje občutljivih informacij (Bdc, n. d.). Takšna elektronska sporočila se pošiljajo količinsko, torej napadalec enako sporočilo pošlje več uporabnikom oz. žrtvam s podobnimi interesi. Takšna tehnika pošiljanja e-poštnih sporočil se od tradicionalne razlikuje po tem, da se lahko pošilja množično skupini uporabnikov ali pa več organizacijam (Shaw, 2020).

- Zlonamerna programska oprema je vsaka programska oprema, ki ima škodljiv namen. Lahko ukrade ali poškoduje poslovne podatke, povzroči odpoved sistemov ali na skrivaj beleži računalniško dejavnost. Zlonamerna programska oprema običajno okuži računalnik po napadu z lažnim predstavljanjem ali če zaposleni pomotoma prenese okužene datoteke (Bdc, n. d.). Zlonamerna programska oprema vključuje računalniške viruse, črve, trojanskega konja, vohunsko programsko opremo ali celo izsiljevalsko programsko opremo (Pranggono in Arabo, 2020).
- Čeprav ima veliko ponudnikov storitev v oblaku dobro internetno varnost, je nimajo vsi. Ogroženost predstavlja, če ima ponudnik slabo varnost, zaradi česar so podatki ranljivi za napad. Odvisno od dogovora s ponudnikom je lahko njihova odgovornost omejena na mesečno naročnino in morda ne krije izgub zaradi prekinitve poslovanja. Če je ponudnik napaden, lahko odgovornost za ogrožanje podatkov strank pade na samo organizacijo. Podjetja se soočajo s podobnimi tveganji, če najamejo zunanje tehnike za servisiranje njihovih potreb IT. Organizacija je ranljiva tudi, če je osebje IT slabo usposobljeno ali ne upošteva najboljših praks (Bdc, n. d.).
- Zaradi slabo zavarovanega sistema Wi-Fi je lahko podjetje ranljivo za hekerje v dosegu omrežja. Heker lahko pridobi občutljive podatke, poškoduje sisteme ali namesti izsiljevalsko programsko opremo. Če je dostop do poslovnega omrežja omogočen na daljavo prek nezaščitenega strežnika, lahko drugi vidijo promet in dostopajo do sistema. Na javnem območju je ogroženost še večja, če je povezava v splet vzpostavljena preko »prevarantskega« internetnega strežnika. Dostop do interneta preko takega omrežja daje napadalcu dostop do sistema in morda poslovnega omrežja (Bdc, n. d.).
- Slabo izbrana gesla zaposlenih lahko povečajo izpostavljenost podjetja varnostnim tveganjem. Veliko težav se pojavi, ko zaposleni izberejo gesla, ki jih nepooblaščene osebe zlahka uganejo (Bdc, n. d.).
- Nepravilno odlaganje starih naprav lahko nekomu preda vse poslovne podatke. Če so informacije zelo občutljive, brisanje podatkov ali formatiranje trdega diska nista dovolj (Bdc, n. d.).

Kibernetsko tveganje je tveganje za motnje v delovanju podjetja, škode, ki se zgodi zaradi okvar digitalnih tehnologij, finančne izgube zaradi nepooblaščenega dostopa, razkritja, spreminjanja ali uničenja proizvodnega sistema (Markelj in Zgaga, 2018). V povezavi s samo definicijo je kibernetsko tveganje povezano s kibernetskim napadom, saj je tveganje možnost, da do napada pride.

Poleg drugih tehnoloških tveganj se organizacije in podjetja vsakodnevno soočajo tudi s kibernetskimi napadi, ki predstavljajo resno nevarnost. Najpogostejši napad je lažno predstavljanje, pri katerem zaposleni prejme lažno elektronsko sporočilo, s katerim jih napadalci poskušajo preslepiti, da z njimi delijo zaupne podatke in informacije. Tudi zlonamerna programska oprema predstavlja tveganje. Namesti jo zunanji subjekt in povzroči škodo napravi ali IT sistemom podjetja. Ena izmed oblik zlonamerne programske opreme je na primer trojanski konj. Nevarnost predstavljajo tudi kršitve podatkov, do katerih pride, ko so občutljivi podatki ukradeni ali razkriti nepooblaščenim osebam. Do teh kršitev lahko pride preko zunanjih napadov, kot so vdori, zlonamerna oprema ali lažno predstavljanje. Notranji vdori so prav tako mogoči predvsem s strani nezadovoljnih ali neustrezno usposobljenih zaposlenih. Tveganje predstavlja tudi stara oprema. S posodabljanjem programske opreme se zavarujemo pred novimi in razvijajočimi se kibernetskimi tveganji (RiskOptics, 2023).

Stopnja kibernetskih napadov se stalno povečuje oziroma so bolj sistematično spremljani. Samo zavedanje o možnostih ogrožanja v kibernetskem prostoru in strah pred kriminaliteto sta povezana s poznavanjem virov ogrožanja in njihovim dojemanjem (Bernik in Meško, 2011).

4.8 Ranljivost gospodarskih subjektov

V gospodarstvu večine sodobnih držav v strukturi lastništva prevladujejo zasebni lastniki, imetniki bogastva, ki so ranljivi in ogroženi, torej »tisti, ki morajo sami upravljati svoja tveganja, upoštevati grožnje (ne samo tiste s kriminaliteto, ampak tudi z nezgodami in drugimi nevšečnostmi)« ter so na ta način prisiljeni gospodarno ravnati predvsem s svojo ranljivostjo. Ranljivost pa je kakršnakoli slabost oz. napaka v fizičnem stanju (položaju) organizacije, postopkov, menedžmenta, administracije, hardwara in softwara, ki se lahko izrabi za povzročitev škode tako instituciji, poslovnosti ali dejavnosti« (Pečar, 2000, str. 108). V najširšem pogledu se gospodarski subjekti soočajo s poslovno, ekonomsko, finančno, socialno, tehnično-tehnološko, razvojno, tržno, požarno, kriminalno, sabotažno, teroristično, vohunsko, logistično, ekološko ranljivostjo in drugimi ogroženostmi ter tveganji.

Kakšen je pomen učinkovitega načrtovanja, se največkrat ugotavlja, ko je že prepozno, ko pride do škodnih primerov, do nezgod, nesreč in drugih nenadzorovanih dogodkov.

V praksi se ugotavlja, da gospodarske družbe nimajo izdelanih dokumentov in dejavnosti ali pa so ti slabi, strokovno vprašljivi in pomanjkljivi. To so ocene ogroženosti, nevarnosti in poslovno-varnostnih tveganj; varnostni načrti, navodila, protokoli; načrti obvladovanja izrednih dogodkov, kriznih situacij in razmer; načrti neprekinjenega delovanja; politika in strategija poslovanja po izrednem dogodku; pisana in nepisana pravila obnašanja in ravnanja so nedorečena; varnostna kultura in etika nista na ustrezni ravni; nadzor nad izvajanjem varnostnih storitev ni zadovoljiv in podobno.

Odgovorite na vprašanja

Kaj je tveganje?

Kateri elementi sestavljajo tveganje?

Kaj je analiza tveganja in kaj vključuje?

Kako poteka zaznava tveganja? Pojasnite s svojimi besedami.

Kako poteka obravnava tveganja? Pojasnite s svojimi besedami.

Kaj pomeni ocenjevanje tveganja?

Kaj je najpomembnejše pri izvedbi ocene tveganj? Pojasnite.

Zakaj je ocena tveganja pomembna?

Katere metode analize tveganj poznamo? Naštejte.

S svojimi besedami na kratko pojasnite zgoraj naštete metode.

Kaj je analiza SWOT? Pojasnite.

Kaj so lahko prednosti in kaj slabosti organizacije? Naštejte nekaj lastnih primerov.

Kaj so lahko priložnosti in grožnje organizacije? Naštejte nekaj lastnih primerov.

Kaj predstavljajo notranje grožnje?

Opredelite nekaj notranjih groženj, s katerimi se soočajo organizacije.

Kaj so zunanje grožnje?

Naštejte nekaj primerov zunanjih groženj, s katerimi se soočajo ogranizacije.

Kateri so ukrepi za preprečevanje zunanjih groženj? Pojasnite.

S svojimi besedami opišite, kaj so tehnološka tveganja.

Naštejte nekaj primerov tehnoloških tveganj.

Kako bi se po vašem mnenju lahko izognili tehnološkim tveganjem? Pojasnite.

Kaj za vas pomeni ranljivost gospodarskih subjektov?

Na kakšen način lahko zaščitimo gospodarske subjekte? Pojasnite.

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

5 Načrtovanje korporativne varnosti

Po besedah Kovačiča in Podvršiča (2014) morajo imeti organizacije, ki želijo biti uspešne, dober oz. učinkovit varnostni menedžment za obvladovanje korporativnih varnostnih tveganj. Brez varnostnega menedžmenta je obvladovanje notranjih in zunanjih varnostnih tveganj zelo težko. Pri oblikovanju oziroma izdelavi varnostne politike je zelo pomembno, da se izhaja iz metodološke in vsebinske sheme pristopa k upravljanju same korporativne varnosti, ki nam daje celovit vpogled, kakšne so nevarnosti, škoda in protiukrepi (Dvojmoč, 2017a).

5.1 Oblikovanje varnostne politike

Varnostna politika organizacije je skupek pravil, napotkov in postopkov, ki opredeljujejo, kako v organizaciji upravljati, ščititi in ravnati z določenimi viri z namenom doseganja konkretno zastavljenih varnostnih ciljev. Dobra varnostna politika je živa, preprosta, prilagojena delu in predvsem takšna, da jo zaposleni in zunanji uporabniki poznajo in uporabljajo. Je krovni dokument upravljanja korporativne varnosti in varnostnega elaborata, ki predstavlja implementacijo sprejete varnostne politike in je tudi kazalnik varnostne strategije ter podlaga za izdelavo notranjih aktov in operativne varnostne dokumentacije, kamor spadajo načrti varovanja, varnostni režimi, navodila in podobno (Vršec, 2014).

Varnostna politika prispeva k celotni nacionalni varnostni politiki in s tem k razvoju celovitega sistema korporativne varnosti v organizacijah. Pri tem je pomembno tudi, da se kot taka izvaja tudi v praksi. Z usklajevanjem varnostne politike in izvajanjem rednih dejavnosti klasični varnostni subjekti neposredno izpolnjujejo varnostno funkcijo (Trivan, 2017).

Predvsem zaradi groženj in tveganj, ki zadevajo ekonomsko-poslovno, tehnično, fizično in informacijsko varnost, vsaka organizacija potrebuje lastno varnostno politiko. Ta omogoča prepoznavo potencialnih varnostnih izzivov, za katere se določijo ukrepi (Lobnikar in Sotlar, 2006).

Vsaka varnostna politika ima dva dela. Prvi se ukvarja s preprečevanjem zunanjih groženj za ohranitev celovitosti omrežja, drugi pa se ukvarja z zmanjševanjem notranjih tveganj z opredelitvijo ustrezne uporabe omrežnih virov.

Obravnavanje zunanjih groženj je tehnološko usmerjeno. Čeprav je na voljo veliko tehnologij za zmanjšanje zunanjih omrežnih groženj, kot so požarni zidovi, protivirusna programska oprema, sistemi za zaznavanje vdorov, e-poštni filtri in drugo, pa te vire večinoma izvaja osebje IT, s čimer jih uporabnik ne zazna (Duigan, 2003).

Dobra varnostna politika mora vsebovati:

- Namen: Jasni cilji in pričakovanja politike.
- Skladnost s pravilnikom: Zvezni in državni predpisi lahko vodijo nekatere zahteve varnostnega pravilnika, zato je ključnega pomena, da so navedeni.
- Datum zadnjega testiranja: Politike morajo biti živ dokument, kar pomeni tudi, da jih je treba pogosto preizkušati.
- Datum zadnje posodobitve politike: Dokumente varnostne politike je treba posodobiti, da se prilagodijo spremembam v organizaciji, zunanjim grožnjam in tehnologiji.
- Kontakt: Varnostno politiko informacij naj bi prebrali, razumeli in upoštevali vsi posamezniki v organizaciji, zato mora vsebovati podatke lastnika, če obstajajo kakršna koli vprašanja. (Buckbee, 2015)

Model varnostne politike predstavlja vsebinski in strukturni okvir varnostne kulture v sami organizaciji. Zajema vse potrebne elemente varovanja, pri čemer se vse začne s temeljno varnostno kulturo, kot so pogledi, stališča, zamisli in nazori o varovanju organizacije, varnostnih interesov in tudi motivov zaščite. Časovno je razvojna varnostna politika

naravnana na 3–5 let, kar je odvisno od samih sprememb v okolju organizacije in tudi od ocene njene ogroženosti (Dvojmoč, 2017a).

Načela varnostne politike usmerjajo udeležence organizacije, predvsem lastnike, menedžment in varnostne strokovnjake v uspešnost, ki je predvsem rezultat dopustnega tveganja, zmanjšanja ekonomske in socialne negotovosti ter preprečevanja škod v organizaciji. Gre za uresničevanje varnostnega koncepta, kamor spadajo oblikovanje, sprejemanje in vodenje varnostne politike. Pomembno je predvsem, da lastniki in vodstvo organizacije oblikujejo in izvajajo varnostno politiko (Podbregar, 2007).

5.2 Vloga in odgovornosti uprave

Vodje poleg vodenja svojega oddelka opravljajo tudi mnoge druge naloge. Za nemoteno delovanje morajo skrbeti tudi za logistiko in sodelovati z zainteresiranimi stranmi. Razumevanje različnih nalog, ki jih opravljajo vodje, lahko pomaga bolje razumeti, kakšne so vsakodnevne odgovornosti v vodstveni vlogi (Herrity, 2023).

Vodje načrtujejo, usmerjajo in nadzorujejo vire za doseganje splošne vizije podjetja. S postavitvijo jasno opredeljenih ciljev lahko vodje pomagajo motivirati zaposlene za doseganje uspeha in zagotavljajo mentorstvo za rast. Vloga upravitelja ima tri komponente:

- Medosebnost: Vodje pogosto komunicirajo z različnimi ljudmi, vključno z zaposlenimi, vodstvom in skupnostjo.
- Informativno: vodje imajo lahko vlogo, kjer zagotavljajo informacije zaposlenim in skupnosti.
- Odločanje: Vodstvo lahko zaposluje nove sodelavce, izvaja ocenjevanje obstoječih zaposlenih in sprejema odločitve o poslovanju. (Herrity, 2023)

Pomen menedžmenta v organizaciji je večplasten. Menedžerji so pomembni za vsako organizacijo pri doseganju njenih ciljev. So hrbtenica vsake organizacije, njihova vloga pa je zagotoviti, da v podjetju vse teče gladko. Uspeh ali neuspeh organizacije je odvisen od tega, kako dobro njeni vodje opravljajo svoje odgovornosti (Online manipal editorial team, 2023).

Vodje lahko kategoriziramo kot generalne direktorje, ki nadzirajo več oddelkov organizacije; funkcionalne menedžerje, ki se ukvarjajo z enim vidikom vodenja podjetja, kot je prodaja ali računovodstvo; in vodje projektov, ki nadzirajo določen projekt znotraj svojega oddelka, ali oddelka. Generalni direktor nadzira vse različne oddelke, medtem ko funkcionalni vodja upravlja en določen oddelek. Vodja projekta je odgovoren za nadzorovanje določenega projekta ali naloge znotraj organizacije (Online manipal editorial team, 2023).

V organizacijah vlogo uprave predstavljajo varnostni menedžerji, ki so del varnostnega menedžmenta, ki skrbi za korporativno varnost. So vodje in predvsem sprejemajo odločitve, na podlagi katerih se kasneje oblikujejo varnostni ukrepi (Reinfelder idr., 2019). Vloga varnostnih menedžerjev je zelo pomembna, saj so enakopravni partner pri vodenju in upravljanju organizacije. Za svoje delo morajo biti dobro usposobljeni, njihova naloga pa je tudi oblikovanje varnostnega načrta, s katerim se identificirajo in tudi preprečujejo varnostna tveganja. Na podlagi ugotovljenih groženj se oblikuje varnostni načrt, s katerim se oblikuje tudi varnostna strategija organizacije. Načrt vsebuje ukrepe s področja zagotavljanja integritete delovanja organizacije, kar vključuje tudi protokole, politike in odgovornosti, namenjen je obvladovanju notranjih in zunanjih tveganj (Sotlar in Dvojmoč, 2021).

Gostič (2014) navaja, da so temeljne naloge in odgovornosti varnostnega menedžerja soodgovornost za strateško odločanje in upravljanje; upravljanje sprememb v organizaciji na podlagi varnostne kulture, socialne mreže, povezanosti in učenja; zagotavljanje sodelovanja osnovnih in podpornih poslovnih procesov; izvajanje dolžnostnega nadzorstva nad delom; zagotavljanje varnosti in ozaveščanje drugih o tem; izobraževanje s področja varnosti; vodenje delovnih skupin in podobno. Na svoj način varuje organizacijo in vzpostavi okoliščine, na podlagi katerih je dosežena maksimalna varnost pri delu in vzdrževano varno okolje ter varnost zaposlenih. Varnostni menedžer mora poiskati vse slabosti in pomanjkljivosti, ki bi delovanje in poslovanje organizacije lahko ogrozile (Stankovski, 2012).

Zelo pomembno je predvsem, da je varnostni menedžer izobražen, profesionalen in prodoren, saj mora biti kot oseba sposoben biti vodja varnostne službe. Z dobrim delom pripomore k ohranjanju in zviševanju vrednosti organizacije, ustvarjanju dobička, izkazovanju integritete, pospeševanju prodaje izdelkov, ugledu organizacije itd. Umeščenost korporativnega varnostnega menedžerja v organizaciji je izjemnega pomena. Glede na pretekle izkušnje je priporočljivo, da je varnostni menedžer odgovoren

neposredno upravi organizacije oz. njenemu predsedniku, saj je na ta način samostojen in neodvisen od drugih služb v organizaciji (Dvojmoč, 2017a).

Omeniti je treba tudi, da ima vsaka organizacija oddelek, sektor, odsek ali službo, ki je zadolžena za zagotavljanje varnosti. Pri tem imajo večje organizacije varnostno službo kot samostojno enoto, manjše organizacije pa kot del splošnega upravljavskega oddelka (Dvojmoč, 2017a). Nekatere organizacije imajo oddelek korporativne varnosti ločen od drugih, vseeno pa je pomembno, da oddelki med seboj sodelujejo in na ta način zagotavljajo najvišjo mogočo varnost.

5.3 Obveznosti zaposlenih

Z »Zakonom o delovnih razmerjih (ZDR-1)« (2013) je določeno, da je v delovnem razmerju vsaka od pogodbenih strank dolžna izvrševati dogovorjene in predpisane pravice in obveznosti. Zaposleni mora tako vestno opravljati delo po navodilih in zahtevah delodajalca, kar je v skladu s sklenjeno pogodbo o zaposlitvi. Prav tako mora upoštevati ukrepe za varnost in zdravje pri delu, obveščati delodajalca o bistvenih okoliščinah in spremembah podatkov v zvezi z opravljanjem obveznosti, vzdrževati se škodljivih ravnanj oziroma ravnanj, ki bi škodila poslovnim interesom delodajalca ter spoštovati prepoved konkurence že med trajanjem delovnega razmerja, lahko pa tudi po njegovem prenehanju (Data, 2018). Zaposleni je prav tako dolžan varovati poslovne skrivnosti, ki jih kot take določi delodajalec, in tudi podatke, za katere je mogoče, da bi nastala škoda, če bi zanje izvedela nepooblaščena oseba (Kompare, 2014).

Za zaposlene v gospodarski družbi je usposabljanje s področja varnosti ključnega pomena, saj se tako seznanijo s potencialnimi tveganji, ukrepi za upravljanje tveganj in postopki za minimaliziranje posledic, če do teh že pride. Posameznikom, ki so v podjetju zadolženi za področje varstva in varnosti, velja nameniti še posebno skrb za redno usposabljanje, izobraževanje in izpopolnjevanje, saj je od kakovosti tega odvisno njihovo opravljanje delovnih nalog. Oba vidika usposabljanja s področja varnosti posledično vodita v razvoj visoke stopnje varnostne kulture v podjetju (Podbregar, 2007).

Zaradi nenehnega razvoja morajo tudi organizacije stalno izobraževati svoje zaposlene. Izobraževanja lahko izvajajo sama, s pomočjo zunanjih institucij, ali pa jih izvajajo le zunanje institucije. Najbolj pogosta izobraževanja, ki jih izvajajo organizacije same, so izobraževanje novozaposlenih, pripravnikov, usposabljanje poslovnih partnerjev in izobraževanje za kakovost. Oblike, ki jih izvajajo le zunanje institucije, so usposabljanja

osebja za izvajanje internih oblik izobraževanja, učenje tujih jezikov, uporabo računalniških sistemov in programov ter izobraževanje menedžmenta (Kastelic, 2016).

S stalnim izobraževanjem zaposlenih se dosega uresničevanje poslovne strategije organizacij. Na izobraževanjih gre tudi za izmenjavo znanj in izkušenj med zaposlenimi, torej gre za prenos znanja s starejših na mlajše ali obratno, z izkušenih na manj izkušene, ali preko zaposlenih na novince. Ena izmed oblik izobraževanja je tudi seminar za novozaposlene, na katerem se novim sodelavcem predstavijo strateški cilji, vizije in kultura organizacije, seznanijo pa se tudi z drugimi pomembnimi podrobnostmi (Kastelic, 2016).

Torej, izobraževanja lahko delimo na notranja in zunanja oz. na interna in eksterna. Le-ta delimo na naslednje skupine:

- individualna izobraževanja posameznika,
- timska izobraževanja,
- skupinska izobraževanja in
- kombinacija vseh oblik. (Mihalič, 2006)

Interna ali eksterna izobraževanja se zaradi potreb po izobraževanju, ki izhajajo iz potreb delovnega procesa, načrtujejo in izvajajo v sodelovanju z oddelkom za človeške vire (Kohont, 2019).

Pod interna izobraževanja vključujemo, kot že prej omenjeno, uvajanje za novozaposlene; mentorstvo; pripravništvo; predavanje; rotiranje; coaching; e-izobraževanje; osebni razvoj in obratno mentorstvo. Z uvajanjem novozaposlenih se jim olajša vključitev v delovno okolje organizacije (Kastelic, 2016). Prednosti mentorstva so med drugim bolj osebna pomoč posameznikom in zagotavljanje spodbudnega okolja (Merkač Skok, 2013). Pripravništvo lahko služi kot strategija zaposlovanja in izbire, ki organizacijam olajšajo zbiranje podatkov o zmožnostih potencialnih zaposlenih (Putra in Purba, 2020). Rotiranje pa je metoda internega usposabljanja in omogoča lažje nadomeščanje odsotnih zaposlenih z drugimi zaposlenimi (Možina, 2009).

Eksterna izobraževanja vključujejo delavnice in seminarje; razstave in sejme; lastna dejavnost zaposlenih ter benchlearning. Delavnice in seminarji so podobni projektnemu delu, kjer se posamezniki učijo teoretične vsebine in s tem pridobivajo nova znanja ali nadgrajujejo obstoječa (Zagorc, 2016). Benchlearning oz. primerjalno učenje pa je

učinkovit način uvajanja organzacijskih sprememb ter zmanjševanje organizacijskih tveganj (Ministrstvo za javno upravo, 2020).

5.4 Etični kodeksi

V *Slovarju slovenskega knjižnega jezika* [SSKJ] (2014) je kodeks opredeljen kot zakonik, zbirka zakonov, družbeno priznan in uveljavljen sistem načel, predpisov (»Kodeks«, n. d.).

Etični kodeks je vodnik načel, ki je zasnovan tako, da strokovnjakom pomaga pri poštenem poslovanju. Dokument o etičnem kodeksu lahko opiše poslanstvo in vrednote podjetja ali organizacije, kako naj bi strokovnjaki pristopili k težavam, etična načela, ki temeljijo na temeljnih vrednotah organizacije, in standarde, ki jih strokovnjak upošteva (Hayes, 2023).

K višji etičnosti lahko organizacija pripomore z doslednim izvajanjem različnih programov za doseganje visoke etike med svojimi zaposlenimi, z usposabljanji o etiki, z zgledom vodilnih ter tudi z etičnimi kodeksi (Schermerhorn, 2002).

Etični kodeks lahko zajema področja, kot so poslovna etika, kodeks poklicnega ravnanja in kodeks ravnanja zaposlenih. Kodeksi poslovne etike pojasnjujejo, kako naj bi zaposleni dosegali cilje in delovali v skladu z vrednotami organizacije. Prav tako zagotavlja okvir za to, kako morajo zaposleni med seboj komunicirati in kakšno komunikacijo morajo imeti s strankami, da javnosti kažejo pozitivno podobo organizacije. Kodeksi poslovne etike lahko privabijo pozameznike, ki delijo podobne vrednote. Poslovna etika se nanaša na to, kako etična načela vodijo poslovanje podjetja. Pogosta vprašanja, ki spadajo pod okrilje poslovne etike, vključujejo odnose med delodajalcem in zaposlenimi, diskriminacijo, okoljska vprašanja, podkupovanje, trgovanje z notranjimi informacijami in družbeno odgovornost (Indeed, 2023a).

Čeprav obstajajo številni zakoni, ki določajo osnovne etične standarde v poslovni skupnosti, je razvoj etičnega kodeksa v veliki meri odvisen od vodstva podjetja. Tako podjetja kot organizacije imajo običajno nekakšen etični kodeks, ki naj bi ga njihovi zaposleni ali člani upoštevali. Kršitev etičnega kodeksa lahko povzroči odpoved iz organizacije. Etični kodeks je pomemben, ker jasno določa pravila obnašanja in zagotavlja podlago za preventivno opozorilo (Hayes, 2023). Etični kodeks prav tako spodbuja visoke standarde, opredeljuje poklicna pričakovanja in sporoča ravnanje organizacij. Lahko rečemo tudi, da odraža temeljne vrednote organizacije.

– Vrste etičnih kodeksov

Etični kodeks ima lahko različne oblike, vendar je splošni cilj zagotoviti, da podjetje in njegovi zaposleni upoštevajo državne in zvezne zakone, se obnašajo v skladu z ideali in zagotavljajo, da je poslovanje, ki se vodi, koristno za vse deležnike.

a. Etični kodeks, ki temelji na skladnosti

Za vsa podjetja zakoni urejajo vprašanja, kot so zaposlovanje in varnostni standardi. Etični kodeksi, ki temeljijo na skladnosti, ne določajo le smernic za ravnanje, temveč določajo tudi kazni za kršitve.

V nekaterih panogah poslovno ravnanje urejajo posebni zakoni. Te industrije oblikujejo etične kodekse, ki temeljijo na skladnosti, za uveljavljanje zakonov in predpisov. Zaposleni običajno opravijo formalno usposabljanje, da se naučijo pravil obnašanja. Ker lahko neskladnost povzroči pravne težave za podjetje kot celoto, se lahko posamezni delavci v podjetju soočijo s kaznimi zaradi neupoštevanja smernic (Hayes, 2023).

Da bi zagotovili upoštevanje ciljev in načel etičnega kodeksa, nekatera podjetja imenujejo nadzornika za skladnost. Ta posameznik je zadolžen za obveščanje o spremembah predpisov in spremljanje ravnanja zaposlenih za spodbujanje skladnosti.

Ta vrsta etičnega kodeksa temelji na jasnih pravilih in natančno opredeljenih posledicah, ne pa na individualnem spremljanju osebnega vedenja. Kljub strogemu spoštovanju zakonodaje nekateri kodeksi ravnanja, ki temeljijo na skladnosti, ne spodbujajo vzdušja moralne odgovornosti v podjetju (Hayes, 2023).

b. Na vrednotah temelječ etični kodeks

Etični kodeks, ki temelji na vrednotah, obravnava temeljni vrednostni sistem podjetja. Lahko opiše standarde odgovornega ravnanja, ki se nanašajo na širše javno dobro in okolje. Etični kodeksi, ki temeljijo na vrednotah, lahko zahtevajo večjo stopnjo samoregulacije kot kodeksi, ki temeljijo na skladnosti (Dublino, 2023).

c. Na ravnanju temelječ etični kodeks

Nekateri kodeksi ravnanja vsebujejo jezik, ki obravnava skladnost in vrednote. Na primer, veriga trgovin z živili lahko ustvari kodeks ravnanja, ki zagovarja zavezanost podjetja zdravstvenim in varnostnim predpisom nad finančnim dobičkom. Ta veriga trgovin z živili

bi lahko vključevala tudi izjavo o zavračanju pogodbe z dobavitelji, ki hranijo živino s hormoni ali gojijo živali v nehumanih življenjskih razmerah (Hayes, 2023). Kodeks ravnanja je seznam pravil podjetja in kot tak opredeljuje posebna zahtevana in prepovedana vedenja. To so lahko pravila oblačenja, obnašanje do sodelavcev, pravila glede nadlegovanja, upoštevanje regulativnih in zakonskih zahtev in podobno. Kodeks ravnanja krepi pričakovanja pozitivnega vedenja, zato mora biti prepovedano vedenje natančno določeno. Pojasnjene pa morajo biti tudi posledice, ki lahko doletijo kršitelje (Dublino, 2023).

Pomembno je tudi vedeti, kako se etični kodeks določi oziroma napiše, saj to zahteva določen čas in trud. Najprej je treba določiti namen in obseg kodeksa. Pojasniti je treba pomen etičnega vedenja in na kakšen način bo kodeks pomagal zaposlenim pri sprejemanju etičnih odločitev. Določiti je treba tudi področja poslovanja, pri katerih bo kodeks vključen. Nato je treba prepoznati ključne vrednote in načela, ki vodijo organizacijo in odražajo njeno poslanstvo ter vizijo. Razviti je treba posebne standarde vedenja, ki podpirajo omenjene vrednote in načela. Standardi morajo biti jasni in razumljivi ter zajemati vse vidike poslovanja. Naslednji korak je vključitev posledic ob neupoštevanju kodeksa, kot so disciplinski ukrepi, opozorila in podobno. Zaposlene je treba ves čas spodbujati, da domnevne kršitve prijavijo, zato mora biti tudi postopek prijave jasen in anonimen. Etični kodeks mora biti redno pregledan, s čimer se zagotovi njegova ustreznost in učinkovitost. Po potrebi ga je treba posodobiti in o tem obvestiti vse zaposlene. Po oblikovanju etičnega kodeksa je treba o tem obvestiti vse zaposlene, stranke in zainteresirane posameznike, ki morajo biti poučeni o njegovi vsebini (Fermin, 2023).

Odgovorite na vprašanja

Kaj varnostni menedžment predstavlja za organizacijo?

Kaj je varnostna politika?

Zakaj je varnostna politika pomembna?

Kako je razdeljena varnostna politika?

Kaj vse vsebuje dobra varnostna politika?

Katero vlogo ima vodja v organizaciji?

Kakšen mora biti dober vodja po vašem mnenju? Pojasnite.

Kako lahko kategoriziramo vodje?

Kakšna je vloga varnostnega menedžerja?

Kakšen mora biti varnostni menedžer?

Kakšne so po vašem mnenju obveznosti zaposlenih? Pojasnite.

Zakaj je usposabljanje s področja varnosti za zaposlene zelo pomembno?

Kako so razdeljena izobraževanja zaposlenih? Naštejte.

Opišite zgoraj našteta izobraževanja.

Kaj je etični kodeks in zakaj je pomemben?

Katere vrste etičnih kodeksov poznamo? Naštejte.

Na kratko pojasnite zgoraj naštete etične kodekse.

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

6 Načrtovanje varnostnih ukrepov

Kot je bilo že omenjeno, je varnostna politika za organizacijo in korporativno varnost izredno pomembna. Poleg tega je pomembno tudi oblikovanje varnostnih programov, ki zagotavljajo varnost in zdravje na delovnem mestu oz. med zaposlenimi, pri čemer je pomembno sodelovanje vseh v organizaciji, torej tako vodstva kot vseh zaposlenih. V kriznih situacijah je krizno upravljanje ključen dejavnik zagotavljanja varnosti, saj se ustvari sistem, ki je odporen proti tveganjem in grožnjam (Haimess, 2009). Na podlagi tega se naredi tudi načrt kriznega upravljanja, ki mora biti pripravljen že pred samo krizo (Lesjak, 2020). Tako kot je pomemben krizni načrt, pa je pomembna tudi ocena ogroženosti, ki opozarja na grožnje in na njihovo uresničitev.

6.1 Razvoj varnostne politike

Varnostna politika določa, kaj se v organizaciji želi zaščititi in kaj se pričakuje od uporabnikov sistema.

Na grobo lahko varnostno politiko razdelimo na štiri vrste: politika na ravni programa; politika na ravni programskih okvirov; politika, ki naslavlja specifične probleme; politika, ki naslavlja specifične sisteme (Schweighofer, 2010).

Vsaka internetna storitev, ki jo uporablja ali nudi organizacija, predstavlja tveganje za sistem in omrežje, s katerim je povezana. Varnostna politika je nabor pravil, ki veljajo za dejavnosti za računalniške in komunikacijske vire, ki pripadajo organizaciji. Ta pravila

vključujejo področja, kot so fizična varnost, varnost osebja, upravna varnost in varnost omrežja. Zagotavlja osnovo za varnostno načrtovanje, ko so načrtovane nove aplikacije ali se širi trenutno omrežje. Opisuje odgovornosti uporabnika, kot je varovanje zaupnih informacij in pravila za ustvarjanje gesel (IBM, 2021).

Varnostna politika mora opisati tudi, kako oz. na kakšen način se spremlja učinkovitost varnostnih ukrepov. Takšno spremljanje pomaga ugotoviti, ali morda nekdo poskuša zaobiti zaščitne ukrepe organizacije. Za razvoj varnostne politike morajo biti jasno opredeljeni varnostni cilji. Ko je varnostna politika ustvarjena, je treba narediti tudi korake za uveljavitev pravil, ki jih vsebuje (IBM, 2021).

Varnostne smernice je smiselno poslati vsem zaposlenim, s čimer se poudarijo varnostne politike glede fizične in sistemske varnosti. V te smernice se vključijo tudi navodila o tem, kako zaščititi varnost sistema, kot je odjava z delovnih postaj, ustrezna uporaba gesel in zaščita omrežja pred nepooblaščenimi vsiljivci. Varnostna politika lahko pojasni tudi postopek usposabljanja zaposlenih in namestitev potrebne programske in strojne opreme za zagotavljanje varnosti sistema (IBM, 2021).

Varnostna politika se lahko nenehno spreminja. Če so v računalniškem okolju narejene spremembe, mora biti varnostna politika prav tako spremenjena oziroma posodobljena, da bo obravnavala morebitna nova tveganja, ki jih prinašajo te spremembe. Večina podjetij ugotovi, da potrebujejo strožjo varnost, ko rastejo in se razvijajo.

Koraki, ki se izvajajo za razvoj varnostne politike, so naslednji:

- Pogovor z drugimi člani vaše organizacije, kot so varnostni revizorji za boljše določitev varnostnih potreb.
- Pregled tehnologije, ki je uporabljena v podjetju. Na primer: če je sistem povezan z internetom, se uporabi bolj restriktivno varnostno okolje za zaščito sistema pred zunanjimi uporabniki interneta.
- Določitev splošnega pristopa k varnosti: strog, povprečni, sproščeni.
- Ugotoviti, katera informacijska sredstva potrebujejo zaščito. Za pomoč pri tej odločitvi je treba upoštevati zaupnost, konkurenčnost in operacije.
- Ustvariti je treba izjavo o politiki podjetja glede varnosti. To je dogovor med najvišjimi uradniki v podjetju. Varnostna politika mora navajati, kakšen je splošni pristop in katera sredstva potrebujejo zaščito.
- Ustvariti je treba osnutek varnostne politike.

- Med delom skozi proces načrtovanja si je dobro narediti dodatne opombe, ki se uporabijo za dokončanje varnostne politike.
- Izpopolniti je treba varnostno politiko in jo razdeliti zaposlenim v vašem podjetju. Uporabljena mora biti, ko se izvaja in spremlja varnost v sistemu (IBM, 2021).

Varnostne politike bi morale vključevati ključne informacije o delovanju, ki jih morajo zaposleni sprejeti in upoštevati skozi vsakodnevno delovno življenje. Te politike bi morale vključevati vse od splošnih operativnih postopkov (npr.: kaj storiti v primeru požara, kako pogosto se izvajajo požarne vaje) do podrobnih navodil za ravnanje v primeru poškodb, če je nekdo poškodovan na delovnem mestu ali v stavbi. Pomembna je varnostna politika, ki je pogosto posredovana in dostopna vsem. Ključnega pomena je, da organizacije razpravljajo o varnostnih politikah z zaposlenimi in vodji, da zagotovijo razumevanje in sprejetje (iReport Source, 2022).

6.2 Oblikovanje varnostnih programov

Pomena dobro zasnovanega programa varnega upravljanja se večina zaveda, vendar ga vsi žal ne izvajajo. Sposobnost organizacije, da poskrbi za varnost svojih zaposlenih, je odvisna od njene sposobnosti oblikovanja, izvajanja in izboljšanja procesov ter programov upravljanja varnosti v podjetju.

Kritični elementi učinkovitega programa upravljanja varnosti so zaveza vodstva, komunikacija, vključenost zaposlenih, analiza delovnega mesta, preprečevanje in nadzor nevarnosti, usposabljanje za zaposlene, nadzornike in vodje (SHRM, 2024).

Zaveza vodstva predstavlja dejavno podporo vodij. Tudi vodstvo mora biti vključeno v izvajanje in obveščanje o programih, saj na tak način tudi zaposleni stvar jemljejo resneje. Vodstvo lahko svojo zavezanost izkazuje tudi z vključevanjem varnosti in zdravja v poslovne prakse; vključevanjem zaposlenih v dejavnosti, povezane z varnostjo in zdravjem, ter zagotavljanjem, da so vsi cilji, politike, postopki in načrti posredovani zaposlenim. Učinkovitost varnostnih ukrepov in programov temelji tudi na komunikaciji. Komunikacijska strategija mora biti oblikovana in izvajana na način, da podpira cilje celotnega programa varnega upravljanja. To lahko poteka preko beležk, e-pošte, internih sporočil, spletnih seminarjev, osebnih sestankov osebja, virtualnih skupinskih srečanj in podobno. Osnovna zahteva vsakega dobrega programa varnosti in zdravja je zagotavljanje sodelovanja zaposlenih pri oblikovanju in delovanju samega programa. Sodelovanje zaposlenih pomeni, da se spodbuja k polni udeležbi na programih, občasnimi pregledi na delovnem mestu in rednimi varnostnimi ter zdravstvenimi pregledi. Učinkovit program

varnega upravljanja pa vključuje tudi usposabljanje zaposlenih in vodij. Program mora vsebovati določene komponente, kot so usposabljanje o nevarnostih; usposabljanje o odgovornostih; pisne odgovornosti vodij; načrt za ravnanje v primeru nevarnosti; izobraževanje in usposabljanje, osredotočeno na trenutne nevarnosti, in podobno (SHRM, 2024).

Najboljša podjetja na svetu dajejo prednost zdravju in varnosti zaposlenih, tako da je to skupna odgovornost za vse. Ta podjetja to počnejo na strateški način, ki jim omogoča učinkovito izvajanje preprečevanja, hkrati pa jih opremi za učinkovito obvladovanje morebitnih incidentov.

Varnost, zdravje, zadovoljstvo, motivacija in kreativnost so predpogoji, ki morajo biti izpolnjeni, če želimo, da zaposleni dosegajo kakovostni delovni učinek. Skrb za varnost zaposlenih predstavljajo tudi programi za varnostno ozaveščanje in izobraževanje zaposlenih (Dvojmoč, 2020).

Načini, s katerimi se lahko zmanjšajo tveganja za poškodbe na delovnem mestu, so naslednji:

- Vključitev ljudi z različnih delov organizacije, da bo varnost deljena odgovornost.
- Dobra organizacija in struktura, da se zagotovita dosledna rast in uspešnost.
- Proaktivnost, preventiva in integriranost v kulturo celotne organizacije. (iReport Source, 2022)

Prav tako je dobro, da se zaposlene pogosto opomni, da ima varnost prednost pred produktivnostjo. To sporočilo se lahko včasih izgubi zaradi vsakodnevnih pritiskov izpolnjevanja naročil. Zaposleni imajo včasih občutek, da prejemajo mešana sporočila, zato jih je treba opomniti na prednostno nalogo varnosti. Nevarno vedenje je naravna navada večine zaposlenih, ki se tega ne zavedajo. Pogosto se dejavnost izvaja na napačen način tako dolgo, da se zaposleni v mnogih primerih niti ne zavedajo nepravilnega vedenja. Podjetja lahko ustvarijo dobro vedenje z oblikovanjem pozitivnih navad in opuščanjem starih. Tu pride v poštev koncept spremembe navad (iReport Source, 2022).

Sposobnost hitrega in natančnega prepoznavanja situacij z visokim tveganjem je nekaj, kar bi moralo biti na kontrolnem seznamu vsakega vodje varnosti za varnostno delovanje. Vodilni kazalniki lahko zagotovijo vpogled tako, da lahko organizacija predvidi, kaj bi se lahko zgodilo, in ukrepa, da prepreči nastanek nesreč. Vodilni kazalniki vključujejo ukrepe, kot so pogostost varnostnega usposabljanja, število in rezultati varnostnih revizij in

inšpekcij, kot tudi vedenje, ki odraža operacije, vključno s srednjim časom dokončanja korektivnih ukrepov, vključenost zaposlenih v proaktivne dejavnosti in celo vključenost vodstva. S pridobivanjem vpogleda v vodilne in zaostajajoče kazalnike lahko organizacije pridobijo popolno sliko vseh dejavnosti varnostnega programa, s končnim ciljem preprečiti nesreče, še preden se zgodijo (iReport Source, 2022).

Podjetja z nizkimi stopnjami poškodb svoje zaposlene opremijo za uspeh in to počnejo z več kot le procesi in programi upravljanja varnosti. Izkoriščajo vrhunska orodja in sisteme, da so njihovi zaposleni pripravljeni in imajo na razpolago vse, kar potrebujejo. Najučinkovitejši program upravljanja varnosti je tisti, ki vsakega zaposlenega opremi za hiter dostop do informacij, ki jih potrebuje, in poročanje o težavi. Ne glede na to, ali so te informacije varnostni list, zapis o usposabljanju ali rezultat revizije varnosti, podjetja zdaj izkoriščajo rešitve za upravljanje mobilne varnosti za izboljšanje pravočasnosti odziva in komunikacije. Tako kot podjetja svojim zaposlenim zagotavljajo osebno zaščitno opremo, tudi najboljši voditelji varnosti priznavajo pomen mobilne varnostne programske opreme za izboljšanje njihovega splošnega programa upravljanja varnosti (iReport Source, 2022).

Naravno je, da želimo delo končati v predvidenem roku – ali celo pred časom – toda z odnosom »opravimo hitro« se zgodijo nesreče. Organizacije na najvišji ravni poudarjajo pomen poročanja o morebitnih težavah, preden se pojavijo, ali poročanja o varnostnih incidentih v trenutku, ko se zgodijo. Poskrbeti je treba, da bodo zaposleni razumeli, da ne smejo izbirati bližnjic in da je varnost na prvem mestu. Nesreča vpliva na produktivnost bolj kot kar koli drugega v podjetju, zato je nujno, da bodo vsi razumeli povezavo med varnostjo in produktivnostjo – še posebej tisti menedžerji, ki se ocenjujejo na podlagi produktivnosti (iReport Source, 2022).

»Resolucija o nacionalnem programu varnosti in zdravja pri delu 2018–2027 (ReNPVZD18–27)« (2018) želi povezati vse deležnike v sistemu varnosti in zdravja pri delu, da bodo po svojih najboljših močeh in v skladu s svojim poslanstvom združili moči in sodelovali pri uresničevanju splošno sprejete vizije na področju varnosti in zdravja pri delu v Sloveniji. V Resoluciji so določeni ukrepi za uresničitev vseh strateških ciljev, usmerjenih v zagotovitev varnosti in zdravja pri delu (»ReNPVZD18–27«, 2018). Strateški cilji na področju varnosti pri delu so zmanjšanje števila nezgod pri delu za 20 % v naslednjih 10 letih, zagotovitev varne uporabe nevarnih kemičnih snovi in zagotovitev kakovostnega izvajanja strokovnih nalog varnosti pri delu. Na področju zdravja pri delu pa so ti cilji med drugimi ureditev, uveljavitev, spremljanje in nadgrajevanje sistema ugotavljanja, potrjevanja in prijavljanja poklicnih bolezni; vzpostavitev mehanizmov za

zgodnje odkrivanje in pomoč v primeru z delom povezanih duševnih obremenitev; zagotovitev kakovostnega izvajanja strokovnih nalog izvajalcev medicine dela in podobno.

Zaposleni bi morali biti zainteresirani in dolžni prijaviti nevarnost ali potencialno težavo, ko jo opazijo. Ko bodo vsi čutili odgovornost za izvajanje varnostnih politik in postopkov, bo celotna organizacija izboljšala svojo varnost. Zavedati se je treba, da se zavezanost varnosti in vzpostavljanju varne in zdrave kulture nikoli ne konča. Vedno se najdejo področja in s tem priložnosti za izboljšave, nove zaposlene za usposabljanje, nove nevarnosti za obravnavanje in še več. Z vrhunskim programom upravljanja varnosti se pridobi sistematičen pristop k ocenjevanju, izboljšanju in pregledu varnostnih dejavnosti za povečanje organizacijske uspešnosti (iReport Source, 2022).

Programi stalnega strokovnega usposabljanja morajo vsebovati vsaj enega od naslednjih programskih sklopov:

- delovno okolje, sredstva za delo in druge strokovne naloge,
- naloge izvajalca medicine dela,
- promocijo zdravja,
- aktualno kampanjo Evropske agencije za varnost in zdravje pri delu.

Programi, ki so prilagojeni usposabljanju delodajalcev kot strokovnih delavcev trajajo vsaj 16 ur, in zajemajo določene programske sklope, kot so pregled predpisov, ocenjevanje tveganja, informiranje delavcev, promocijo zdravja in podobno (Sektor za varnost in zdravje pri delu, 2020).

6.3 Izdelava poslovnih načrtov za odziv na krizne situacije

Kriza je stanje v gospodarstvu, ko se ugodne razmere za razvoj začnejo hitro slabšati. Lahko je kot pomanjkanje česa ali kot neugodno, težko rešljivo stanje (»Kriza«, n. d.).

Krizno upravljanje je del korporativne varnosti in pomeni sprejemanje učinkovitih ukrepov za zmanjšanje, omejitev in preprečitev tveganj. Cilj le-tega je ustvariti sistem, ki je manj ranljiv in odpornejši na različna tveganja in grožnje (Haimess, 2009). Krizno upravljanje prav tako zajema vse vidike, ki so potrebni za varnost in zaščito človeških življenj, premoženja in ugleda same organizacije. Ekipa za krizno upravljanje je sestavljena iz stalnih in specifičnih članov. Najpogosteje je sestavljena iz glavnega korporativnega menedžerja in njegovih pomočnikov, ki tudi opravljajo menedžersko funkcijo. V

določenih situacijah se ekipi pridružijo tudi drugi posamezniki, ki imajo potrebna, specifična znanja, ki so potrebna za reševanje nastale situacije (Cabric, 2015).

Pri kriznem upravljanju je pomembno predvsem strateško razmišljanje, ki pripomore k predvidevanju mogočih dogodkov, analiziranju ranljivosti in sestavi načrtov ukrepov. Ko pride do krize, jo je treba čim prej analizirati in ugotoviti vzroke za nastanek (Khodarahmi, 2009). Krizno upravljanje je povzeto tudi kot skupek nekih dejavnosti, ki rešujejo in obvladujejo krizo in krizne situacije. Z določenimi postopki, dogovori in odločitvami vpliva na potek same krize (Vidic, 2008).

Omenjena strateška komunikacija pripomore k spopadanju s kriznimi razmerami. Z že vnaprej določenimi kanali komuniciranja je omogočeno hitrejše in učinkovitejše ukrepanje v kriznih razmerah. S tem se zmanjšajo negativni vplivi krize in se zagotavlja nemoteno poslovanje organizacije, kar pa je seveda najpomembnejše (Frandsen in Johansen, 2017).

Za učinkovito in uspešno izdelavo načrta kriznega upravljanja je treba ta načrt razdeliti na manjše, bolj dosegljive korake. To lahko pomaga prepoznati verjetna tveganja, ne da bi morebitna kriza močno vplivala na organizacijo in jo kot celota preobremenila. Za organizacijo načrta je dobro slediti naslednjim korakom (Team Asana, 2022):

- **Določitev ekipe za krizno vodenje**

Pred prvim korakom pri načrtovanju kriznega upravljanja je treba izbrati skupino vodij za sodelovanje med postopkom kriznega načrtovanja. Ekipa mora vključevati ljudi, ki bodo ukrepali v krizi. Sestavljena mora biti na samem začetku načrtovanja kriznega upravljanja, z namenom, da bodo vsi poznali podrobnosti krizne strategije. Člani ekipe morajo biti strokovnjaki s posebnimi znanji z različnih področij, ki lahko pomagajo v nastalih kriznih situacijah (Parsons, 2021).

- **Ocenitev tveganja**

Za začetek procesa načrtovanja je dobro organizirati t. i. »brain storming«, da se ocenijo različna tveganja, s katerimi se lahko podjetje sooči. Pri tem se lahko uporabi register tveganj za prepoznavanje in analizo verjetnosti pojava tveganj. Register tveganj lahko odpravi zamude pri napredku in se pripravi na morebitne zastoje. Prav tako pomaga vizualizirati, katera tveganja se bodo najverjetneje pojavila, na podlagi katerih se lahko načrtuje odziv na ta tveganja.

– Določitve poslovnega učinka

Ko so visokoverjetna tveganja, ki bi lahko vplivala na podjetje identificirana, je treba določiti vpliv teh tveganj na poslovanje s pomočjo ekipe za krizno vodenje. Vsako tveganje lahko povzroči različne rezultate, zato jih je pomembno analizirati ločeno. Potencialni vplivi na poslovanje lahko vključujejo izčrpavanje strank, poškodovan ugled, zamudo pri prodaji, izgubljeni dohodek ali regulativne kazni.

– Načrtovanje odziva

Sprejeti je treba vsako tveganje, ki je bilo identificirano. Na podlagi tega se določi, katere ukrepe bi morala ekipa sprejeti, da bi se odzvala na grožnjo, če bi se zgodila. Na primer, če je pri delu uporabljena programska oprema in podjetje doživi kibernetski napad, bo najverjetneje potrebna pomoč nekoga, ki bo objavil novice strankam, in druge osebe, ki bo opravila oceno škode.

– Utrditev načrta

Načrt je dobro utrditi po tem, ko se razumejo grožnje, s katerimi se lahko soočita podjetje oz. organizacija. Načrt kriznega upravljanja je več kot pisna ali ustna strategija. Vključevati mora ključne elemente, kot so aktivacijski protokol in stiki za nujne primere. Prav tako je treba sodelovati s ključnimi zainteresiranimi stranmi, da vsi razumejo, kaj storiti in kdaj.

– Pregled in posodobitev

Ko je krizni načrt končan, je treba pregledati končni izdelek in se prepričati, da ni vrzeli. Načrt kriznega upravljanja je dobro posodobiti vsaj enkrat letno, ker se morebitna tveganja lahko sčasoma spremenijo (Team Asana, 2022).

Krizni menedžment je v času krize prisoten tako na državni ravni kot tudi na ravni organizacij. Grožnje, ki ogrožajo državo, ogrožajo tudi organizacije. Primer krizne situacije je epidemija covida-19, pri čemer je ukrepe najprej sprejela Evropska unija, nato Republika Slovenija, potem so jih začele upoštevati tudi organizacije na lokalni ravni s pomočjo varnostnega menedžerja. Covid-19 je bil velik kazalnik, kaj lahko kriza naredi tako malim kot tudi velikim organizacijam in podjetjem. Obdobje pandemije je bil krizni čas, v katerem je bilo pomembno predvsem vodstvo organizacij, ki je moralo sprejemati pomembne odločitve in ukrepe, ki so spreminjali njihovo poslovanje in delovanje. Pri vsaki krizni situaciji je pomembno, da zaposlene o tem obvestijo vodilni posamezniki, saj se s tem

ohranja predvsem pošten odnos med njimi. Pomembno je tudi sprotno obveščanje, kar se je izkazalo kot zelo dober ukrep v začetku pandemije. Kot je bilo že omenjeno, sta komunikacija in sprotno obveščanje ključ do dobrega delovnega okolja in tudi boljših rezultatov, ko pride do kriznih situacij (Lesjak, 2020).

Lesjak (2020) opozarja, da bi morale organizacije krizni načrt pripraviti še pred nastankom krize oz. krizne situacije. Predvsem kriza v času covida-19 je omogočila vpogled tudi na to področje, saj organizacije in podjetja niso bili pripravljeni na nastalo situacijo. Treba se je predhodno pripraviti, opazovati svet okoli sebe, poleg tega pa razumeti tveganja in ranljivosti ter se soočiti z dejstvom, da pridejo tudi slabši časi, na katere pa se lahko pripravimo.

6.4 Varnostni protokoli in postopki

Varnostni postopek je sestavljen iz korakov in nalog, ki so potrebni za zagotavljanje varnosti pri vsakodnevnem delovanju organizacije. Varnostni postopki delujejo skupaj z varnostnimi politikami, standardi in smernicami za izvajanje orisov za varnostne operacije v katerem koli podjetju.

Poleg tega lahko varnostni postopek implementira, omogoči ali uveljavi varnostne kontrole, določene v pravilnikih vaše organizacije. Te varnostne politike, standardi, smernice in postopki se upoštevajo v vsakem varnostnem protokolu. Prav tako varnostne politike delujejo kot temelj varnostnega programa organizacije (Van Deventer, 2023).

Kar zadeva raven podrobnosti, obstajajo bistveni koncepti in komponente, ki jih je treba poznati za varnostne postopke.

Varnostni postopki igrajo ključno vlogo pri delovanju in funkcijah katere koli organizacije. Ti postopki in politike zagotavljajo, da ima organizacija metode za varovanje svojih zaposlenih, podatkov, ugleda in delovnega mesta. Pomagajo preprečiti nesreče in poškodbe, ki bi lahko resno ovirale delovanje organizacije. Postopki, osredotočeni na kibernetsko varnost, zagotavljajo tudi raven obrambe pred kibernetskimi napadi, ki lahko poškodujejo funkcije organizacije in povzročijo izgubo pomembnih podatkov (Van Deventer, 2023).

Poleg tega lahko prisotnost varnostnih postopkov tako delavcem kot strankam da občutek varnosti in zagotovila. To pa lahko do neke mere izboljša moralo in produktivnost delavcev (Van Deventer, 2023).

Vsaka organizacija bo imela drugačno varnostno politiko na delovnem mestu, ki zajema različne teme. To lahko temelji na dejavnikih, kot so velikost organizacije, lokacija ali panoga. Tukaj je nekaj pogostih varnostnih tem, ki bi morale biti vključene v pravilnik o delovnem mestu (Kirkham, 2022).

– Fizična varnost na delovnem mestu

Fizična varnost je pogosto prva obrambna linija za varnost zaposlenih. Gre za varnost fizičnih pisarniških lokacij. Zajemati mora vse od nadzora dostopa, preverjanja osebne izkaznice ter alarmov in nadzora. Vključevati mora tudi preprečevanje požarov, sisteme za sledenje obiskovalcev in zaposlenih ter vseh fizičnih sredstev, ki so v pisarni. To vključuje prenosne računalnike, monitorje, mize in drugo (Kirkham, 2022).

– Kibernetska varnost

65 % organizacij po vsem svetu poroča o porastu kibernetskih napadov. Varnostne ekipe morajo posvetiti veliko časa zaščiti podjetja pred hekerji, lažnim predstavljanjem, notranjimi napadi in še več. Tu nastopi politika kibernetske varnosti. Politika mora organizacijo zaščititi pred kakršno koli kršitvijo ključnih podatkov organizacije. To vključuje podatke, shranjene v napravah, omrežjih in oblaku. Varnostni ukrepi v politiki bodo prav tako pomagali preprečiti nezaželene goste in potencialne hekerje. Dvostopenjska avtentikacija, šifriranje in varnostno kopiranje so odlični primeri varnostnih ukrepov, ki bi jih morale uporabljati organizacije. Priporočljivo je izvajati redna usposabljanja zaposlenih, da se naučijo kibernetske ozaveščenosti, kot je odkrivanje prevarantskih e-poštnih sporočil ali uporaba VPN v javnih domenah (Kirkham, 2022).

– Varnost infrastrukture

Varnostna politika infrastrukture je ključnega pomena za zaščito neprekinjenega poslovanja. Prav tako pomaga zaščititi podjetje pred motnjami storitev in zunanjimi grožnjami. Infrastrukturna politika mora zajemati področja, kot so požarni zidovi spletnih aplikacij, navidezna zasebna omrežja, varnost programskega vmesnika aplikacij, sistemi za preprečevanje vdorov in brezžična varnost. Zajemati mora tudi varnost v oblaku, vključno s shranjevanjem podatkov ter procesi in sistemi v oblaku.

Zagotoviti je treba, da varnostna politika infrastrukture na delovnem mestu ponuja postopke, ki jih morajo ljudje upoštevati. Pomembna je tudi vključitev varnostnih standardov za zaščito organizacijske infrastrukture. Na primer, politika mora opisati

ukrepe, ki so opredeljeni za zaščito organizacije v primeru požara. Vključevati mora tudi različne varnostne postopke na delovnem mestu, ki jih morajo ljudje upoštevati, na primer, kateri požarni izhod uporabiti in kje se zbirati zunaj (Kirkham, 2022).

- **Zdravstvena varnost**

Zdravje in varnost sta še vedno pomembna, ko je govora o splošni varnostni politiki na delovnem mestu. Politika zdravstvene varnosti mora zajemati vse, od preverjanja cepiv, zdravstvenih pregledov, tehnologije brez dotika do prve pomoči itd. Odvisno od vrste organizacije je treba imeti tudi strogo politiko glede kemikalij ali zdravil v prostorih (Kirkham, 2022).

- **Krizno upravljanje**

Varnostna politika kriznega upravljanja bi morala zaposlene pripraviti in zaščititi pred nepričakovanimi krizami na delovnem mestu. To je lahko politika obnovitve po nesreči v primeru naravne nesreče. To bi lahko bila tudi politika ukrepanja v sili v primeru napada. Politika mora vključevati tudi načrte neprekinjenega poslovanja v primeru kakršne koli nepričakovane krize. To je lahko delo od doma ali samodejni dopust po nujnem primeru (Kirkham, 2022).

Z vzpostavljenim postopkom lahko zaposleni pomagajo pri doslednem vzdrževanju zaščite pred notranjimi in zunanjimi tveganji. Varnostni postopki morajo biti neposredni pri tem, kako temeljito rešiti vsak problem (Van Deventer, 2023).

6.5 Ocena ogroženosti

Ocena ogroženosti je nekakšna ocena verjetnosti, da bo prišlo do uresničitve določenih groženj zoper določeno tarčo v nekem določenem obdobju (Britovšek, 2019).

Zajema:

- Opis dejavnosti subjekta, iz katerega je mogoče razbrati, katere so tiste stopnje v procesu, ki so izpostavljene tveganju ali ogrožanju.
- Opis objektov, ki jih uporablja subjekt, na osnovi katerega jo možno ugotavljati kritične točke, na katerih je možno pričakovati ogrožanja varnosti.

- Opis dokumentacijskih in informacijskih procesov, ki jih uporablja subjekt, na osnovi katerega je mogoče določiti tiste kritične točke v procesih, ki zahtevajo uvedbo določenih varnostnih ukrepov.
- Na podlagi zgornjih postopkov identificirana tveganja.

Ocena stanja, ogroženosti in tveganj, stroškov in koristi se izdela na podlagi: zahtev naročnika; zakonskih predpisov, ki urejajo področje varnosti v podjetju (predpisi s področja zaščite premoženja; varnosti in zdravja pri delu; požarnega varstva; ekologije; logistike; ergonomije; industrijske lastnine; obrambe, zaščite in reševanja ter drugih področij varovanja); varnostnih standardov ter ponudb o varnostnih in zavarovalnih storitvah (Vidic, 2008).

Celovita ocena ogroženosti predstavlja temelj za oblikovanje dokumenta o varnostni politiki, torej za vzpostavitev varnostne politike gospodarske družbe (Vršec, 2006). Ocena ogroženosti tako zagotavlja, da bodo identificirana vsa tveganja in grožnje ter da bodo predvideni vsi ukrepi za primerno raven varnosti (Podbregar idr., 2010).

Za izdelavo realne ocene ogroženosti je treba storiti predvsem naslednje (Čas, 2006): a) opraviti temeljit pregled gospodarske družbe, ki vključuje pregled vseh objektov z okolico, pregled dislociranih enot, pregled prostorov, dostopa do objektov in drugo; b) prepoznati objektivne nevarnosti v notranjem in zunanjem okolju gospodarske družbe, vključno s proizvodnimi, poslovnimi in logističnimi procesi; c) opraviti razgovore s pristojnimi odgovornimi osebami v podjetju in d) pregledati obstoječe varnostne načrte, poročila in druge notranje akte, ki pokrivajo varnostna in sorodna področja.

Glede posameznih elementov ocene ogroženosti si avtorji niso enotni, vendar pa se v svojih opredelitvah bistveno ne razlikujejo. Kljub različnim pristopom bi morala vsaka ocena ogroženosti imeti naslednje sestavine (Podbregar, 2007): a) opis dejavnosti gospodarskega subjekta, iz katerega je mogoče razbrati, katere so tiste stopnje v procesu, ki so izpostavljene tveganju ali ogrožanju; b) opis objektov gospodarskega subjekta, na osnovi katerega jo možno identificirati kritične točke, na katerih obstaja možnost ogrožanja varnosti; c) opis dokumentacijskih in informacijskih procesov gospodarskega subjekta, na osnovi katerega je mogoče določiti tiste kritične točke v procesih, ki zahtevajo uvedbo določenih varnostnih ukrepov, in d) tveganja, identificirana na podlagi zgornjih opisov.

Pomembnost ocen ogroženosti je predvsem v tem, da nas opozarjajo na grožnje (Britovšek, 2019). Ocene ogroženosti so del ocene tveganj, za korporativno varnost pomembne predvsem z vidika upravljanja varnosti in zdravja pri delu. Ocena tveganja pomaga pri ustvarjanju zavedanja o nevarnostih; ugotovitvah, kdo bi lahko bil ogrožen; ocenitvah, ali je potreben program nadzora; ugotovitvah, ali so ukrepi ustrezni; preprečevanju poškodb ali bolezni; določitvi prednostnih razvrstitev nevarnosti ter pri izpolnjevanju zakonskih zahtev (Infocenter, 2023).

6.6 Načrt za krizne situacije

Načrt kriznega upravljanja opisuje, kako se bo podjetje odzvalo, če pride do krize oziroma do krizne situacije, ki bi negativno vplivala na dobičkonostnost, ugled ali sposobnost delovanja organizacije. Načrt mora opredeliti, kdo bo ukrepal in kakšne bodo njegove/njihove vloge. Cilj načrta kriznega upravljanja je zmanjšati škodo in čim hitreje vzpostaviti poslovanje. Sam načrt mora organizacije pripraviti na kakršno koli katastrofo ali motnjo, ki se lahko zgodi (Meyer, 2023).

Načrt kriznega upravljanja je živi dokument, na katerega se lahko ekipa sklicuje in ga pogosto posodablja. Obstaja več načinov, kako začrtati načrt, vendar je tipični krizni načrt videti kot kontrolni seznam. Ko pride do nesreč, lahko ekipa preveri, kaj je treba narediti, da se odzove na krizo (Team Asana, 2022).

Na primer, podjetje za trženje družbenih medijev je lahko bolj izpostavljeno tveganju za organizacijsko nesrečo, ki zahteva javno opravičilo, medtem ko je lahko tehnološko podjetje bolj izpostavljeno tveganju kibernetskega napada. Panoga, v kateri ste, vam lahko pomaga določiti morebitne krize in ugotoviti, kako se z njimi spopasti (Team Asana, 2022).

Odnosi z javnostmi so pogosto sestavni del procesa kriznega upravljanja. Organizacija se lahko odloči, da bo pri komunikacijskih vidikih, kot je delo z mediji, pridobila zunanjo pomoč pri odnosih z javnostmi. Z javnim odzivom na krizne razmere se lahko organizacija zoperstavi vsem zavajajočim in lažnim informacijam ter si prizadeva zmanjšati skrbi. Če organizacija dovolj hitro reši krizo, morda javnosti ne bo treba seznaniti z dogodkom in pritegniti neželene pozornosti (Barney, 2023).

Načrt kriznega upravljanja je zelo pomemben, zato je pomembno vedeti tudi, kako ga ustvariti. Najprej je treba oceniti vsa mogoča tveganja in grožnje. Pri tem sodeluje celotna ekipa, pomembno pa je tudi, da je osredotočenost na panogi, v kateri organizacija posluje. Tveganja so lahko na primer kibernetski napadi, ekstremni vremenski dogodki, napake

družbenih medijev, težave na delovnem mestu, napake v odnosih z javnostmi in podobno. Naslednji korak je ustanovitev krizne ekipe, ki mora imeti svojega vodjo. Vsi v ekipi morajo poznati vse podrobnosti načrta in tudi prispevati k le-temu. Tretji korak je ugotovitev, kakšen vpliv bi lahko imela potencialna tveganja na organizacijo in njeno poslovanje. Vsako tveganje je treba posebej analizirati, saj imajo lahko različne vplive. To so na primer regulativne globe, škoda ugledu, izgubljeni dohodek in podobno. Pomembno je vedeti, kako se načrta sploh lotiti in predvsem katere ukrepe sprejeti, ko pride do kriznega dogodka. Načrt se mora začeti s pisno (ali ustno) strategijo in mora vključevati kontakte za nujne primere ter aktivacijski protokol. Korak, ki sledi temu, je pregled načrta. To pomeni, da mora vsak posameznik načrt pregledati in se prepričati, da je ta dovolj podroben in so določena vsa tveganja in grožnje. Ta korak predstavlja povratne informacije vseh vpletenih in sodelujočih pri načrtu. Prav tako je treba načrt redno pregledovati, saj se tudi tveganja spreminjajo. Šesti korak je združitev dokumenta, ki opisuje načrt kriznega upravljanja. Ta služi kot referenca za ekipo v času krize, na podlagi katere bodo vsi vedeli, kaj storiti. Predzadnji korak je zagotovitev, da načrt razumejo vsi vpleteni. Dostop do načrta mora biti preprost, zaposleni pa morajo biti o vsem usposobljeni. Zadnji korak je ocenitev stanja po nastopu krize. Po vsaki krizi je dobro načrt posodobiti in pregledati, saj se na ta način zagotovijo spremembe in izboljšajo prihodnji odzivi (Duplain, 2023).

Odgovorite na vprašanja

Kaj določa varnostna politika?

Kaj mora varnostna politika opisati?

Kaj pomeni razvoj varnostne politike in kako poteka?

Ali se varnostna politika lahko spreminja? Opredelite.

Kaj je program varnega upravljanja?

Kateri so elementi učinkovitega programa upravljanja? Naštejte jih.

Opišite zgoraj naštete elemente.

Kako se na delovnem mestu zmanjšajo tveganja? Podajte nekaj primerov.

Kaj so kazalniki v organizaciji?

Na kaj opozarjajo kazalniki?

Katere tri komponente so ključne za zmanjšanje pogostosti incidentov na delovnem mestu?

Kaj so krizne situacije? In kaj je krizno upravljanje?

Kaj je načrt kriznega upravljanja?

Kako se organizira načrt kriznega upravljanja? Opredelite po korakih.

Kakšna je vloga kriznega menedžmenta v času krize?

Kako bi opredelili, kaj so varnostni protokoli in kaj varnostni postopki? Pojasnite s svojimi besedami.

Katera področja varnosti bi morala biti vključena v pravilnik o delovnem mestu?

Kaj je ocena ogroženosti?

Kaj vse zajema ocena ogroženosti?

Zakaj je ocena ogroženosti priporočljiva oziroma »dobra« za organizacijo?

Kako se izdela ocena ogroženosti?

Kateri so glavni elementi ocene ogroženosti?

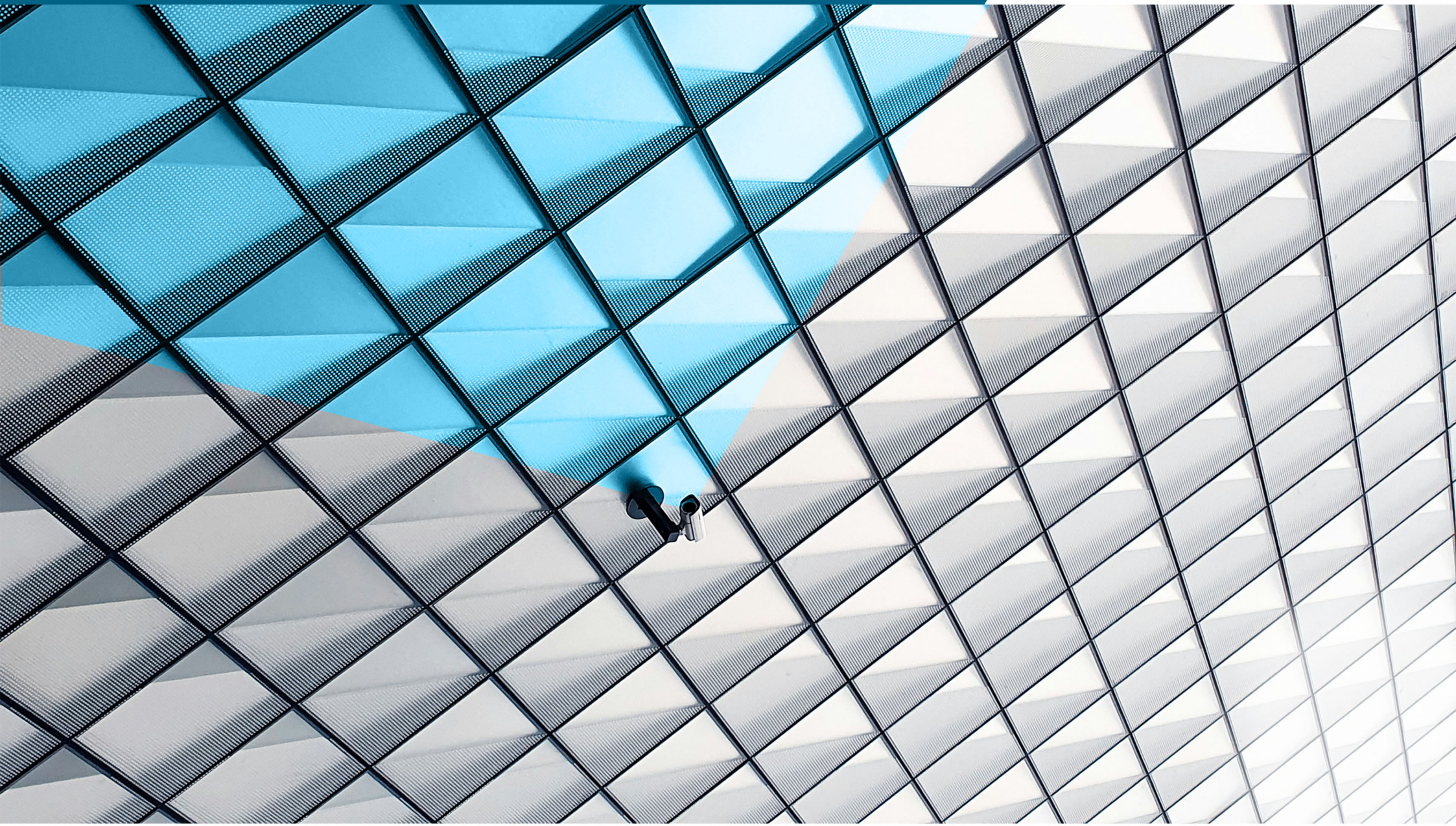
Kaj opisuje načrt za krizne situacije?

Kaj opredeljuje načrt za krizne situacije?

Kateri so koraki pri načrtovanju načrta za krizne situacije oz. kriznega upravljanja?

ZAPISKI

DEL II



SPECIFIČNA PODROČJA KORPORATIVNE VARNOSTI

Univerzitetna založba
Univerze v Mariboru

7 Menedžment neprekinjenega poslovanja

V pravni proces zagotavljanja zakonitega in nemotenega poslovanja spadajo neprekinjeno poslovanje, zaščita poslovnih skrivnosti, ki smo jih že omenili in tudi predstavili, zakoni, ki jih določajo, ter pravna ureditev protikorupcijskih procesov in integritete zaposlenih.

Neprekinjeno poslovanje je eden izmed ključnih elementov korporativne varnosti in zagotavlja podporo organizacijam po tem, ko pride do varnostnih incidentov in neugodnih razmer, kot so na primer pandemije, naravne nesreče, bolezni, teroristični napadi, hekerski napadi in druge nepričakovane spremembe v poslovnem okolju (Will in Brauweiler, 2020). Neprekinjeno poslovanje vključuje identifikacijo ključnih kritičnih točk v poslovanju organizacije in na podlagi tega pripravo strategije odzivanja v primeru pojava neželenih dogodkov. Lahko rečemo, da je cilj neprekinjenega poslovanja ta, da organizacija ne glede na dane okoliščine in pojave varnostnih tveganj še naprej opravlja svoje delo in posluje nemoteno ter sproti tudi obvlada tveganja in tudi čim hitreje okreva (Wu, 2021). V tem kontekstu lahko upravljanje neprekinjenega poslovanja definiramo kot holističen pristop, ki identificira potencialne grožnje in tveganja ter tudi kakšen bi lahko bil njihov vpliv na delovanje in poslovanje organizacije (ICS, Institut za korporativne varnostne študije, 2019). Pri tem se je treba zavedati tudi dejstva, da ni vse v organizaciji ključnega pomena, kar pomeni, da se je pomembno odločiti, kaj je najbolj pomembno, da se ohrani za samo delovanje in kaj bi lahko bilo vzpostavljeno tudi kasneje. Celotni postopek vključuje celotno organizacijo, kar pomeni, da so vključeni tako vodje kot tudi vsi zaposleni (Infocenter, n. d. b).

Organizacije se morajo za uspešno delovanje zavedati morebitnih nevarnosti in dejstva, da je celovito obvladovanje tveganj in neprekinjenega delovanja oz. poslovanja nujni dejavnik za uspešno in neprekinjeno poslovanje (Gerginova, 2018). Pri zagotavljanju neprekinjenega poslovanja je pomembna tudi strateška komunikacija, ki je ključna pri spopadanju s kriznimi razmerami. Ker so kanali komuniciranja že vnaprej določeni, omogočajo hitrejše in učinkovitejše ukrepanje v kriznih razmerah, s čimer se zmanjšajo negativni vplivi dane situacije, z vidika korporativne varnosti pa se zagotavlja neprekinjeno poslovanje, ki je, kot že večkrat omenjeno, izredno pomembno (Frandsen in Johansen, 2017).

Glavni cilji menedžmenta neprekinjenega poslovanja so torej:

- Omogočanje osredotočenega pristopa pri razvoju načrta poslovanja.
- Omogočanje pragmatičnega, stroškovno učinkovitega in iznajdljivega načrta sanacij, da lahko organizacija nemoteno posluje tudi v času tveganj in krize.
- Zmanjševanje vpliva krize na delovanje celotne organizacije in njene zaposlene.
- Zagotavljanje varnosti osebja, zaščita ugleda organizacije in blagovne znamke ter dokazovanje učinkovitega upravljanja medijem in trgom.
- Zaščita sredstev in izpolnjevanje zakonskih, regulatornih in zavarovalnih zahtev (Riantini Supriadi in Sui Pheng, 2017).

Tri ključne sestavine načrta neprekinjenega poslovanja so torej odpornost, obnovitev in nepredvidene razmere. Odpornost organizacije se lahko poveča z oblikovanjem kritičnih funkcij in infrastruktur. Hitra obnova je prav tako zelo pomembna oz. je ključnega pomena. Določiti je treba cilje glede časa obnovitev za različne sisteme, lahko pa se popisujejo tudi viri in dogovori s tretjimi osebami za prevzem dejavnosti organizacije. Na podlagi nepredvidenih razmer je treba imeti načrt ukrepov za različne zunanje scenarije, ki se lahko zgodijo. Sem sodi tudi razdeljevanje odgovornosti znotraj organizacije, zamenjava strojne opreme, najem zasilnih pisarniških prostorov, ocena škode in podobno (Infocenter, n. d. b).

Omenja se tudi načrten pristop k upravljanju neprekinjenega poslovanja, ki ima preventivno in represivno funkcijo. O tem pristopu govorimo takrat, ko je v skrajnem primeru treba računati na izpad poslovanja na osnovni lokaciji in je treba poslovanje premestiti na rezervno lokacijo, ki pa mora imeti vzpostavljeno strojno, programsko in drugo opremo, ki omogoča delovanje ključnih poslovnih fukcij in procesov ter je za delovanje organizacije potrebna. Tako lahko načrte neprekinjenega poslovanja s kriznimi

načrti označimo kot glavno poslovno orodje za obvladovanje tveganj v organizaciji. Načrti neprekinjenega poslovanja predstavljajo učinkovito sredstvo za zagotavljanje poslovanja in delovanja organizacije tudi v kriznih situacijah in razmerah z izrednimi dogodki. Zagotavljajo korporativno vodenje, varnost, skladnost, poslovno uspešnost in tudi vzdržujejo konkurenčnost, ugled ter zaupanje v organizacijo samo (ICS, Institut za korporativne varnostne študije, 2019).

Neprekinjeno poslovanje je povezano z analizo ocene tveganj, ki mora biti izvedena na samem začetku procesa načrtovanja. Če je poslovni proces moten, je treba narediti analizo in na njeni podlagi ugotoviti, kakšen je vpliv na poslovanje, sestaviti načrt, testirati in izvajati tudi redne periodične preglede (Wright, 2017). Vse to so postopki, ki organizaciji pomagajo pri motnjah v poslovanju in po njih. Lahko zaključimo, da načrtovanje neprekinjenega poslovanja vključuje analizo in oceno tveganja, ukrepe za obvladovanje tveganj ter načrt o obnovitvi delovanja po krizni situaciji (Reid, 2021).

V sodobnih gospodarstvih se zavedajo, da se nešteti viri ogrožanja povezujejo z večino kriznih situacij, ki zahtevajo celovit, organiziran in dosleden pristop k njihovemu razreševanju. Uvaja se nov koncept pripravljenosti in preprečevanja različnih izrednih dogodkov (nesreč, katastrof, kriz), ki se je iz načrtovanja, ukrepanja ob nesrečah in neprekinjenega poslovanja (predvsem informacijske tehnologije) razvil v vseobsegajoč menedžment neprekinjenega poslovanja različnih organizacij. Da pa se program menedžmenta neprekinjenega poslovanja lahko vključi v organizacijsko kulturo, so potrebni: razumevanje organizacije, opredelitev strategij, vpeljava in implementacija, izvajanje, vzdrževanje in pregled. Vsi ti postopki potekajo v neprekinjenem ciklu. Poleg tega lahko tudi načrt neprekinjenega poslovanja vsebuje več načrtov, kot so načrti za ponovno vzpostavitev poslovanja; neprekinjeno obratovanje; zagotavljanje informacijske podpore; komuniciranje ob izrednih dogodkih; odziv na incidente; ponovno vzpostavitev po nesreči in zaščito življenj in lastnine (Dvojmoč, 2020).

Odgovorite na vprašanja

Zakaj je zagotavljanje neprekinjenega poslovanja pomembno za organizacijo?

Kaj vse vključuje menedžment neprekinjenega poslovanja?

Kateri so glavni cilji neprekinjenega poslovanja? Naštejte in opišite.

Kaj je načrt neprekinjenega poslovanja in kaj vsebuje?

S čim je povezan proces neprekinjenega poslovanja? Pojasnite.

Razmislite in zapišite svoje mnenje, kako lahko moteno poslovanje vpliva na organizacijo.

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

8 Fizična varnost

Zagotavljanje zasebne varnosti (angl. security), ki je prav tako eden izmed pravnih procesov korporativne varnosti, v Sloveniji zagotovljajo predvsem zasebnovarnostna podjetja, ki delujejo v skladu z Zakonom o zasebnem varovanju (»ZZasV-1«, 2011). Zasebno varovanje lahko opravljajo le podjetja in posamezniki, ki izpolnjujejo zakonske pogoje (Sotlar in Čas, 2011). V primeru zunanjih in notranjih groženj poleg zasebnovarnostnih podjetij varnost zagotavljajo tudi detektivi, v primeru varnostnega načrtovanja pa tudi Civilna zaščita (Dvojmoč, 2020).

8.1 Obvladovanje dostopa in varovanje objektov

Fizično varovanje vključuje ljudi, opremo in grajeno okolje za nadzor določenih dostopnih točk znotraj organizacije (Brooks, 2010). Fizična varnost predstavlja varnost, ki poskrbi za preživetje. Poudarek je na fizičnem vhodu osebe v stavbo oziroma na objekt ali okolje ter na škodo, ki jo oseba lahko povzroči. Glavni cilj fizičnega varovanja je preprečitev napadalcem, da bi fizično dostopali oziroma vstopali in vzeli, kar želijo. Pri tem je pomembno opozoriti na dejstvo, da morajo biti napadalci fizično prisotni s ciljem izkoristiti fizično ranljivost organizacije. Pod fizične napade štejemo prerezane kable, krajo podatkovnih strežnikov, tatvine sefov in podobno (Al-Fedaghi in Alsumait, 2019). Namen fizičnega varovanja je preprečiti, da bi osebe prišle do občutljivih predmetov oziroma predmetov, ki imajo določeno vrednost (Hunter, 2001).

Gospodarski subjekti imajo v praksi dve možnosti vzpostavitve varovanja objektov. Prva možnost predstavlja varovanje z lastnimi varnostniki, druga pa je pogodbeni najem varnostne službe na trgu varnostnih storitev. Prav tako se pojavljajo tudi primeri kombiniranega pristopa, ko varnostno dejavnost opravljajo lastni varnostniki v sodelovanju z najetimi (Vršec in Vršec, 2006). Izbor prve, druge ali tretje možnosti je odvisen od mnogih dejavnikov znotraj in zunaj posamezne gospodarske družbe.

V Sloveniji je veljavna ureditev s področja zasebnega varovanja urejena v Zakonu o zasebnem varovanju (»ZZasV-1«, 2011) iz leta 2011. S tem zakonom so določene pravice in dolžnosti oz. obveznosti gospodarskih družb, samostojnih podjetnikov, državnih organov, zavodov in drugih pravnih in fizičnih oseb na področju varovanja, ki ga država ne zagotavlja (Savski idr., 2017). Zasebni varnostniki imajo tako na razpolago veliko več ukrepov, kot so jih imeli pri predhodnih zakonih. Prav tako so pogoji, kdaj lahko varnostnik uporabi kateri ukrep, širši (Sotlar in Čas, 2011). Detektivska dejavnost je prav tako ena izmed možnosti zagotavljanja notranje varnosti v državi, spada k zasebnemu varstvu in je zakonsko regulirana dejavnost, ki zahteva sistemsko urejenost in učinkovit nadzor (Dvojmoč, 2017b). Urejena je z Zakonom o detektivski dejavnosti (»ZDD-1«, 2011), delo detektiva pa lahko izvaja posameznik, ki ima izdano licenco in izpolnjuje pogoje v skladu z zakonom. Detektivi opravljajo dejavnosti, kot so zbiranje, obdelava, posredovanje podatkov in informacij ter svetovanje na področju preprečevanja kaznivih ravnanj (Dvojmoč in Sotlar, 2018).

Zasebno varovanje lahko poteka v obliki pogodbe ali pa kot interno varovanje oz. varovanje za lastne potrebe. V Sloveniji sta za interno varovanje registrirani le dve podjetji, za pogodbeno delovanje pa okoli 150, kar nanese približno 7.000 zasebnih varnostnikov, tehnikov, operaterjev varnostnonadzornega centra, pooblaščenih inženirjev varnostnih sistemov in varnostnih menedžerjev (Dvojmoč idr., 2020). Pri varovanju gospodarskih subjektov se vzpostavi sodelovanje zasebne in korporativne varnosti za učinkovito zagotavljanje varnosti.

8.2 Tehnologija in sistemi za fizično varnost

Fizično varovanje vključuje inženirske naprave v določenem okolju, ki so zasnovane z namenom zmanjšanja groženj z nadziranjem in upravljanjem prostorskega gibanja. Fizično varovanje je usmerjeno na nadzor v okolici objekta in tudi njegovo notranjost ter vsebino. Cilj je tudi oblikovanje okolja in fizičnih ukrepov, s katerimi bi se grožnje in deviantnosti zmanjšale na minimalne (Coole in Brooks, 2021).

Fizična varnost prav tako vključuje funkcijo odvračanja, odkrivanja, zakasnitve in odzivanja. Funkciji odvračanja in odkrivanja vključujeta protiukrepe, kot so na primer postavitev straž, patruljiranje, senzorji gibanja in tudi drugi ukrepi, ki lahko pripomorejo k zaznavi neželenih dejanj. Po tem, ko je varnostni dogodek zaznan, se analizira in poda ocena o potrebnih dodatnih varnostnih ukrepih. Zakasnitev je del funkcije fizične varnosti in vključuje protiukrepe, ki zagotovijo, da mora storilec za izvedbo kaznivega dejanja uporabiti več fizičnih virov. Med protiukrepe spadajo na primer stebrički za preprečitev dostopa za vozila, izboljšani mehanizmi vrat in tudi vsi drugi podobni ukrepi. Med odziv kot funkcijo fizičnega varovanja štejemo protiukrepe, katerih namen je nevtralizacija storilca oziroma njegovega kaznivega dejanja s tem, da se ga ujame oziroma prepreči njegov beg. To se izvaja z varnostniki ali organi kazenskega pregona (Williams, 2019).

Pomembno je, da se fizično varovanje začne že zunaj gospodarskega subjekta, ki je temelj varovanja. Z dobro načrtovanim načrtom varovanja se lahko izognemo številnim nevarnostim in tveganjem. Prva »ovira«, ki jo lahko uporabimo, so ograje, pregrade in zidovi, ki nekako preprečijo vstop nezaželenim osebam, vendar ne v celoti. Naslednja ovira so dvoriščna vrata, ki so najpogosteje del prve ovire, ki smo jo omenili. Naslednja ovira so luči oz. razsvetljava/osvetljava, ki mora biti dobro premišljena, saj lahko prepreči vstop oz. napadalce od vstopa odvrne. Vse tri ovire, ki smo jih omenili, spadajo v prvo fazo varovanja. V drugo fazo, imenovano zunanja in notranja varnost, prištevamo okna, ki bi morala biti dobro zaščitena; vrata, za katera je treba narediti dober načrt glede mesta postavitve; način shranjevanja ključavnic in ključev mora biti dobro premišljen oz. se namesto ključev uporabijo magnetne kartice in podobno; ter strehe in zunanje stene, ki bi morale biti pogosto pregledane. Tretja faza se imenuje notranja varnost. Sem spadajo okna in vrata s samodejnim zapiranjem, z močnimi in težkimi zapahi. Prav tako bi morali biti vsi vstopi nadzorovani. Vzpostavljeno bi moralo biti nadzorovanje in kontroliranje »prometa« v in iz stavbe, ki je varovana. To se lahko izvaja tudi z identifikacijo osebnih ali delovnih izkaznic. Zadnja, četrta faza zajema varnost vsebine, ki je pomembna za organizacijo. Sem spadajo datoteke, sefi in trezorji. Ti morajo biti zelo dobro varovani (Lee Seungmug, 2020).

Varnostno osebje tvori celovit sistem fizičnega varovanja ljudi in premoženja. Osebje na podlagi zakonov in druge zakonodaje s področja zasebnega varovanja in načrtov varovanja na varovanih območjih neposredno izvaja ukrepe varovanja ljudi in premoženja. Posreduje tudi intervencijska služba, na podlagi načrtov alarmiranja in ukrepanja, ter tudi varnostno obhodna služba, ki ugotavlja dejansko stanje na nadzorovanih lokacijah in tudi ukrepa ob ugotovitvah odstopanj (ICS, Institut za korporativne varnostne študije, 2019).

Fizično varovanje je varovanje, ki ga izvajajo za to strokovno usposobljeni delavci – varnostniki (Dvojmoč, 2020). Da lahko varnostniki naloge in ukrepe izvajajo zakonito ter strokovno, morajo imeti določene kompetence. To so predvsem družbena odgovornost, zanesljivost, sposobnost dejavnega poslušanja, sledenje navodilom in prilagodljivost (Dvojmoč, 2016). Ministrstvo za notranje zadeve zagotavlja pogoje, da je varnostno osebje strokovno usposobljeno za opravljanje nalog zasebnega varovanja in tudi: sodeluje pri pripravi poklicnih standardov in katalogov standardov strokovnih znanj in spretnosti v skladu s predpisi, ki urejajo nacionalne poklicne kvalifikacije; določa programe strokovnega usposabljanja, izpopolnjevanja in obdobnega izpopolnjevanja ter skrbi za strokovno izvajanje teh programov; nudi strokovno pomoč pri pripravi in izvajanju izobraževalnih programov; vodi evidence strokovnega usposabljanja in izpopolnjevanja ter imenuje člane komisij za preverjanje strokovne usposobljenosti (Savski idr., 2017).

Pred opravljanjem posameznih vrst dela mora varnostno osebje – varnostnik opraviti strokovno usposabljanje in izpopolnjevanje, poleg tega pa tudi uspešno opraviti preizkus strokovne usposobljenosti. Usposabljanje in izpopolnjevanje je določeno na vseh ravneh in je stopenjsko. Določeni so tudi pogoji, na podlagi katerih je varnostno osebje določeno kot usposobljeno glede na vrsto dela. Prav tako se mora varnostno osebje vsakih pet let od opravljenega osnovnega strokovnega usposabljanja udeležiti obdobnega strokovnega izpopolnjevanja po programih, ki jih določi ministrstvo za notranje zadeve. Delodajalci morajo prav tako redno izvajati interno strokovno izpopolnjevanje, saj so objektivno odgovorni za delo varnostnega osebja (Savski idr., 2017).

Na podlagi usposobljenosti in tudi drugih določb, kot sta polnoletnost in ustrezno državljanstvo, oseba pridobi službeno izkaznico, na podlagi katere lahko opravlja delo. Izkaznico izda Ministrstvo za notranje zadeve, poleg omenjenih pogojev pa so še drugi, določeni z zakoni. Tudi detektiv lahko delo opravlja le v primeru, da ima za to izdano licenco, ki jo izda Detektivska zbornica (Dvojmoč in Sotlar, 2018).

8.3 Načrtovanje in izvajanje varnostnih pregledov

Lahko rečemo tudi, da je fizično varovanje sistem, ki združuje ljudi, varnostne postopke in opremo za zaščito pred zlonamernimi napadi človeka (Zimmerman in Restrepo, 2021). S samo analizo tveganj se lahko klasificirajo prostori na podlagi njihove občutljivosti pred samimi tveganji, s čimer se na podlagi ugotovitev prilagodi načrt fizičnega varovanja (Lincke, 2015). Na podlagi tega se naredi sistem varnostne mreže, ki spodbuja vzpostavitev varnostnega sistema, ki zmanjša ogroženost in negotovost oziroma ju minimalizira glede na dejansko zmogljivost sistema (Lichte idr., 2021).

To imenujemo ocena stopnje tveganja, ki predstavlja stopnjo ogroženosti in temelji na varnostnih potrebah določenega območja, ki je varovano, na predpisih, mogočih posledicah in drugih okoliščinah. Ta ocena predstavlja podlago za izvedbo načrta varovanja, ki je dokument, v katerem so navedeni postopki, način in potek varovanja. Postopek vključuje varnostno osebje, sisteme tehničnega varovanja in ukrepe za zagotovitev varnosti (»ZZasV-1«, 2011).

Odgovorite na vprašanja

Kaj je fizično varovanje? Opredelite s svojimi besedami.

Kako se izvaja fizično varovanje in kaj je glavni cilj tega varovanja?

Kaj vse spada pod fizično varovanje?

Katero področje je v Sloveniji povezano oz. deluje na področju fizičnega varovanja?

Predstavite omenjeno področje in tudi vsa druga področja.

Kaj je ocena stopnje tveganja v fizičnem varovanju?

Kakšna je vloga varnostnega osebja?

Kateri so pogoji za usposabljanje varnostnega osebja in kje je to določeno?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

9 Tehnična varnost

Tako kot fizična varnost je tudi tehnična varnost del pravnega procesa zagotavljanja zasebne varnosti (Dvojmoč, 2020). Nanaša se na vrsto tehnik, ki so uporabljene predvsem za preverjanje pristnosti in zaščito pred krajo občutljivih podatkov v organizacijah. Vsebuje več različnih področij, kamor spadajo na primer kibernetska varnost, varnost IT, upravljanje pristnosti omrežja in podobno.

9.1 Obvladovanje dostopa in varovanje objektov

Tehnično varovanje spada med oblike izvajanja zasebnega varovanja. Podlaga za izvajanje tehničnega varovanja je v »ZZasV-1« (2011), ki v 2. členu pravi: »Zasebno varovanje je varovanje ljudi in premoženja na varovanem območju, določenem objektu ali prostoru pred nezakonitimi dejanji, poškodovanjem ali uničenjem z varnostnim osebjem ter sistemi tehničnega varovanja, ki se opravlja v oblikah, določenih s tem zakonom.«

Opravljanje zasebnega in s tem tudi tehničnega varovanja je določeno v 11. členu »ZZasV-1« (2011). Imetnik licence mora imeti z varnostnim osebjem sklenjeno delovno razmerje. Prav tako mora imeti imetnik licence sklenjeno pogodbo z naročnikom, v njej pa morata biti jasno določena vrsta in obseg varovanja. Varnostno osebje mora imeti ves čas opravljanja delovnih nalog veljavno in vidno službeno izkaznico. Izpolnjevanje pogojev preverja inšpektor inšpektorata ministrstva, pristojnega za notranje zadeve (»ZZasV-1«, 2011). Določeno je tudi, da je treba zasebno varovanje opravljati v skladu s sprejetimi in objavljenimi nacionalimi standardi.

Tehnična varnost se nanaša na vrsto tehnik, ki so uporabljene za preverjanje pristnosti in zaščito pred krajo občutljivih podatkov in informacij v organizacijah. Tehnična varnost vsebuje komponente, kot so kibernetska varnost in preiskave, varnostna arhitektura za programske aplikacije, strategija varnosti IT, upravljanje pristnosti omrežja ter specializirane inženirske rešitve za organizacijsko varnost (Rouse, 2015).

Med standarde tehničnega varovanja gospodarsko-poslovnih objektov spadajo naslednji standardi:

- standardi, ki zmanjšujejo pogoje za kriminalne napade;
- sprejeti standardi s področja vlomnega odkrivanja in javljanja;
- sprejeti standardi s področja požarnega odkrivanja in javljanja ter
- sprejeti standardi s področja mehanskega varovanja (Dvojmoč, 2020).

Za tehnično varnost skrbijo usposobljeni strokovnjaki, ki z uporabo sodobnih alarmnih in videonadzornih sistemov ter sistemov mehanske zaščite zagotavljajo visoko stopnjo varnostnih storitev na tem področju dela (Policija, n. d. a). Pomembno je tudi, da so sistemi za tehnično varovanje redno servisirani in da se redno pregledujejo. V nasprotnem primeru lahko storilci to izkoristijo in jih v pripravljalnem dejanju onesposobijo ali preprečijo njihovo optimalno delovanje, spremenijo kot delovanja kamer in javljalnikov ali onesposobijo sirene in razsvetljavo (Breznik, 2012).

9.2 Tehnologija in sistemi za tehnično varnost

Sistemi tehničnega varovanja so različna tehnična sredstva in mehanske naprave, ki so med seboj povezani. Njihov namen je protivlomno in protiropno varovanje ter tudi nadzor nad vstopnimi in izstopnimi točkami, pregled oseb, prtljage, preprečevanje nasilnih vstopov in podobno. Sem spadajo tudi varnostni alarmi, senzorji, detektorji gibanja, električne in biometrične naprave za kontrolo vstopov in izstopov in podobno.

Med tehnična sredstva spadajo:

- sredstva za preprečevanje: protivlomni sistemi;
- sredstva za nadzorovanje: sistem nadzora gibanja, alarmni sistemi, sistem video nadzora;
- sredstva za prenos alarmnih signalov: sistemi za notranji in zunanji prenos signalov;
- tehnična sredstva v nadzornem centru: sistemi za opozarjanje, za prikazovanje, shranjevanje in obdelavo signalov;

– specialna sredstva: sredstva za komunikacijo, za izvajanje varnostnih nalog, protipožarna sredstva in sredstva za osebno zaščito. (Dvojmoč, 2020)

Sredstva in oprema za tehnično varovanje poslovnega subjekta so lahko mehanski, elektronski in kombinirani (v praksi najpogostejši primer). To so: naravne fizične ovire; mehanske zaščite (različne vrste ograj, klančin, posebnih gradbenih konstrukcij, blagajn, trezorjev in podobno); elektronska zaščita – alarmni sistemi, alarmni centri, senzorji, sirene, magnetni kontakti, alarmno obveščanje; kamere, monitorji in druge komponente sistema CCTV; sistemi za nadzor dostopa in zaznavanje; sistemi za nadzor obiskov objektov; sistemi elektronskih nadzornih sredstev; elektronski sistemi za zaščito pred vohunjenjem in integrirani sistemi zaščite (Duvnjak, 2004).

Celovit sistem tehničnega varovanja tako vključuje varnostnonadzorni center (VNC), centralni nadzorni center (CNS), komunikacijske povezave za prenos alarmnih sporočil, sisteme tehničnega varovanja, sisteme za zagotavljanje neprekinjenega poslovanja, redno vzdrževanje in servisiranje, varnostno dokumentacijo, navodila za rokovanje in vzdrževanje, alarmno odzivni sistem in podobno. Pomemben del tehničnega varovanja so sistemi mehanske zaščite, kot so varnostne rešetke, varnostne folije za vrata, varnostna stekla, varnostna vrata, varnostne ključavnice in podobno (ICS, Institut za korporativne varnostne študije, 2019).

Za sisteme tehničnega varovanja po zakonu se štejejo tudi drugi sistemi, ki so neločljivo povezani s sistemi tehničnega varovanja po omenjenem zakonu. Poseg v te sisteme bi pomenil poseg v sisteme tehničnega varovanja po tem zakonu (varstvo pred požarom, javljanje eksplozivnih in drugih plinov, socialni alarmi, sistemi za detekcijsko merjenje eksplozivnih in strupenih snovi, plinov in par, varnostne blagajne, varnostna vrata, ključavnice, trezorji in sefi). Med sisteme tehničnega varovanja pa ne štejejo naprav za nadzor nad zalogami in inventuro ter drugih naprav in sistemov, ki niso namenjeni za varovanje v skladu s tem zakonom (»ZZasV-1«, 2011).

Sistemi tehničnega varovanja se po svoji funkcionalnosti delijo na šest večjih skupin, in sicer so to sistemi protivlomnega varovanja, protipožarnega varovanja, video nadzora, pristopne kontrole, mehanske zaščite ter za detekcijo merjenja eksplozivnih plinov in drugi tehnični alarmi (Fefer, 2013).

9.3 Načrtovanje in izvajanje varnostnih pregledov

Načrtovanje sistemov tehničnega varovanja zajema izdelavo projektov tehnične dokumentacije za samo izvedbo sistemov tehničnega varovanja s pooblaščenimi inženirji varnostnih sistemov, kar mora biti v skladu z ZZasV-1 in zakoni, ki urejajo gradnjo objektov (Ministrstvo za digitalno preobrazbo, 2023).

Odgovorite na vprašanja

Kaj za vas predstavlja tehnična varnost? Opredelite.

Katere komponente vsebuje tehnična varnost?

Kateri standardi spadajo med standarde tehničnega varovanja gospodarsko-poslovnih objektov?

Kaj vse spada pod tehnično varovanje? Naštejte.

Kaj zajema načrtovanje sistemov tehničnega varovanja?

Kdo skrbi za tehnično varnost?

Katera sredstva in opremo za tehnično varovanje poznamo?

Kaj predstavlja celotni sistem tehničnega varovanja?

Kako se delijo sistemi tehničnega varovanja?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

10 Informacijska varnost

Informacijska varnost predstavlja enega izmed šestih pravnih procesov zagotavljanja korporativne varnosti. S pripravo in sprejemom ustreznih notranjih aktov in spremljanjem ter nadzorom nad izvajanjem navedenih pravil se zagotavljata informacijska varnost in zaščita tehnologij (Dvojmoč, 2020). Informacijska varnost je definirana kot stanje zaupnosti, popolnosti in dostopnosti informacij, ne glede na obliko, v kateri obstajajo. To stanje dosegamo z uporabo ustreznih informacijskovarnostnih ukrepov in standardov ter organizacijsko podporo za načrtovanje, izvajanje, preverjanje in izpopolnjevanje teh ukrepov in standardov (Ivandić Vidović idr., 2011).

10.1 Varnost informacijskih sistemov

Prislan in Bernik (2019) definirata informacijsko varnost kot varovanje informacij ne glede na njihovo obliko. Poznavanje informacijske varnosti je zelo pomembno za organizacije, saj lahko nepoznavanje le-te ogrozi njeno delovanje in jo s tem naredi manj učinkovito (Rashid idr., 2013).

Informacijska varnost pomeni varovanje podatkov informacijskih sistemov pred nezakonitimi dostopi, uporabo, razkritjem, spremembami ali uničenjem (Urad Republike Slovenije za intelektualno lastnino, 2024). Skrbi za zaupnost, razpoložljivost in celovitost informacij ter tudi nadzoruje skupno rabo teh informacij in preprečuje informacijska tveganja (Ashenden, 2008). Prav tako predstavlja ravnovesje med samimi tveganji in nadzorom nad le-temi (Anderson, 2003). Informacijski sistem je opredeljen kot skupek

strojne in programske opreme, podatkov, postopkov ter ljudi (Dobrovoljc, 2018). Dobro zasnovan sistem informacijske varnosti je ključnega pomena za preprečevanje nevarnosti in ranljivosti (Rakar, 2006). Zanimiva in pomembna je tudi ugotovitev, da je problematika zagotavljanja informacijske varnosti v večji meri vezana na ljudi in v manjši na tehnologijo, kar opozarja na pomembnost ukrepov kadrovske varnosti (Belič in Lesjak, 2006).

Pri informacijski varnosti je zelo pomembna učinkovita politika informacijske varnosti, ki je dokument, ki usmerja potek informacijske varnosti v organizaciji. Prav tako mora biti politika informacijske varnosti usklajena z vizijo in poslanstvom organizacije. Politika je učinkovita v primeru, ko organizaciji pomaga doseči varnostne cilje (Höne in Eloff, 2002).

Je ključna za ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij ter tudi za zaščito pred različnimi tveganji. Za učinkovito izvajanje zasebnosti, zaupnosti in razpoložljivosti je potrebno poznavanje konceptov avtentikacije, ki je postopek, s katerim strežnik preveri istovetnost entitete; avtorizacije, ki pomeni določanje pravic dostopa do virov; odgovornosti, ki je sledljiva povezava med pošiljateljem in prejemnikom s sredstvi, kot so digitalni podpis ali različna potrdila (Graham idr., 2011).

Če želimo zagotoviti zaupnost informacij, je te treba zaščititi pred nepooblaščenim razkritjem tistih, ki za dostop do njih niso pooblaščeni. Dostop imajo le pooblaščeni uporabniki. Celovitost pomeni zaščito informacij pred kibernetskimi kriminalci ali različnimi motnjami med prenosom ali sprejemom. Informacije so zaščitene takrat, ko jih ni mogoče spreminjati, ne da bi sistem to zaznal. Razpoložljivost pa zagotavlja, da pretok informacij poteka nemoteno in so te vedno na voljo pooblaščenim uporabnikom (Farooq idr., 2015).

Učinkovita informacijska varnost se zagotavlja tudi z notranjim organizacijskim ozadjem, ki vključuje skupne vrednote in prepričanja o varnosti na vseh ravneh delovanja organizacije. Te morajo sprejeti tudi celostno strategijo, ki združuje vidike informacijske varnosti, organizacijske kulture ter notranje človeške dejavnosti in odnose (Chang in Lin, 2017).

Organizacije morajo izvajati določene naloge za zagotavljanje nenehne informacijske varnosti, kot so analiza trenutnega stanja, analiza groženj, predlogi za takojšnje ukrepanje, analiza tveganja in glede na to sprejemanje odločitev o tveganjih ter na podlagi vseh omenjenih postopkov skrbeti za zagotavljanje čim boljše varnosti (Dombora, 2016).

Za zagotavljanje informacijske varnosti je izredno pomembno tudi usposabljanje in izobraževanje zaposlenih o morebitnih tveganjih, odgovornostih in informiranje o varnosti. Z usposabljanjem so vsi zaposleni seznanjeni z morebitnimi tveganji za IT sisteme in tudi z ukrepi, ki jih lahko sprejmejo. K usposabljanju spadajo področja, kot so varnost gesel, prepoznava lažnih sporočil, pomen varovanja občutljivih podatkov ter fizična varnost strežnikov in opreme ter podobno. Z rednim usposabljanjem zaposleni vedo, kako se pred določenimi tveganji zaščititi, kar prispeva k preprečevanju varnostnih incidentov in zaščiti sredstev ter informacij (Arain idr., 2019).

10.2 Zaščita podatkov in osebnih informacij

Razpoložljivost pomeni, da ima organizacija vedno na voljo podatke, ki jih potrebuje. Če se podatki izgubijo, to lahko pomeni tudi prenehanje delovanja nekaterih poslovnih procesov, zato je pomembno, da ima organizacija vzpostavljen vzporedni sistem, ki se aktivira, če se glavni sistem ustavi oziroma preneha delovati. Zaupnost pomeni oziroma zagotavlja, da podatki ne pridejo do nepooblaščenih oseb. To pomeni, da zaupnost zagotavlja, da imajo le pooblaščene osebe dostop do določenih podatkov. Celovitost pomeni, da so podatki celotni, nepoškodovani in točni. To se lahko prepreči preko namernega ali nenamernega vnosa, zaradi česar je zelo pomembno, da se dostop do podatkov zagotovi le pooblaščenim osebam, ki do podatkov oziroma informacij dostopajo le preko operacijskega sistema z uporabniškim imenom in geslom ter informacijskega sistema (Lapuh Bele, 2021).

Podatki oziroma informacije so zaščitene tudi z zakoni. Tu gre predvsem za informacije, ki se navezujejo na določenega posameznika, kot so na primer ime, identifikacijska številka, spletni kazalnik, podatki o lokaciji in podobno (»Uredba (EU) 2016/679«, 2016). Vsaka obdelava osebnih podatkov oziroma informacij mora biti zakonita in obdelana na pošten in pregleden način. Obdelava je zakonita, ko:

- je podano soglasje posameznika, na katerega se podatki nanašajo;
- so podatki oziroma njihova obdelava potrebni za izvajanje pogodbe oziroma prvih korakov pred njeno sklenitvijo;
- je to potrebno za izpolnitev zakonske obveznosti upravljavca;
- je to potrebno za varnost posameznika in njegovih življenjskih interesov;
- je obdelava osebnih podatkov potrebna za opravljanje naloge v javnem interesu;
- je to potrebno za zakonite interese, za katere si prizadeva upravljavec. (»Uredba (EU) 2016/679«, 2016)

V Sloveniji je varstvo osebnih podatkov določeno z Zakonom o varstvu osebnih podatkov (»ZVOP-2«, 2022), katerega glavni cilj je ravno zaščita informacijske zasebnosti in varnosti posameznikov. Ureditve zakona so usklajene z Ustavo Republike Slovenije (»Ustava Republike Slovenije (URS)«, 1991), pri tem pa je prišlo tudi do nekaterih sprememb v primerjavi s predhodnim zakonom na tem področju. Poleg ZVOP-2 je treba upoštevati tudi Splošno evropsko uredbo o varstvu osebnih podatkov (GDPR), ki je v veljavi vse od leta 2018 in je obvezna za vse organizacije, podjetja, ustanove ter druge subjekte in objekte, ki uporabljajo in kakor koli obdelujejo osebne podatke državljanov Evropske unije. Uredba je pomembna predvsem zaradi krepitve varstva osebnih podatkov državljanov EU in določanjem obveznosti podjetij in organizacij, ki te podatke obdelujejo (Infocenter, n. d. c).

Tajni podatki, ki se vežejo na javno varnost, zunanje zadeve, obveščevalno dejavnost, obrambo in varnostno dejavnost države, prav tako predstavljajo občutljivo skupino podatkov, ki jih je na podlagi razlogov, določenih v Zakonu o tajnih podatkih (»ZTP«, 2001) potrebno zavarovati pred nepooblaščenimi osebami. Tajne podatke delimo na interne zaupne, tajne in strogo tajne. Da se njihovo razkritje prepreči, je potreben dobro razvit informacijski sistem, ki v povezavi z varnostnimi ukrepi ščiti sistem oz. poskrbi za to, da v primeru ranljivosti enega dela sistema ne postane ranljiv celotni sistem. Z ukrepi se zmanjša verjetnost, da bi do varnostnega incidenta sploh prišlo, poleg tega pa se zmanjšajo negativne posledice incidenta, če do tega pride (Hunter, 2001).

10.3 Notranji akti

Samo področje informacijske varnosti je urejeno v »Zakonu o informacijski varnosti (ZInfV)« (2018), ki le-to opredeljuje kot: »Informacijska varnost je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti.«

V Sloveniji so postopki, ukrepi, človekove pravice, zakonitosti, načela, skladnosti, upravičenosti, zasebnosti, tajnost in drugi standardi, ki so povezani z osebnimi podatki, urejeni z »ZVOP-2« (2022). Ta ureja tudi uresničevanje pravil, ki urejajo prosti pretok osebnih podatkov za izvajanje uredbe GDPR (»ZVOP-2«, 2022).

Osnovni cilji standarda BS 7799 je zagotavljanje že prej omenjene zaupnosti, celovitosti in razpoložljivosti informacij. Koristi standarda so celovito pokrivanje področja zagotavljanja informacijske varnosti; neprestano izboljševanje ravni informacijske varnosti

na podlagi nepristranskega merjenja; zmanjševanje verjetnosti za uresničitev groženj varnosti in/ali ublažitev posledic, ki jih te lahko povzročijo; povečanje ugleda organizacije, zaupanja poslovnih partnerjev in strank; povečanje konkurenčnosti ter pripravljenost na prihodnje zahteve zakonodajalca ali poslovnih partnerjev (Dvojmoč, 2020).

10.4 Preprečevanje kibernetskih napadov

Razumeti je treba tudi kibernetsko varnost, ki jo Prislan (2016) opredeljuje kot podpomenko informacijske varnosti, saj slednja zajema najširše področje varnosti in širok nabor dejavnosti za premagovanje informacijskih groženj, ki pretijo informacijskim sistemom.

Na področju kibernetske varnosti lahko definiramo tri vrste groženj, in sicer kibernetsko kriminaliteto, kibernetske napade in kibernetski terorizem (Kaspersky, 2022). Za boj proti kibernetskim grožnjam so bila razvita priporočila, med katera sodijo tudi naslednja:

- Države morajo med seboj sodelovati in se združiti ter oblikovati skupne programe predvsem zato, ker so to grožnje globalne narave.
- Zakone je treba posodabljati in jih tudi izvajati. Za to je potreben tudi usposobljen kader in sredstva za njihovo izvajanje.
- Vsi kibernetski napadi morajo biti prijavljeni kriminalistom, saj to pripomore k boljšemu razumevanju problema.
- Kibernetski napadi vplivajo na uporabnike tehnologije, zato je treba upoštevati tudi njihove potrebe pri obravnavi groženj. (Gupta in Agarwal, 2017)

K večji varnosti poslovnega okolja pripomorejo izobraževanje zaposlenih, posodobljena programska oprema, uporaba oblaka ali lastnih strežnikov in kopiranje podatkov (Datalab, 2022).

Preprečevanje kibernetskih napadov zajema vse od tehnične zasnove komponent informacijskih sistemov do zagotavljanja nacionalnih in mednarodnih zakonskih okvirov ter predpisov. Ti pripomorejo k razvoju varnejših aplikacij in infrastrukture.

Izobraževanje zaposlenih je pomembno, saj se skrb za informacijsko varnost začne in konča pri zaposlenih. Ti morajo imeti na računalnikih nameščen protivirusni program in tudi uporabljati močna gesla, ki jih ne delijo z drugimi. Nevarno je tudi povezovanje na javne točke Wi-Fi, odpiranje neznanih strani in prenašanje sumljivih datotek.

Zelo pomembno je tudi, da je programska oprema vedno posodobljena, saj se s tem zagotovi zaščita podatkov. To ne velja le za posodabljanje operacijskih sistemov, ampak tudi za posodabljanje poslovnih programov (Datalab, 2022).

Zaupanja vredni ponudniki oblačnih storitev ponujajo boljšo raven informacijske varnosti, kot si jo lahko zagotovi organizacija sama. Pomembno je, da so podatkovni centri, kjer so podatki shranjeni, ustrezno varnostno potrjeni, uporabljajo najsodobnejše požarne zidove in do podatkovnih strežnikov lahko dostopa le pooblaščeno osebje. S tem se zagotovita ustrezna varnost in diskretnost.

Zadnji ukrep, ki lahko pripomore k preprečevanju kibernetskih napadov, je tudi varnostno kopiranje podatkov. Z rednim arhiviranjem in izdelovanjem varnostnih kopij preprečimo izgubo podatkov, ki so za organizacije zelo pomembni (Datalab, 2022).

Poleg zgoraj omenjenih ukrepov lahko omenimo še požarni zid, ki se uporablja za zaščito varnejšega omrežja pred manj varnim. Predvsem se požarni zidovi uporabljajo za zaščito notranjega/zasebnega omrežja pred zunanjim (internetom). Požarni zidovi preprečujejo nepooblaščen dostop do občutljivih podatkov, prav tako pa pomagajo preprečevati širjenje zlonamerne programske opreme (Liu in Gouda, 2008). Poleg požarnega zidu poznamo tudi šifriranje podatkov, ki je postopek pretvarjanja podatkov v šifrirano besedilo z namenom, da jih nepooblaščeni uporabniki ne morejo prebrati (Kaspersky, 2022).

Kot ukrep za preprečevanje kibernetskih napadov se uporablja tudi biometrija, ki je statistično in matematično merjenje edinstvenih fizičnih ali bioloških značilnosti za namene identifikacije. Opredelitev biometrije se nanaša na uporabo edinstvenih bioloških značilnosti za digitalno preverjanje pristnosti in nadzor dostopa. Organizacije morajo pri tem zagotoviti zbiranje, hranjenje in obdelavo podatkov v skladu z ustreznimi zakoni in drugimi predpisi (Molinaro, 2022).

Tudi antivirusni program se uporablja kot sredstvo za preprečevanje kibernetskih napadov. Je programska aplikacija, ki je namenjena odkrivanju, preprečevanju in odstranjevanju zlonamerne programske opreme iz računalniškega sistema. Običajno podatke pregleduje računalniški sistem v realnem času ali po rednem urniku in išče sumljivo vedenje (National Cyber Security Centre, 2021).

Na področju informacijske varnosti in s tem tudi kibernetske varnosti je pomembno tudi upravljanje gesel. Nanaša se na možnost upravljanja gesel za celotno organizacijo. A samo močna gesla niso dovolj za preprečevanje kršitev varnosti podatkov, saj so kibernetski napadi vse bolj izpopolnjeni (Kinzer, 2022).

Odgovorite na vprašanja

Kaj je informacijska varnost?

Zakaj je informacijska varnost pomembna?

Kaj vsebuje sistem informacijske varnosti in za kaj skrbi?

Kaj si predstavljate pod pojmom politika informacijske varnosti? Pojasnite.

Na katere načine se zaščitijo podatki in informacije v organizaciji?

Na kateri način organizacije zagotavljajo nenehno informacijsko varnost?

Kako je v Sloveniji poskrbljeno za varstvo osebnih podatkov?

Kaj pomenijo pojmi razpoložljivost, zaupnost in celovitost? Pojasnite s svojimi besedami.

Kaj je standard BS 7799?

Kako je opredeljena kibernetska varnost?

Kaj so kibernetski napadi in kako jih preprečimo?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

11 Zagotavljanje »know-howa« in zaščita stvarnopravnih pravic in pravic intelektualne lastnine

Zagotavljanje varnostnega »know-howa«, specifičnega za organizacije, in zaščita stvarnopravnih pravic ter pravic intelektualne lastnine sta dva pravna procesa korporativne varnosti (Dvojmoč, 2020).

11.1 Zagotavljanje varnostnega »know-howa«, specifičnega za organizacije

Pri sami implementaciji in zagotavljanju »know-howa« je poudarek predvsem na preiskovanju in odkrivanju protipravnih ali deviantnih ravnanj v organizacijah, pri čemer si lahko pomagamo z vzpostavitvijo obveščevalne – OSINT (Open source intelligence) in protiobveščevalne oz. kontraobveščevalne dejavnosti. Zraven spada tudi preiskovanje in odkrivanje preslepitev in prevar v škodo organizacije (Dvojmoč, 2020).

Korporativno obveščanje predstavlja orodje povečanega ozaveščanja sodobnih organizacij, ki želijo poslovati varno, predvsem z vidika globalnega poslovanja, ob upoštevanju tveganj na trgu in tudi priložnosti lastnega konkurenčnega razvoja. Samo zavedanje o nujnosti korporativne varnosti v sodobnem globalnem poslovanju kot orodje za obvladovanje izzivov in nadgradnjo poslovanja z vidika konkurenčnosti in varnosti na trgu predstavlja neizogiben korak h konkurenčnemu in varnemu poslovanju, z zavedanjem

vseh vrst tveganj in poznavanjem značilnosti trga. Razvoj tradicionalnih obveščevalnih služb gre v smeri »privatizacije« obveščevalnih služb, s ciljem oblikovanja in razvoja nove discipline, tj. ekonomskega preiskovanja ali konkurenčnega obveščanja, ki se lahko uporablja v drugem (korporacijskem ali poslovnem) svetu (Dvojmoč, 2019).

Zbiranje podatkov kot enega izmed temeljnih elementov obveščevalne dejavnosti lahko kategoriziramo po različnih obveščevalnih disciplinah, med katerimi je tudi zbiranje iz javno dostopnih virov v obliki odprtokodnih obveščevalnih podatkov (OSINT) (Dvojmoč, 2019). Britovšek idr. (2017) izpostavljajo, da je OSINT ključnega pomena pri zbiranju in analizi podatkov v zasebnem sektorju, kjer so zasebniki omejeni predvsem na odprtokodno zbiranje.

OSINT je izraz, ki sega več kot 70 let nazaj in se je v primerjavi s svojimi začetki, predvsem glede načina pridobivanja informacij, zaradi tehnološkega napredka konkretno spremenil. Najbolj poznana definicija OSINT je, da so to obveščevalni podatki, ki so izdelani iz javno dostopnih informacij, ki se zbirajo, izkoriščajo in pravočano razširjajo ustreznemu občinstvu z namenom obravnavanja posebne obveščevalne zahteve. Schaurer in Störger (2013) sta koncept nekoliko razširila na zbiranje, obdelavo, analizo, proizvodnjo, klasifikacijo in širjenje informacij, pridobljenih iz virov in s sredstvi, ki so javno in zakonito dostopni ter tudi uporabni za javnost kot odziv na uradne zahteve nacionalne varnosti.

Odprti viri podatkov so odlični za pridobivanje večine informacij, ki jih v našem primeru potrebuje organizacija (Primc, 2021). Konkurenčno obveščanje je proces in v prihodnost usmerjena praksa, ki se uporablja za ustvarjanje znanja o konkurenčnem okolju za izboljšanje organizacijske uspešnosti ter vključuje sistematično zbiranje in analizo informacij iz več virov (Madureira idr., 2021). Skozi desetletja se je področje zbiranja podatkov iz javno dostopnih virov spreminjalo in prilagajalo spremembam, najbolj izrazito pa se to kaže predvsem v zadnjem desetletju, v obdobju pospešene digitalizacije. Področje OSINT je danes usmerjeno predvsem v digitalne medije (Primc, 2021). Javno dostopne informacije se zbirajo predvsem preko spletnih strani, socialnih omrežij, člankov, javnih evidenc, slik, medijev in podobno. Cilj je primerjava teh informacij in njihova analiza, ki ustvari celotno sliko dogodkov, organizacij, posameznikov in potencialnih tveganj. OSINT s svojim zbiranjem podatkov ne posega v posameznikovo zasebnost (Gill, 2023).

OSINT poteka v tako imenovanem obveščevalnem ciklusu, ki je sestavljen iz petih korakov, in sicer iz načrtovanja, zbiranja podatkov, procesiranja podatkov, analiziranja ter diseminacije (Gill, 2023). Omenjata se tudi dva pristopa uporabe pridobivanja podatkov

iz javno dostopnih virov, in sicer ofenzivni in defenzivni pristop. Prvi pristop je umeščen v okvir konkurenčnega obveščanja, torej pridobivanja informacij o konkurentih, drugi pristop pa je veliko bolj izrazit in služi pridobivanju informacij iz javnih virov za pravočasen odziv na kibernetske in druge grožnje, kar organizacijam omogoča predvsem konkurenčno prednost. Pridobivanje javno dostopnih podatkov ima lahko velike koristi za organizacijo, po drugi strani pa je to področje še v zelo zgodnji fazi razvoja in vprašanje je, ali lahko razvoj novih tehnologij dohiteva z vidika učinkovite uporabe orodij in modeli za zbiranje javnih podatkov (Primc, 2021).

Protiobveščevalna dejavnost je pomemben dejavnik za zagotavljanje varnosti. Njene naloge so predvsem ugotavljanje, nadzorovanje, raziskovanje in preiskovanje kaznivih dejanj organizacije in posameznikov (Šaponja, 1999). Pomembni elementi protiobveščevalne dejavnosti so: prepoznavanje, iskanje, preprečevanje in manipulacija delovanja sovražnikov, tujih obveščevalnih služb, organizacij ali posameznikov; varovanje in zaščita države pred obveščevalnimi dejavnostmi sovražnikov (Hribar idr., 2012).

Cilji protiobveščevalne dejavnosti so:

- odkriti nasprotnika tuje obveščevalne službe in ga prisiliti v sodelovanje s protiobveščevalno službo z namenom, da se prodre v tuje obveščevalne službe in si s tem zagotoviti vir podatkov;
- izvajanje varnostnih ukrepov na področju nadzora svojih zaposlenih oz. svojega osebja, sil in podjetij ter tudi tujega osebja obveščevalnih služb;
- tehnični, fizični in organizacijski varnostni ukrepi. (Hribar idr., 2012)

Razlika med obveščevalnimi in protiobveščevalnimi službami je v uporabi različnih metod in sredstev za delo ter tudi po vlogi in funkciji, ki jo ima tako ena kot druga v varnostnem sistemu (Anžič, 1997). Prav tako protiobveščevalno dejavnost delimo na ofenzivno in defenzivno, in sicer se ofenzivna neposredno spopada s tujimi obveščevalnimi službami doma ali v tujini, defenzivna pa obsega varnostne ukrepe, kot so organizacijski, fizični, tehnični, ter tudi varnostno preverjanje ljudi in podjetij (Črnčec, 2009).

Korporativna varnost vključuje tudi odkrivanje goljufij in drugih kriminalnih dejavnosti. Ko varnostno podjetje odkrije goljufijo ali drugo obliko kaznivega dejanja, mora o tem nemudoma obvestiti policijo, ki nato zadevo preganja. V okviru korporativne varnosti morajo organizacije razviti preventivne ukrepe za odpravo vseh tveganj, zmanjšati nevarnosti na najnižjo možno raven, razviti operativni načrt za krizne situacije, povečati

konkurenčnost in produktivnost, izboljšati tehnologijo in ukrepati, ko pride do varnostnih groženj (Kubale idr., 2023).

11.2 Zaščita stvarnopravnih pravic in pravic intelektualne lastnine sta dva pravna procesa korporativne varnosti

Pravna zaščita stvarnopravnih pravic in pravic intelektualne lastnine zajema predvsem varovanje in zaščito določenih patentov, predvsem pa blagovnih znamk, modelov in podobno, saj je nujno, da v različnih kriznih situacijah delujejo brezhibno in niso izpostavljeni fizičnim ali virtualnim grožnjam. Zraven spadata tudi pravno varovanje lastninske pravice in pravna zaščita materialnih avtorskih pravic organizacije (Dvojmoč, 2020).

V Sloveniji temeljna načela stvarnega prava, posesti in stvarnih pravic ter načine njihove pridobitve, prenosa, varstva in prenehanja ureja »Stvarnopravni zakonik (SPZ)« (2003). Stvarne pravice so:

- lastninska pravica,
- zastavna pravica,
- pravica služnosti,
- pravica stvarnega bremena,
- stavbna pravica. (»SPZ«, 2003)

»Lastninska pravica je pravica imeti stvar v posesti, jo uporabljati in uživati na najobsežnejši način ter z njo razpolagati. Omejitve uporabe, uživanja in razpolaganja lahko določi samo zakon.« (»SPZ«, 2003)

Intelektualna lastnina se nanaša na vrsto lastnine, ki izvira iz človekovega intelekta oz. razuma. Med te pravice spadajo patenti, dodatni varstveni certifikati, modeli, znamke, avtorska in sorodne pravice in podobno. Pravica intelektualne lastnine je izključena, vendar je ta pogojena z naravo predmeta varovane pravice, ki temelji na treh načelih, in sicer:

- imetnik pravice lahkko prepove komercialno izkoriščanje predmeta;
- varstvo pravic se nanaša na gospodarsko dejavnost;
- pravice so ozemeljsko in praviloma časovno omejene, razen blagovnih znamk, trgovskih imen in podobno (Sektor za varnost in zdravje pri delu, 2020).

Področje pravne zaščite materialnih avtorskih pravic pa je podrobneje opredeljeno v »Zakonu o avtorskih in sorodnih pravicah (ZASP)« (1995).

Odgovorite na vprašanja

Kaj vključuje proces zagotavljanja varnostnega »know-howa«?

Kaj je OSINT? Pojasnite.

Zakaj je OSINT pomemben za organizacijo oz. na kakšen način?

Kje poteka OSINT in katere korake vključuje?

Katera dva pristopa uporabe pridobivanja podatkov poznamo? Pojasnite ju.

Kako razumete protiobveščevalno dejavnost?

Kateri so cilji protiobveščevalne dejavnosti?

Kakšne so razlike med obveščevalnimi in protiobveščevalnimi službami? Pojasnite.

Kako organizacija postopa ob odkritju kaznivih dejanj?

Pojasnite proces zaščite stvarnopravnih pravic in pravic intelektualne lastnine s svojimi besedami.

Kaj v Sloveniji ureja »Stvarnopravni zakonik (SPZ)« (2003)?

Kaj je lastninska pravica? Pojasnite s svojimi besedami.

Kaj je intelektualna lastnina?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

12 Finančna varnost

Pri korporativni varnosti je pomembna tudi finančna varnost, saj lahko tveganja in grožnje vplivajo tudi na finančno poslovanje in stanje organizacije, kar bi lahko pomenilo velike finančne izgube, izgubo finančnih podatkov strank in tudi moteno delovanje celotne organizacije.

12.1 Preprečevanje finančnih prevar

Prevara je v širšem smislu opredeljena kot neko dejanje z namenom zavajanja drugih z neupravičenim navajanjem ali pripisovanjem dosežkov. V ožjem pomenu je definirana kot namerna goljufija zavajanja posameznika ali organizacije z namenom pridobitve neupravičene prednosti ali povzročitve škode drugi osebi ali subjektu (Sood in Bhushan, 2020).

Kakšna je trenutna strategija za preprečevanje goljufij? Katere so visoko tvegane transakcije organizacije? Izvesti je treba tudi oceno tveganja, s pomočjo katere se odkrijejo morebitne šibke točke varnosti. Ocena tveganja mora vključevati tudi pregled varnosti pri določenih transakcijah kot tudi pri novih vlogah za račune. Preprečevanje goljufij oz. prevar je edini način za zmago.

Spodaj je določenih 17 načinov, s katerimi lahko organizacija poveča varnost spletnega bančništva in prepreči goljufije:

- Pozorni moramo biti na tradicionalne prevare, kar pomeni, da s pojavom novih načinov goljufij in prevar to še ne pomeni, da starih ni več.
- Stranke in zaposlene je treba poučiti o napadih z lažnim predstavljanjem in socialnim inženiringom, saj le-ti še vedno predstavljajo velik problem. Ljudje morajo biti ves čas previdni, pri čemer je izobraževanje velik dejavnik pri samem ozaveščanju in preprečevanju goljufij in prevar.
- V svoj spletni bančni sistem je treba vključiti sistem za spremljanje goljufij, kar pomeni, da je priporočljiva uporaba sofisticirane programske opreme, ki spremlja transakcije.
- Dnevni ročni pregledi revizijske sledi in poročil so zelo pomembni, saj se prevarantom oziroma goljufom že na začetku prepreči dostop do računov.
- Stranke je treba opozoriti, ko pride do sumljive dejavnosti.
- Dobro je nastaviti pravila in omejitve po meri, s čimer se še dodatno zavarujejo računi.
- Uporaba daljših gesel, ki so bolj zapletena ali lažje zapomljiva, saj je to učinkoviteje kot njihovo pogosto spreminjanje.
- Zahtevanje dvostopenjske avtentikacije in izzivnih vprašanj ob prijavi ter za določene transakcije, kar otežuje goljufije in prevare. Uporaba je priporočljiva pri transakcijah z visokim tveganjem.
- Posodabljanje sistemov je izredno pomembno, saj novejše različice vsebujejo popravke, ki izboljšujejo ranljivost prejšnjih različic.
- Uporaba protivirusne in zlonamerne zaščite je prav tako zelo priporočljivo, saj lahko nekdo od zaposlenih nevede nasede goljufiji in s tem v organizacijo prinese okuženo kodo.
- Paziti se je treba notranjih goljufij, saj včasih napadi pridejo tudi iz organizacij samih oz. s strani zaposlenih. Priporočljivo je tudi spremljanje vedenja zaposlenih na delovnem mestu.
- Preizkusi prodora so priporočljivi pri zaznavi samih ranljivosti.
- Uporabljanje preverjanja pristnosti ReCAPTCHA, s čimer se prepreči »polnjenje poverilnic« s strani botov, kar predstavlja vse večjo težavo.
- Shranjevanje vseh zasebnih podatkov v varnem omrežju, s pomočjo požarnih zidov in drugih varnostnih ukrepov, ki akterjem preprečuje dostop do informacij.
- Uporabljanje javnega omrežja Wi-Fi je lahko zelo nevarno, saj osebe zlahka pridejo do informacij, ki se delijo preko nešifriranega omrežja. (De Visser, 2022)

Ključni dejavnik pri preprečevanju poslovnih goljufij oziroma prevar je na primer poznavanje zaposlenih. Storilci goljufij pogosto kažejo vedenjske lastnosti, ki bi lahko kazale na namero goljufanja. Zato je predvsem za vodstvo pomembno, da sodeluje s svojimi zaposlenimi in si vzame čas, da jih tudi spozna. Vsaka sprememba odnosa lahko nakazuje na težave zaposlenega. Spremljanje sprememb in odnosa zaposlenih ni priporočljivo le zaradi odkrivanja goljufij, ampak tudi zaradi celotnega delovanja in poslovanja organizacije, saj organizacija posluje bolje, ko predstavlja mesto, na katerem so zaposleni zadovoljni. Pomembna je tudi ozaveščenost zaposlenih o politiki delovanja, tveganjih, ki jih goljufije lahko prinesejo in vrstami goljufij ter vsemi mogočimi posledicami. Na ta način bodo posamezniki, ki nameravajo zagrešiti goljufijo, obveščeni, da so opazovani, kar jih bo mogoče odvrnilo od samega dejanja. Izvajati je treba tudi notranje kontrole, ki so načrti in/ali programi, ki se izvajajo za varovanje sredstev organizacije in zagotavljajo celovitost evidenc. Prav tako je ločevanje nalog pomemben sestavni del notranjega nadzora, ki zmanjšuje tveganje goljufije (CG Team, 2023).

Zelo pomembna je tudi dokumentacija, ki lahko prav tako pripomore k zmanjšanju števila goljufij. Same programe notranjega nadzora je treba dosledno spremljati in pregledovati, saj se s tem zagotovi njihova učinkovitost. Pri samem nadzoru nad goljufijami lahko najamete tudi strokovnjake z različnih področij, ki imajo pomembne vloge pri oblikovanju politik in postopkov v boju proti goljufijam. Pri njihovem zaposlovanju je potrebno biti izredno previden in pozoren, saj niso vsi strokovnjaki izkušeni in mogoče ne ustrezajo potrebam organizacije. Tudi pozitivno delovno okolje prinaša manj goljufij in kraj zaposlenih. V organizaciji morajo obstajati jasna organizacijska struktura, pisne politike in postopki ter poštena praksa zaposlovanja (CG Team, 2023).

Predvsem pa je pomembno, da so vsi zaposleni seznanjeni z različnimi vrstami prevar, kar pomeni, da se o tem tudi redno opozarja. Biti morajo previdni pri svojem delu in vedeti tudi, kako se določenim prevaram in goljufijam izogniti (Policija, n. d. b).

12.2 Obvladovanje tveganj v poslovnih transakcijah

Kaj sploh je transakcijsko tveganje? To je izpostavljenost dejavnikom negotovosti, ki lahko vplivajo na pričakovani donos posla ali transakcije. Vključuje lahko valutno tveganje, blagovno in časovno tveganje. V bistvu zajema vse negativne dogodke, ki lahko preprečijo sklenitev posla. Posel z visokim transakcijskim tveganjem bo običajno zahteval višji pričakovani donos, zato je pomembno upoštevati takšno tveganje pri ocenjevanju prihodnje naložbe. V nekaterih primerih lahko transakcijsko tveganje prepreči izvedbo posla zaradi morebitnih negativnih rezultatov, povezanih s transakcijo (CFI Team, 2023).

Nekatera najpogostejša transakcijska tveganja, ki lahko vplivajo na posel ali vrednost transakcije, vključujejo naslednje:

- Valutno tveganje, ki je nepredvideno nihanje deviznega tečaja, ki lahko vpliva na pričakovano vrednost posla.
- Blagovno tveganje, ki obravnava nepričakovana nihanja cen blaga.
- Obrestno tveganje preučuje, kako lahko nihanje obrestnih mer vpliva na vrednost transakcije.
- Časovno tveganje.
- Tveganje nasprotne stranke. (CFI Team, 2023)

Za ublažitev učinkov transakcijskega tveganja lahko nekateri previdnostni ukrepi, ki jih lahko sprejme vsaka stranka v poslu, vključujejo spodaj navedene tehnike ublažitve. Te metode, ki se uporabljajo za obvladovanje transakcijskega tveganja, so pogosto vključene v klavzule transakcijske pogodbe ali v proces posla (CFI Team, 2023).

- **Varovanje pred tveganjem**

Podjetja se bodo vključila v dogovore o varovanju pred tveganjem, da bi zmanjšala stopnjo potencialnega tveganja zaradi gibanja cen različnih sredstev. Varovanje pred tveganjem zagotavlja podjetjem zaščito pred neugodnimi spremembami cen sredstev, ki lahko negativno vplivajo na naložbe. V okviru transakcij bodo podjetja pogosto sklenila dogovore o varovanju pred tveganjem, da zmanjšajo učinke valutnega in blagovnega tveganja, povezanega s poslom.

- **Refinanciranje**

V okolju nihajočih obrestnih mer si podjetja pogosto prizadevajo refinancirati svoj dolg, ko obrestne mere padajo. Refinanciranje dolgov omogoča podjetjem, da zmanjšajo svoje dolžniške obveznosti in se zadolžijo po privlačnejših obrestnih merah. Da bi zagotovili upravičenost stranke do refinanciranja, lahko stranka, ki najema posojilo, v svoje pogodbe vključi klavzule o ponovnem pogajanju, ki omogočajo prilagoditve refinanciranja, ko se obrestne mere znatno spremenijo znatne spremembe obrestne mere (CFI Team, 2023).

– Dolžna skrbnost

Da bi zmanjšali možnost, da nasprotna stranka ne bi izpolnila svojih pogodbenih obveznosti, bodo stranke opravile obsežen postopek skrbnega pregleda, da bi ocenile različne komponente transakcije, preden dosežejo dogovor. Če ima nasprotna stranka večje tveganje neplačila, lahko kupec v transakcijsko pogodbo vključi premijo za tveganje neplačila, da ustvari spodbudo za prevzemanje večjega tveganja (CFI Team, 2023).

Zavarovanje je glavno varovalo pri obladovanju tveganj in zelo veliko tveganj je mogoče zavarovati. Nekatera tveganja so nedvomno prednostna, kot je na primer tveganje goljufije ali poneverbe, kjer zaposleni ravnajo z denarjem ali opravljajo računovodske naloge v zvezi z obveznostmi in terjatvami. Specializirane zavarovalnice bodo izdale denarno garancijo za finančno kritje v primeru poneverbe, kraje ali goljufije. Kadar se zavarujete pred morebitnimi tveganji, se morate vedno zavedati najhujših scenarijev. Sam obseg zavarovalnega kritja pa je odvisen od narave posla organizacije (Davis, 2023).

12.3 Sodelovanje z notranjimi regulatorji

Sredstva organizacije so dragocena in zato pogosto predstavljajo veliko tveganje, če niso ustrezno zavarovana in varovana. Notranja revizija proučuje načine, s katerimi lahko organizacija ta sredstva varuje, in ali so vzpostavljena ustrezna varovala. Prav tako mora biti notranji revizor sposoben oceniti, ali so postopki, ki so vzpostavljeni za varovanje sredstev, primerni in zadostni pred izgubami, kot so požar, kraja, nezakonite dejavnosti in podobno. Pri tem moramo vedeti, da sredstva niso le računalniki, tiskalniki, fotokopirni stroji in drugo, temveč spadajo sem tudi zaposleni in informacije, ki so prav tako potrebni varovanja. Tehnologija se razvija vsakodnevno, zato se povečujejo tudi izzivi pri njenem varovanju (Združenje notranjih revizorjev, n. d.).

Odgovorite na vprašanja

Kaj je finančna varnost? Opredelite.

Kaj je prevara?

Kako oziroma na kakšne načine se preprečujejo finančne prevare?

Zakaj je poznavanje zaposlenih pomembno pri finančni varnosti?

Kakšna je vloga dokumentacije pri zmanjševanju goljufij?

Naštejte nekaj načinov, ki sem vam zdijo najpomembnejši pri povečevanju varnosti spletnega bančništva in s tem pri preprečevanju goljufij.

Kaj je transakcijsko tveganje?

Kakšne vrste transakcijskih tveganj poznamo?

Kaj je notranja revizija? Pojasnite.

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

13 Varovanje zaposlenih in objektov

Varovanje zaposlenih in objektov in s tem zagotavljanje varnega delovnega mesta je pravni proces korporativne varnosti, ki pripomore k zagotavljanju celovite varnosti organizacije. Zraven spada varnost na delovnem mestu, ki sestoji iz varstva pri delu, medicine dela, požarne varnosti ter zaščite premoženja in infrastrukture (Dvojmoč, 2020).

13.1 Varnost na delovnem mestu

Varnost zaposlenih zajema ukrepe na naslednjih področjih: kadrovska politika, preverjanje zaposlenih ter usposabljanje s področja varnosti.

Varnost, zdravje, zadovoljstvo, motivacija in kreativnost so predpogoji, ki morajo biti izpolnjeni, če naj zaposleni dosegajo kakovostni delovni učinek (Vršec, 1993). Skrb za varnost zaposlenih predstavljajo tudi programi za varnostno ozaveščanje in izobraževanje zaposlenih. Področje varnosti zaposlenih posredno in neposredno urejajo predpisi s področja varnosti in zdravja pri delu ter s področja požarne varnosti. K varnosti zaposlenih spada tudi zaščita pravic zaposlenih, ki zajema organizacijske ukrepe menedžmenta, v sodelovanju s kadrovsko in pravno službo, s čimer se zagotavljajo pravice s področja delovnega razmerja, socialne varnosti, zdravstvene zaščite in druge (Vršec, 1993). Občutljiv proces, ki posega v varnost in še bolj v zasebnost zaposlenih, je varnostno preverjanje kandidatov za zaposlitev ter redna preverjanja preteklosti.

Delodajalec je dolžan zagotoviti varnost in zdravje svojih zaposlenih v zvezi z delom. V povezavi s tem mora izvajati določene ukrepe, ki so potrebni za zagotavljanje varnosti in zdravja posameznikov, kamor spada tudi preprečevanje nevarnosti pri delu, obveščanje in usposabljanje delavcev (Inšpektorat Republike Slovenije za delo, 2020).

Prav tako mora delodajalec izvajati in sprejemati takšne ukrepe in metode, ki zagotavljajo čim višjo stopnjo varnosti in zdravja na delovnem mestu. Pri tem mora upoštevati načela, kot so: izogibanje nevarnostnim; ocenjevanje tveganj; prilagajanje dela posameznikom; nadomeščanje nevarnega z nenevarnim; dajanje ustreznih navodil in podobno. Delodajalci morajo pisno oceniti tveganja, ki so jim izpostavljeni njihovi zaposleni, po določenem postopku, ki obsega identifikacijo nevarnosti; ugotovitev, kdo bi lahko bil izpostavljen nevarnosti; oceno tveganja; odločitev, ali je tveganje sprejemljivo; odločitev o uvedbi ukrepov. Pomembno je, da oceno tveganja spremeni vsakokrat, ko ukrepi niso več zadostni ali se podatki spremenijo ali pa obstajajo možnosti za njeno dopolnitev. Po izvedeni oceni tveganja mora delodajalec sprejeti tudi izjavo o varnosti z oceno tveganja v pisni obliki, ki vsebuje načrt za izvedbo predpisanih zahtev in ukrepov, načrt za izvedbo ukrepov v primeru nevarnosti in opredelitev obveznosti ter odgovornosti odgovornih oseb za zagotavljanje varnosti in zdravja pri delu (Inšpektorat Republike Slovenije za delo, 2020).

Delavci imajo tudi določene pravice in dolžnosti v povezavi z varnostjo in zdravjem pri delu. Vsak posameznik ima pravico do dela v okolju, ki mu zagotavlja varnost in zdravje pri delu, pri tem pa je tudi sam zavezan k spoštovanju in izvajanju določenih ukrepov za zagotavljanje le-tega. Delo mora opravljati pazljivo in s tem varovati življenje ter zdravje sebe in drugih. Vso delovno opremo mora uporabljati v skladu z navodili in priporočili ter njihovim namenom, pomembno pa je tudi, da na delovnem mestu ni pod vplivom alkohola, drog ali drugih substanc. Pravico ima, da delo odkloni v določenih primerih, predvsem, kadar mu grozi nevarnost za življenje in zdravje. Prav tako ima delavec pravico do zdravstvenih pregledov in ob tem tudi dolžnost, da se jih udeleži, če je tako zakonsko določeno (Inšpektorat Republike Slovenije za delo, 2020).

13.2 Varnost pri delu

Ključna dokumenta varnosti pri delu sta:

– Zakon o varnosti in zdravju pri delu (»Zakon o varnosti in zdravju pri delu (ZVZD-1)«, 2011) usklajen z določbami direktive EU na področju varnosti in zdravja pri delu (»Direktiva 89/391/EGS«, 1989).

– Mednarodni standard OHSAS 18001 (Occupational Health and Safety Assesment Series for health and safety management system).

Po »ZVZD-1« (2011) mora delodajalec za opravljanje strokovnih nalog v zvezi z zagotavljanjem varnosti pri delu med svojimi zaposlenimi določiti enega ali več strokovnih delavcev za varnost pri delu, ki imajo opravljen splošni in posebni del strokovnega izpita iz varnosti in zdravja pri delu. Strokovni delavec je za opravljanje strokovnih nalog neposredno odgovoren delodajalcu.

Ukrepi vključujejo preprečevanje nevarnosti in obveščanje ter usposabljanje delavcev. Pri izvajanju ukrepov mora delodajalec slediti temeljnim načelom »ZVZD-1« (2011).

Med drugimi so našteta:

– izogibanje tveganjem,
– prilagajanje tehničnemu napredku,
– nadomeščanje nevarnega z nenevarnim ali manj nevarnim,
– dajanje ustreznih navodil in obvestil delavcem. (Dvojmoč, 2020)

Med obveznosti delodajalca sodi tudi izdelava in sprejetje izjave o varnosti v pisni obliki, s katero se določijo način in ukrepi zagotavljanja varnosti. Ob vsaki spremembi (nova nevarnost, sprememba ravni tveganja) se varnostna izjava dopolni. Sestavljena je iz ugotovitve možnih vrst nevarnosti na delovnem mestu in v delovnem okolju ter ocene tveganja za nastanek poškodb in zdravstvenih okvar. Delodajalec zagotavlja varnost in zdravje pri delu na naslednje načine:

– dodeli opravljanje nalog varnosti pri delu strokovnemu delavcu, naloge varovanja zdravja pri delu pa pooblaščenemu zdravniku;
– sprejme ukrepe za zagotavljanje požarnega varstva v skladu s posebnimi predpisi;
– sprejme ukrepe za zagotavljanje prve pomoči in evakuacije v primeru ogroženosti;
– obvešča delavce o uvajanju novih tehnologij in sredstev za delo ter o nevarnostih za poškodbe in zdravstvene okvare, ki so povezane z njimi, ter izdaja navodila za varno delo;
– usposablja delavce za varno delo;
– delavcem zagotavlja sredstva in opremo za osebno varnost pri delu in njihovo uporabo, če sredstvo za delo in delovno okolje kljub varnostnim ukrepom ne zagotavlja varnosti in zdravja pri delu;

- zagotavlja periodične preiskave delovnega okolja in periodične preglede ter preizkuse delovne opreme;
- zagotavlja zdravstvene preglede delavcev. (Dvojmoč, 2020)

Zakonsko usposabljanje varnosti pri delu mora delavec opraviti ob sklenitvi delovnega razmerja; pred razporeditvijo na drugo delo; pred uvajanjem nove tehnologije in novih sredstev za delo in ob spremembi v delovnem procesu, ki lahko povzroči spremembo varnosti pri delu. Usposabljanje morajo opraviti tako redno zaposleni kot tudi študenti, dijaki in delavci, ki opravljajo delo na podlagi podjeme pogodbe (Data, 2023).

Za zaposlene v gospodarski družbi je usposabljanje s področja varnosti ključnega pomena, saj se tako seznanijo s potencialnimi tveganji, ukrepi za upravljanje tveganj in postopki za minimaliziranje posledic, če do teh že pride. Posameznikom, ki so v podjetju zadolženi za področje varstva in varnosti, velja nameniti še posebno skrb za redno usposabljanje, izobraževanje in izpopolnjevanje, saj je od kakovosti tega odvisno njihovo opravljanje delovnih nalog. Oba vidika usposabljanja s področja varnosti posledično vodita v razvoj visoke stopnje varnostne kulture v podjetju (Podbregar, 2007).

13.3 Medicina dela

Medicina dela (znana tudi kot »zdravje pri delu«) je osredotočena na zdravljenje poškodb in bolezni pri delu. Zdravniki, usposobljeni za medicino dela, diagnosticirajo in zdravijo poškodbe pri delu veliko učinkoviteje kot večina zdravnikov primarne zdravstvene oskrbe. So na tekočem z zveznimi in državnimi predpisi za zdravje in varnost delovne sile, tako da lahko zagotovijo najboljše zdravljenje, načrtujejo in opravljajo regulativne preglede. Zdravniki medicine dela pogosto sodelujejo neposredno z delodajalci, da zagotovijo delovanje podjetij in varnost ter zdravje zaposlenih pri delu (Concentra, 2023).

Po »ZVZD-1« (2011) mora delodajalec zagotoviti, da zdravstvene ukrepe v zvezi z varnostjo in zdravjem pri delu izvaja izvajalec medicine dela – zdravnik specialist medicine dela, prometa in športa. Naloge so določene v zakonu in so:

- sodelovanje pri izdelavi strokovnih podlag za izjavo o varnosti z oceno tveganja;
- izvajanje zdravstvenih pregledov,
- seznanjanje delavcev s tveganji, povezanimi z njihovim delovnim mestom in delovnim okoljem, ki lahko privedejo do funkcionalnih okvar, bolezni ali invalidnosti;

- spremljanje in analiza stanja v zvezi s poklicnimi boleznimi ter boleznimi, povezanimi z delom, in odkrivanje vzrokov;
- priprava poročila za delodajalce glede na ugotovitve iz analiz zdravstvenega stanja delavcev, ugotovljenega na zdravstvenih pregledih in podobno. (Dvojmoč, 2020)

13.4 Požarna varnost

Sistem varstva pred požarom zajema množico dejavnosti – organiziranje, načrtovanje, izvajanje, nadzor in financiranje ukrepov varstva pred požarom. Cilji sistema varstva pred požarom so zagotavljanje varnosti ljudi, živali, premoženja in okolja pred požarom. Dosegajo se z ustreznim načrtovanjem, upoštevanjem preventivnih ukrepov, pravočasnim odkrivanjem požara, obveščanjem, s preprečevanjem in zmanjševanjem škodljivih posledic požara ter z vzpostavitvijo ekonomskih razmerij med predpisanimi ukrepi in pričakovano škodo (Hrovat in Gorše, 2000).

Pravna podlaga področja požarne varnosti je »Zakon o varstvu pred požarom (ZVPoz-UPB1)« (2007) in predpisi, izdani na njegovi podlagi. Po zakonu so naloge delodajalca naslednje:

- izdelava požarnega reda,
- usposabljanje zaposlenih za požarno varstvo,
- izvajanje ukrepov varstva pred požarom,
- vzdrževanje opreme in naprav za varstvo pred požarom,
- vodenje evidence o požarih, o usposobljenosti zaposlenih, o opremi in napravah za varstvo pred požarom (»ZVPoz-UPB1«, 2007).

Na podlagi zakona je bil izdan pravilnik o izdelavi ocen požarne ogroženosti (»Pravilnik o izdelavi ocen požarne ogroženosti«, 2020), ki obvezuje lastnike in uporabnike poslovnih ter industrijskih objektov, da izdelajo oceno požarne ogroženosti. Z njo se ugotavljajo naslednje stopnje požarne ogroženosti okolja: stopnja 1 – zelo majhna požarna ogroženost; stopnja 2 – majhna požarna ogroženost; stopnja 3 – srednja požarna ogroženost; stopnja 4 – srednja do povečana požarna ogroženost; stopnja 5 – velika požarna ogroženost; stopnja 6 – zelo velika požarna ogroženost (Dvojmoč, 2020).

Pred začetkom izdelave ocene so potrebni naslednji podatki: podatki o oskrbovanosti z vodo za gašenje; podatki o oddaljenosti in kategoriji gasilskih enot; podatki o požarni zaščiti objekta (samodejne stabilne naprave za gašenje požarov, avtomatske naprave za

javljanje požara, industrijske gasilske enote); podatki o obremenjenosti industrije z nevarnimi snovmi in podatki o snoveh (vrsta in količina) (Hrovat in Gorše, 2000).

V »Pravilniku o požarnem redu« (2007) je določeno, pod katerimi pogoji morajo lastniki ali uporabniki stanovanjskih objektov, poslovnih oz. industrijskih objektov izdelati požarni red in požarni načrt ter načrt evakuacije.

Lastniki ali uporabniki objektov morajo določiti požarni red, da preprečijo nastanek požara in izboljšajo požarno varnost. Delodajalec mora o požarnem redu obvestiti vse zaposlene, poleg tega pa tudi določiti osebo, ki bi bila v primeru požara odgovorna za gašenje začetnih požarov in izvajanja načrta evakuacije. Prav tako mora določiti vrste in načine usposabljanja odgovornih oseb za gašenje začetnih požarov in izvajanje evakuacije. Poleg tega je treba imeti tudi izvleček požarnega reda, ki mora vsebovati podatke o organizaciji varstva pred požarom; ukrepe varstva pred požarom in navodila za ravnanje v primeru požara (»Pravilnik o požarnem redu«, 2007).

Požarni načrt je grafični prikaz situacije objekta in delov objekta z označenimi nevarnostmi ter sistemi, napravami in sredstvi za preventivno in dejavno požarno zaščito, s katerim se zmanjšuje nevarnost nastanka požara oziroma zagotavlja učinkovito gašenje, če do požara pride. Namenjen je uporabnikom objekta, gasilcem in drugim reševalcem. Načrt mora vsebovati prikaz objekta v prostoru in prikaz požarne varnosti objekta (»Pravilnik o požarnem redu«, 2007).

Določeno je tudi, da se morajo lastniki ali uporabniki objektov, za katere je treba izdelati načrt evakuacije, najmanj enkrat letno udeležiti praktičnega usposabljanja ter voditi evidenco o času, sodelujočih in načinu izvedbe usposabljanja (»Pravilnik o požarnem redu«, 2007).

S »Pravilnikom o usposabljanju in pooblastilih za izvajanje ukrepov varstva pred požarom« (2011) je določeno, da morajo delodajalci svoje zaposlene usposabljati o varstvu pred požarom. Zagotoviti morajo, da je vsak zaposleni usposobljen za to in seznanjen s požarnim redom; prav tako pa morajo določiti zaposlene, ki se usposobijo za gašenje; določiti število, vrste in način usposabljanja oseb, ki so odgovorni za gašenje prvih požarov; poskrbeti za praktično usposabljanje za izvajanje evakuacije v skladu s predpisi.

13.5 Zaščita premoženja in infrastrukture

Poslovna sredstva oziroma premoženje organizacije se nanaša na vse vire ali lastnino, ki pripada organizaciji, vključno s fizičnimi sredstvi, kot so oprema, inventar, nepremičnine in intelektualna lastnina, kot so patenti in avtorske pravice. Finančna sredstva, kot so denarne rezerve, naložbe in terjatve, se prav tako lahko štejejo za poslovna sredstva. Ta sredstva so bistvenega pomena za uspeh in rast podjetja, zato morajo podjetja nujno dati prednost njihovi zaščiti (Nanda, 2023).

Če se poslovna sredstva ne zaščitijo, lahko pride do hudih posledic, vključno s finančno izgubo, pravnimi bitkami z dobavitelji ali strankami in prekinitvami poslovanja, ki lahko med drugim povzročijo zmanjšan prihodek in škodo ugledu. Ta tveganja lahko tudi zavirajo prihodnje poslovne priložnosti in ovirajo rast. Poskrbeti je treba, da ima organizacija kvalificiranega poslovnega odvetnika, s katerim se zagotovijo ustrezni ukrepi za zaščito premoženja in se učinkovito odzove, če pride do incidenta (Nanda, 2023).

Načinov, kako zaščititi premoženje, je ogromno. Predstavili bomo nekaj ukrepov, ki so pogosto uporabljeni in priporočljivi.

- Sporazumi o nerazkritju (NDA) so pravne pogodbe, ki ščitijo zaupne informacije, poslovne skrivnosti in intelektualno lastnino podjetja pred posredovanjem ali razkritjem s strani zaposlenih ali drugih zainteresiranih strani. NDA so ključnega pomena za podjetja, ki morajo razkriti občutljive informacije ali deliti IP z drugimi strankami, hkrati pa zagotoviti, da te informacije ostanejo zaupne. Podjetja lahko oblikujejo in uveljavljajo NDA tako, da sodelujejo z izkušenimi poslovnimi pravniki, ki lahko pripravijo trdne pogodbe, ki zajemajo vse pravne vidike, da zagotovijo ustrezno zaščito sredstev podjetja.
- Pridobitev blagovnih znamk in patentov lahko zagotovi pravno zaščito intelektualne lastnine podjetja. Patenti dajejo imetniku izključne pravice do izdelave ali uporabe izuma, medtem ko blagovne znamke ščitijo edinstvene logotipe, imena in druge oznake, ki identificirajo izdelke ali storitve podjetja.
- Podjetja, ki ustvarjajo izvirna avtorska dela, kot so literarne, dramske, glasbene in umetniške stvaritve, za zaščito uporabljajo avtorske pravice le-teh. Avtorske pravice dajejo lastniku izključne pravice za reprodukcijo, distribucijo in javno izvedbo njihovega dela. Poleg tega avtorske pravice zagotavljajo pravna sredstva za kršitve in omogočajo lastnikom, da izterjajo odškodnino, če se njihovo delo uporablja brez dovoljenja. Ta zaščita spodbuja ustvarjalnost in podjetjem zagotavlja sredstva za zaščito svojih dragocenih sredstev.

- Imeti trden finančni načrt je ključnega pomena za podjetja, da zaščitijo svoje premoženje. Razumevanje, kakšne odločitve sprejeti, ko gre za vlaganje, varčevanje in porabo, je prvi korak pri ustvarjanju celovitega finančnega načrta. Podjetja bi morala sodelovati z usposobljenimi strokovnjaki, kot so finančni svetovalci in računovodje, da bi jim pomagali pri krmarjenju s kompleksnostjo davčne zakonodaje in regulativnih zahtev. Poleg tega lahko podjetja razmislijo tudi o pridobitvi zavarovalnih polic, ki posebej pokrivajo njihovo premoženje in zagotavljajo finančno zaščito v primeru škode ali izgube.
- V nekaterih primerih morajo podjetja zagotoviti, da dejavno vzdržujejo svoja sredstva, da jih zaščitijo. Če ima podjetje v lasti fizična sredstva, kot so oprema, zgradbe ali vozila, je pomembno, da jih vzdržujejo v dobrem stanju z rednim vzdrževanjem in pregledi. To ne pomaga preprečiti le nesreč in dragih izpadov, temveč lahko tudi podaljša življenjsko dobo sredstev.
- Če se finančno stanje podjetja nepričakovano spremeni, je pomembno, da imamo vzpostavljen rezervni načrt za zaščito sredstev. To lahko vključuje rezerviranje sredstev za nujne primere, diverzifikacijo naložb ter redno pregledovanje in prilagajanje finančnega načrta, da se zagotovi stalna zaščita sredstev. Poleg tega lahko podjetja razmislijo tudi o uvedbi varnostnih ukrepov, kot so nadzorni sistemi, tehnologije za nadzor dostopa in kibernetski varnostni protokoli, da zaščitijo svoja digitalna sredstva pred krajo ali kibernetskimi napadi. Ostati morajo pazljivi, da zaščitijo premoženje, in nenehno dejavno ocenjevati tveganja, da naredijo potrebne prilagoditve.
- Vedno je treba upoštevati previdnostne ukrepe, s katerimi se izognemo prevaram in goljufijam. Tudi pri e-pošti in telefonskih klicih se morajo podjetja zavedati morebitnih prevar in poskusov goljufij, ki lahko povzročijo izgubo sredstev. Poskrbeti je treba, da so zaposleni poučeni o običajnih vrstah prevar in goljufij ter tudi določiti jasne politike za odzivanje na sumljivo komunikacijo. Zaščititi je treba vse podatke, vključno z osebnimi in finančnimi podatki strank, tako da se ustrezno zavaruje s šifriranjem, požarnimi zidovi, gesli in drugimi varnostnimi ukrepi. Pri tem lahko na pomoč priskoči tudi podjetje za kibernetsko varnost, da oceni ranljivosti in zagotovi priporočila za izboljšanje obrambe kibernetske varnosti.
- Dobro je izvesti oceno tveganja, s katero se prepoznajo morebitne grožnje in ranljivosti sredstev. To podjetjem pomaga ugotoviti, katera sredstva so najbolj ogrožena, in temu primerno določiti prednost svojih prizadevanj za zaščito. To vključuje ukrepe, kot so pravilniki o geslih, dvofaktorska avtentikacija in nadzor dostopa na podlagi vlog. (Nanda, 2023)

Infrastrukturna varnost je praksa zaščite kritičnih sistemov in sredstev pred fizičnimi in kibernetskimi grožnjami. Z vidika IT to običajno vključuje sredstva strojne in programske opreme, kot so naprave končnih uporabnikov, viri podatkovnega centra, omrežni sistemi in viri v oblaku (Hewlett Packard, 2023).

Podjetja so za vzdrževanje delovanja odvisna od svojih tehnoloških sredstev, zato varovanje tehnološke infrastrukture ščiti samo organizacijo. Lastniški podatki in intelektualna lastnina mnogim podjetjem zagotavljajo pomembne konkurenčne prednosti na trgu, vsaka izguba ali motnja dostopa do teh informacij pa ima lahko globok negativen vpliv na dobičkonosnost podjetja (Hewlett Packard, 2023).

Zaradi povečane medsebojne povezljivosti in povečanega sprejemanja storitev v oblaku, mikrostoritev in komponent programske opreme na različnih platformah v oblaku in na robovih omrežij podjetij je varovanje tehnološke infrastrukture bolj zapleteno in pomembnejše kot kdaj koli prej. Sprejetje varnostnih arhitektur ničelnega zaupanja je eden od načinov, kako se podjetja spopadajo s tem izzivom. Ničelno zaupanje je filozofski pristop k upravljanju identitete in dostopa, ki določa, da nobenemu uporabniku ali delovni obremenitvi ni privzeto zaupanja. Zahteva, da vsi uporabniki, naprave in primerki aplikacij dokažejo, da so to, za kar se predstavljajo, in da so pooblaščeni za dostop do virov, ki jih iščejo (Hewlett Packard, 2023).

Usposabljanje zaposlenih o varnosti gesel in poverilnic prav tako igra pomembno vlogo pri zaščiti IT infrastrukture. Pogosto je človeški element lahko najšibkejši člen v varnostni strategiji organizacije in neusmiljeni poskusi vdorov pomenijo, da lahko celo kratka in na videz manjša napaka v varnostnem območju povzroči znatno škodo (Hewlett Packard, 2023).

In ker se lahko kadar koli pojavijo nove vrste groženj ali pa imajo katastrofalne posledice, ki so večje od pričakovanih, robustna in pogosta strategija varnostnega kopiranja zagotavlja ključno varnostno mrežo za neprekinjeno poslovanje. Ker količine podatkov vztrajno naraščajo, bi morala podjetja iskati rešitev za zaščito podatkov, ki zagotavlja stalno razpoložljivost preko preproste, hitre obnovitve po motnjah, globalno doslednega delovanja ter brezhibne mobilnosti aplikacij in podatkov v več oblakih (Hewlett Packard, 2023).

Ker se vse več poslovanja izvaja digitalno in se podjetja vse bolj zanašajo na podatke za sprejemanje ključnih poslovnih odločitev, postaja zaščita virov, ki omogočajo te dejavnosti, vse pomembnejša. In z več napravami, ki imajo dostop do omrežij podjetij,

večjim številom uporabnikov, ki dostopajo do dragocene intelektualne lastnine podjetja z uporabo nezavarovanih javnih omrežij na lokacijah po vsem svetu, in z več podatki, ki se generirajo in porabijo prek robov in oblakov, ima veliko organizacij ranljivo vse večjo površino napadov do groženj.

Kriminalci, hekerji, sovražni nacionalno-državni akterji, teroristi in drugi uporabljajo vse bolj sofisticirane metode za ciljanje na organizacije vseh velikosti po vsem svetu. Vse varnostne grožnje nimajo zlonamernega namena, saj lahko človeške napake in naravne nesreče prav tako predstavljajo nevarnost za integriteto tehnološke infrastrukture organizacije. Za zaščito neprekinjenega poslovanja je ključna zahteva za delovanje v današnjem digitalno povezanem svetu imeti vzpostavljeno strategijo za kibernetsko in fizično varnost v vseh ključnih sistemih in sredstvih (Hewlett Packard, 2023).

Odgovorite na vprašanja

Kaj za vas pomeni varnost na delovnem mestu? Pojasnite.

Na katerih področjih »deluje« varnost zaposlenih?

Katera sta ključna dokumenta za varnost pri delu?

Kaj so obveznosti delodajalca?

Na katere načine delodajalec zagotavlja varnost in zdravje na delovnem mestu oziroma delu? Naštejte nekaj primerov.

Katere so pravice in dolžnosti delavcev?

Kdaj mora delavec opraviti zakonsko usposabljanje varnosti pri delu?

Kaj je medicina dela?

Katere so naloge, določene po Zakonu o varnosti in zdravja pri delu (»ZVZD-1«, 2011), za izvajalca medicine dela?

Kaj je požarna varnost in kaj zajema?

Katere so naloge delodajalca v povezavi s požarno varnostjo?

Kaj je požarni red?

Kaj je požarni načrt?

Kaj je določeno s »Pravilnikom o usposabljanju in pooblastilih za izvajanje ukrepov varstva pred požarom« (2011)?

Kaj je ocena požarne ogroženosti?

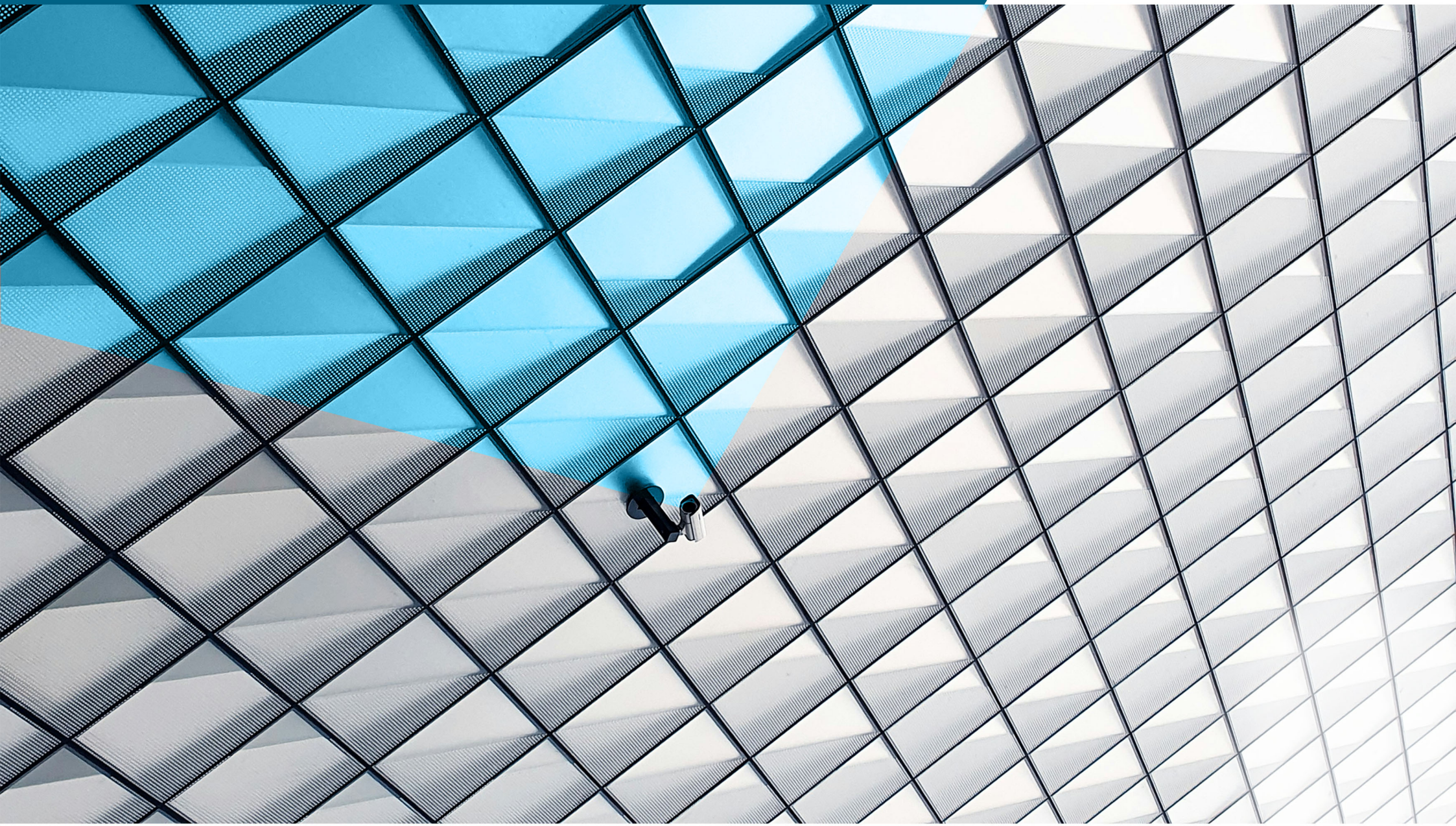
Kaj za vas predstavljata premoženje in infrastuktura organizacije?

Na kakšne načine se lahko zaščiti premoženje organizacije?

Razmislite in zapišite, na kakšne načine bi se po vašem mnenju še lahko zavarovala premoženje in infrastruktura organizacije.

ZAPISKI

DEL III



POSEBNE TEME V KORPORATIVNI VARNOSTI

Univerzitetna založba
Univerze v Mariboru

14 Posebne teme korporativne varnosti

14.1 Korporativna varnost in poslovna skrivnost

Poslovne skrivnosti ščitijo podatke, znanja in vrednosti neke gospodarske družbe pred konkurenco na trgu. Varujejo znanja o:

- načinu in postopku organiziranja določenega delovnega procesa,
- tehnologiji,
- informacijah o poslovnih partnerjih,
- zaposlenih,
- finančnih podatkih in
- drugih vrstah pomembnih informacij, ki so se znotraj gospodarske družbe zbirale in razvijale več let. (Španinger, 2006)

Po »Zakonu o gospodarskih družbah (ZGD-1)« (2006) za poslovno skrivnost štejemo podatke, ki so tako določeni s pisnim sklepom gospodarske družbe. S sklepom morajo biti seznanjeni družbeniki, delavci, člani organov družbe in tudi druge osebe, ki morajo varovati poslovno skrivnost. Obveznost varovanja poslovne skrivnosti imajo osebe znotraj in zunaj gospodarske družbe (»ZGD-1«, 2006).

Poslovna skrivnost je opredeljena tudi kot zaupne informacije, ki imajo komercialno vrednost in so glede na okoliščine predmet ukrepov varovanja. Vsaka država mora zase uskladiti, kako bo poslovne skrivnosti zavarovala z zakoni in drugimi pravnimi predpisi.

Izguba poslovnih skrivnosti na kakršen koli način bi predstavljala izgubo vrednosti organizacije. To so lahko na primer informacije o imenu, elektronskem naslovu in telefonski številki, ki so ključni podatki stranke in se lahko obravnavajo kot poslovna skrivnost (Ollivier in De Leon, 2021).

Poslovna skrivnost je definirana tudi v »Zakonu o podjetjih (Zpod)« (1988), ki jo določa kot listine in podatke, določene s statutom oziroma s pravili ali kakšnimi drugimi samoupravnimi splošnimi akti oziroma splošnimi akti podjetja, katerih posredovanje nepooblaščeni osebi bi bilo v nasprotju s poslovanjem podjetja in bi škodovalo njegovim interesom ter poslovnemu ugledu, če z zakonom ni določeno drugače. Pri tem gre tudi za podatke, ki so znani le omejenemu krogu ljudi. Predmet poslovne skrivnosti je vedno dejstvo, ne le domneva, ki pa mora biti pridobljeno na zakonit način (Žirovnik in Podbregar, 2006).

»ZDR-1« (2013) delavcu prepoveduje izkoriščanje poslovnih skrivnosti za osebno uporabo ali izdajanje le-teh tretji osebi. Poslovne skrivnosti so kot take določili delodajalci in so bile delavcu zaupane ali pa je bil z njimi seznanjen na kakšen drug način. Kot poslovna skrivnost so opredeljeni tudi tisti podatki, za katere je očitno, da bi ob razkritju nepooblaščeni osebi nastala občutna škoda (Dvojmoč, 2020).

»Zakon o poslovni skrivnosti (ZPosS)« (2019) je v slovensko zakonodajo prinesel direktivo Evropske unije iz leta 2016. S tem zakonom je opredelitev poslovne skrivnosti, ki je bila prej razpršena v več različnih zakonih, zdaj združena na enem mestu. Poslovna skrivnost je opredeljena kot nerazkrito strokovno znanje, izkušnje in poslovne informacije, ki izpolnjujejo naslednje zahteve: je skrivnost, ki ni splošno znana ali lahko dosegljiva osebam v krogih, ki se običajno ukvarjajo s to vrsto informacij; ima tržno vrednost; imetnik poslovne skrivnosti je v danih okoliščinah razumno ukrepal, da jo ohrani kot skrivnost. Pomembna novost za organizacije je tudi, da se mora poslovna skrivnost določiti v pisni obliki (Finance PR, 2019).

Poleg zakonske ureditve področja dolžnosti varovanja poslovnih skrivnosti je pomembno, da so znotraj gospodarske družbe oblikovana tudi interna pravila, ki razvijajo čut za varovanje poslovnih skrivnosti in urejajo tudi občutljivo tematiko odnosa posameznikov, ki zapuščajo gospodarsko družbo (Podbregar, 2007).

Poslovne skrivnosti se lahko zaščitijo z ukrepi, ki so:

- kadrovske narave: odklonitev zaposlitve delavca, ki je pri nekdanjem delodajalcu izdal njegovo poslovno skrivnost;
- pravne narave: določilo o dolžnosti varovanja poslovnih skrivnosti v pogodbi o delu;
- tehnološke narave: fizična preprečitev dostopa nepoklicanim v razvojni laboratorij;
- organizacijske narave: skrb za dobro poučenost sodelavcev o zadevah v zvezi z varovanjem poslovnih skrivnosti;
- elektronski prenos informacij: šifriranje in
- elektronska obdelava informacij: preprečitev pristopa do posameznih poslovnih skrivnosti neupravičenim osebam. (Kop, 1995)

Za učinkovito zaščito je potrebno prepletanje več pogojev, pri čemer so bistvenega pomena dobro ozračje v organizaciji, dobra poučenost, dober koncept za varovanje in zaščito ter zagotovitev ugodnih pogojev za učinkovitost ukrepov (Kop, 1995). Poleg tega mora celovit sistem varovanja poslovne skrivnosti vključevati več podsistemov, in sicer kadrovsko, fizično, administrativno, informacijsko in industrijsko varnost (Čaleta, 2005).

V podsistem kadrovske varnosti spadajo (varnostno) preverjanje zaposlenih, varnostno izobraževanje, usposabljanje in izpopolnjevanje zaposlenih ter tudi varovanje oseb na izpostavljenih delovnih mestih, ki se srečujejo s poslovnimi skrivnostmi visoke stopnje. Pri tem je bistvenega pomena, da se s poslovno skrivnostjo seznanijo samo tisti posamezniki, ki za opravljanje delovnih nalog nujno potrebujejo podatke, označene kot poslovno skrivnost (Čas, 2006).

Podsistem fizične varnosti temelji na sistemu fizičnega oziroma tehničnega varovanja ali pa, še pogosteje, na njuni kombinaciji. Ukrepi s področja fizične varnosti poslovne skrivnosti zajemajo predvsem določitev varnostnih območij in opredelitev načina vstopa vanje ter izbor sistema varovanja teh območij (Čas, 2006).

Administrativna varnost zajema naslednje ukrepe: označevanje, obdelovanje, posredovanje, hranjenje in uničevanje medijev z zapisom podatkov, označenih kot poslovna skrivnost; določitev načinov za prenos podatkov, ki so označeni kot poslovna skrivnost; določanje stopnje tajnosti poslovne skrivnosti; opredelitev nalog vseh oseb, ki se ukvarjajo z varovanjem poslovnih skrivnosti (Čas, 2006). Na osnovi identificiranih groženj in v skladu z zgornjimi ukrepi lahko gospodarski subjekt izdela interni predpis, ki

bo jasno predstavljal pravilne načine obravnave poslovnih skrivnosti. Tak predpis bi moral vsebovati naslednje vsebinske sklope: splošne določbe; stopnje tajnosti poslovnih skrivnosti; pooblaščene osebe, odgovorne za določanje poslovnih skrivnosti; merila za določanje stopenj tajnosti; postopek označevanja poslovnih skrivnosti; postopke obdelovanja in dostopa do tajnih podatkov; hrambo poslovnih skrivnosti; razmnoževanje poslovnih skrivnosti; tiskanje poslovnih skrivnosti; postopek uničevanja poslovnih skrivnosti; prehodne in končne določbe (Podbregar, 2007).

Informacijska varnost je za zagotavljanje varnosti podatkov ključnega pomena, saj je z večjo kompleksnostjo sistema večja tudi možnost napak, ki pa jih je še težje odkriti. Dobro zasnovan sistem informacijske varnosti v gospodarski družbi je torej ključnega pomena za preprečevanje nevarnosti in ranljivosti (Rakar, 2006). Zanimiva in pomembna je ugotovitev, da je problematika zagotavljanja informacijske varnosti vezana v večji meri na ljudi in v manjši na tehnologijo (Belič in Lesjak, 2006), kar spet opozarja na hkratno pomembnost ukrepov kadrovske varnosti in govori v korist sistemskemu pristopu varovanja. Čas (2006) obširno predstavlja ukrepe za varovanje poslovnih skrivnosti s področja informacijske varnosti: vzpostavitev in vzdrževanje učinkovitega sistema z zagotovljeno tajnostjo in dostopnostjo podatkov, ki so shranjeni, obdelovani ali poslani preko informacijskega omrežja; koncipiranje politike informacijske varnosti; odobritev ustreznega varnostnega organa pred uporabo informacijskega omrežja za shranjevanje, obdelovanje ali prenos tajnih podatkov; opredelitev pogojev za priključitev zunanjih informacijskih sistemov v informacijsko omrežje gospodarske družbe; določitev načinov sporočanja incidentov, povezanih z informacijsko varnostjo, ustreznemu varnostnemu organu gospodarske družbe.

Španinger (2006) navaja tri osnovne načine ogrožanja poslovnih skrivnosti, in sicer zlorabo, izdajo in gospodarsko vohunstvo:

- Za zlorabo gre, ko posameznik, ki upravičeno (denimo zaradi narave svojega dela) pozna neko poslovno skrivnost, to zlorabi v škodo lastnika poslovne skrivnosti in sebi v korist. Zlorabe večjega obsega povzročijo predvsem odhajajoči zaposleni, ki izkoristijo poslovne skrivnosti za izboljšanje uspeha podjetja oziroma delodajalca, ki ga bo zaposloval v prihodnje.
- Izdaja se zgodi takrat, ko posameznik, ki pozna neko poslovno skrivnost, to razkrije zainteresirani tretji osebi. Motivi za izdajo so raznovrstni in niso vedno povezani z materialnim okoriščanjem.

- Gospodarsko vohunstvo, kot eden izmed možnih načinov ogrožanja poslovnih skrivnosti, pa temelji na uporabi cele palete prikritih metod, v večini primerov je »uspešno« kombinirano z izdajo.

Vsi v organizaciji bi morali razumeti, kaj se lahko zgodi, če pride do ogrozitve poslovnih skrivnosti, in tudi kakšno je pravilno osnovno vedenje za dobro zaščito le-teh. Poleg tega bi morali imeti vsi tudi znanje o fizičnih, tehničnih in organizacijskih sredstvih za praktično zaščito informacij in podatkov v različnih okoliščinah. Sama organizacija bi morala prav tako jasno identificirati in opredeliti ključne nevarnosti in grožnje poslovnih skrivnosti ter ukrepe za zaščito le-teh. Določen je tudi seznam nalog, ki jih je treba upoštevati pri organiziranju praktičnega upravljanja poslovnih skrivnosti. To je predvsem organiziranje medkulturnega sodelovanja; zaznati, kaj vse so poslovne skrivnosti in jih opredeliti ter kot take označiti/določiti; opredeliti status poslovnih skrivnosti (ali so le zaupni podatki ali dejansko poslovne skrivnosti itd.); organizirati sledljivost poslovnih srkivnosti; oceniti dejanski potencial poslovnih skrivnosti; izvajati in preverjati učinkovite ukrepe varovanja poslovnih skrivnosti. Opredelitev statusa pomeni, da se poslovne skrivnosti identificirajo in se opredelijo glede na kategorije in njihovo vrednost; opredeli se razmerje med poslovnimi skrivnostmi in neopredmetenimi sredstvi; prednost se daje glavnim poslovnim skrivnostim (Ollivier in De Leon, 2021).

14.2 Zaščita intelektualne lastnine

Intelektualna lastnina zajema izdelke, ki so nastali kot posledica človeškega intelekta in razmišljanja. Deli se na avtorske pravice in industrijsko lastnino, kamor spadajo patenti, modeli, znamke in podobno. To področje ureja »ZIL-1« (2001), avtorske pravice pa ureja »Zakon o avtorski in sorodnih pravicah (ZASP-UPB3)« (2013) (Patentni biro, n. d.).

Zaščita intelektualne lastnine je zelo pomembna, saj:

- preprečuje tekmecem, da bi izdelke oziroma storitve podjetja kopirali;
- pomaga pri izogibanju nepotrebnih investicij;
- pomaga pri sami postavitvi identitete podjetja preko znamk in trženja;
- pomaga tudi pri pogajanjih za licenciranje, franšize in druge pogodbe;
- pomaga pri povečanju tržne vrednosti podjetja;
- pomaga pri finančnem stanju podjetja;
- pomaga pri povečanju kapitala in drugih možnosti financiranja;
- omogoča dostopnost novim trgom;

- pomaga pri ocenjevanju samega stanja raziskovanja in razvoja ter
- pomaga pri ocenjevanju dela zaposlenih in podjetja. (Patentni biro, n. d.)

Pravno zaščito stvarnopravnih pravic in pravic intelektualne lastnine zajema: pravno varovanje lastninske pravice in drugih stvarnih pravic organizacije; pravno zaščito patentov, blagovnih znamk, modelov, porekla proizvodov in pravno zaščito materialnih avtorskih pravic organizacije (Dvojmoč, 2017a).

Zaščita intelektualne lastnine ima tudi svoje prednosti. To so preprečevanje kopiranja, kar pomeni, da je z zaščito znamk, modelov in patentov pridobljena pravica do preprečevanja komercialne uporabe tretjih oseb. Poleg tega lahko predstavlja dodatni vir prihodka iz licenciranja in prodaje pravic, lažje pridobivanje investicij in strateških partnerjev ter uporabo zaščite pri oglaševanju z visokimi maržami, povečanjem prepoznavnosti in občutka varnosti pri potrošnikih (Gospodarska zbornica Slovenije, n. d.).

14.3 Preprečevanje izgube podatkov

Preprečevanje izgube podatkov se nanaša na identifikacijo in spremljanje občutljivih podatkov. Pri tem se mora zagotoviti, da do njih dostopajo le pooblaščene osebe in da so vzpostavljeni določeni zaščitni ukrepi proti uhajanju podatkov.

Pomembno je, da poznamo strategije, s pomočjo katerih se lahko izognemo izgubi podatkov. To so redne varnostne kopije datotek, saj so v primeru težav le-te zaščitene. Prav tako je priporočljivo imeti več rezervnih sistemov v različnih formatih in na različnih lokacijah. Posodobitev varnostnih sistemov je zelo pomemben korak pri zaščiti podatkov. Pri tem dejstvo, ali je podjetje malo ali veliko, ne igra vloge, saj nevarnost obstaja povsod. Posodabljanje prav tako pomaga pri proračunu, saj je znesek v primeru obnovitve podatkov lahko zelo visok. Če pride do izgube podatkov, je na voljo ogromno programov, ki nam lahko pomagajo pri njihovi obnovitvi. Prav tako je pomembno, da so datoteke v primeru, da so občutljive, šifrirane. Vse bolj je uveljavljeno tudi varnostno kopiranje 3-2-1, ki je časovno preizkušena metodologija zaščite in obnovitve podatkov. Zagotavlja, da so podatki zaščiteni in da so po potrebi na voljo varnostne kopije le-teh (Castagna, n. d.).

V Sloveniji področje izgube podatkov ureja »ZVOP-2« (2022), ki naslavlja Splošno uredbo o varstvu osebnih podatkov (GDPR). GDPR določa, da morajo biti osebni podatki obdelani na način, ki zagotavlja njihovo ustrezno varnost, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo

z ustreznimi ukrepi. Ogranizacije, ki svoje poslovanje usklajujejo z zakonom, boljše razumejo in upravljajo podatke, ki se zbirajo, poleg tega pa jih tudi boljše zaščitijo. Sam način obdelave podatkov mora biti pisno zapisan in urejen v obliki internega akta, torej pravilnika o postopkih in ukrepih za zavarovanje osebnih podatkov (v nadaljevanju pravilnik). Pomembno je, da so k pravilniku zavezani vsi, ki lahko kadar koli in kakor koli pridejo v stik z osebnimi podatki. To so lahko redno zaposleni, študenti, posamezniki na praktičnem usposabljanju, pogodbeni sodelavci, zunanji obiskovalci in podobno (Infocenter, n. d. a).

Splošna uredba o varstvu podatkov (v nadaljevanju Uredba) (»Uredba (EU) 2016/679«, 2016) sledi standardom na področju informacijske varnosti, pri čemer velja načelo, da je treba varnostne ukrepe prilagajati glede na tveganja, ki pretijo. Med ukrepe, ki jih Uredba predpisuje, spadajo tudi: psevdonimizacija in šifriranje osebnih podatkov; zmožnost zagotavljanja stalne zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo; zmožnost pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta; postopki rednega testiranja, ocenjevanja in vrednotenja učinkovitosti ukrepov za zagotavljanje varnosti obdelave podatkov. »ZVOP-2« (2022) pa vsebuje tudi dodatne zahteve, ki se morajo upoštevati poleg zahtev po Uredbi. Pomemben je predvsem 23. člen »ZVOP-2« (2022) , ki ureja varnost osebnih podatkov na področju posebnih obdelav. Gre torej za zahteve za posebej tvegane informacijske sisteme, kjer se obdelujejo občutljivi, zaupni in drugače varovani podatki, ki vključujejo tudi posebno vrsto osebnih podatkov (Informacijski pooblaščenec, n. d.).

14.4 Upravljanje kadrov in vodenje

– Varnostno svetovanje

Varnostno svetovanje je prenos znanja, izkušenj in raziskovalnih spoznanj od svetovalca na menedžment in strokovnjake za varnost v podjetjih in drugih organizacijah.

Prav tako se z varnostnim svetovanjem zagotavlja nadstandardno zasebno varovanje, kar se dosega s profesionalnim, kakovostnim in objektivnim svetovanjem gospodarskim družbam in tudi drugim. Sem spada tudi kakovosten nadzor nad samim izvajanjem varnostnih storitev varnostnih družb, ki varujejo ljudi in premoženje (Čas – Zasebna šola za varnostno izobraževanje, n. d.).

Je učinkovita metoda za izboljšanje varnostnega okolja organizacije. Opozarja na grožnje, ki lahko ogrozijo podatke in zasebnost procesov ter transakcij podjetja.

– Menedžment varovanja

Po neuradni klasifikaciji poklicev lahko rečemo, da obstajajo 3 vrste menedžmenta varovanja: 1. državni menedžment (vojaški, policijski, inšpekcijski, kriminalistični, upravni, pravosodni itd.); 2. menedžment varovanja v varnostnih podjetjih in 3. menedžment varovanja v gospodarskih organizacijah.

– Menedžment varovanja v gospodarskih organizacijah

V gospodarskih organizacijah in javnih ustanovah fizično predstavlja menedžment varovanja varnostni menedžer. Varnostnemu menedžerju vodstvo podjetja delegira kompetence za vodenje naslednjih služb: službe varovanja, službe za varnost in zdravje pri delu in varstvo pred požari, službe informatike, službe za zaščito osebnih in tajnih podatkov in poslovnih skrivnosti, službe za zaščito in varovanje itd. Glavni menedžer varovanja je oseba, ki ji top menedžment delegira kompetence in odgovornost za upravljanje celovitega sistema varovanja.

Lastnosti varnostnega menedžerja so odgovornost, zakonitost, strokovnost in učinkovitost varovanja (»ZZasV«, 2011). Njegovo delo je predvsem doseganje ciljev, ki jih je zastavila organizacija. Uresničevati mora cilje vrednot, ki so določene za organizacijo. Njegova naloga je varovanje organizacije; vzpostavitev okoliščin, s katerimi se doseže maksimalna varnost pri delu; doseganje ciljev organizacije in vzdrževanj varnega okolja ter varnosti zaposlenih (Stankovski, 2012).

Varnostni sistem, ki ga je vzpostavil varnostni menedžer, mora omogočiti nadzor nad varnostnimi tveganji, saj je tveganje na takšen način nevtralizirano, preprečeno in predvideno. Prav tako mora analizirati organizacijsko strukturo in poiskati slabosti ter pomanjkljivost, ki lahko ogrozijo organizacijo. Sama priprava na tveganja pomeni oblikovanje varnostnih postopkov, v katerih so vključeni ukrepi za preprečevanje varnostnih tveganj (Sapiński idr., 2020).

Vloga lastnikov in menedžerjev je tudi kvalitativno in kvantitativno merjenje tveganja v notranjem in zunanjem okolju podjetja; obvladovanje stroškov skozi celotni poslovni proces; obvladovanje metod prenosa tveganj na druge nosilce po vrstah in s tem optimalno

zavarovanje poslov; zagotavljanje nadzora nad poslovnim procesom ter zaostritev notranje odgovornosti za poslovne dogodke (preglednost nadzora nad odločanjem in zaostritev osebne odgovornosti) in za druge dogodke, ki so povezani z vodenjem ljudi; graditev take organizacijske strukture, ki bi bila optimalno v funkciji nadzora nad dogodki v celotnem poslovnem procesu; doseganje zanesljive sinergije v celotnem poslovnem sistemu (Stankovski, 2012).

– Odgovornost menedžerja

Odgovornost menedžerjev je dobro vodenje, kar je ključ do uspešnosti in učinkovitosti organizacije. Za to mora imeti dobro razvit razum in logiko, s pomočjo katerih so mu svet in zakoni lažje razumljivi. Poleg tega mora imeti tudi dobro razvito čustveno inteligenco, s pomočjo katere se lažje spopada s stresnimi situacijami in lažje navezuje stike, spodbuja zaposlene, predvidi situacije, komunicira in podobno. Je tudi bolj odprt in dostopen (Sapiński idr., 2020).

Težavo oziroma moralni konflikt pri odgovornosti menedžerja predstavljajo situacije, v katerih se mora ta odločiti med dvema vsaj navidez slabima izbirama oziroma kadar se pojavijo večplastne etične odločitve, ki so pogosto v medsebojnem konfliktu interesov (Vadnjal, 2014). Odločitve menedžerjev lahko po mnenju Vadnjala (2014) razdelimo na štiri sklope:

- Pravice in dolžnosti: pravila, ki so na nacionalni ravni v obliki zakonov in predpisov.
- Utilitarianizem: usmeritev, da je odločitev najbolj ugodna. Analiza stroškov in koristi.
- Pravičnost: obravnava vseh, ki jih bo odločitev doletela enakopravno in jim dati enake možnosti.
- Čuvanje povezav: koncept, kako odločitve vplivajo na odnose med posameznimi skupinami oziroma obratno.

Pomembno je, da se menedžerji in lastniki organizacij oprimejo načel in meril profesionalne etike upravljanja, vodenja, poslovanja in odgovornosti. Osrednje načelo je, da le-ti organizaciji ne škodujejo namerno. Upoštevati je treba, da se menedžerji in lastniki pri sprejemanju težkih odločitev držijo svojih ključnih vrednot in s tem poskušajo objektivno ter na pošten način pokazati skrb za družbo, organizacijo in celotni sistem (Vadnjal, 2014).

Korporativni varnostni menedžer je enakopravni partner pri vodenju ter upravljanju organizacije in s tem izredno pomemben člen. Njegove naloge so poleg zgoraj omenjenih tudi: soodgovornost za strateško odločanje ter upravljanje; upravljanje sprememb v organizaciji na podlagi graditve zaupanja, varnostne kulture, močne socialne mreže, medsebojne povezanosti ter učenja; zagotavljanje tesnega sodelovanja osnovnih in podpornih poslovnih procesov v organizaciji z namenom zagotavljanja varnosti premoženja, reda, zaščite ter neprekinjenega poslovanja; izvajanje dolžnostnega nadzorstva nad delom v organizaciji; prepričevanje drugih v organizaciji, da je zagotavljanje varnosti sestavni del opravljanja njihovih del; izobraževanje; vodenje delovnih skupin; načrtovanje ukrepov in podobno (Gostič, 2014).

Poleg tega je izredno pomembno, da se sam menedžment in lastniki zavedajo, da je vloga varnostnega menedžerja izredno pomembna, zato je bistvenega pomena, da poskrbijo za izobraženega, profesionalnega in prodornega menedžerja za vodenje varnostne službe, saj le-ta pripomore k ohranjanju ter zviševanju vrednosti premoženja, ustvarjanju dobička, izkazovanju integritete in družbene odgovornosti, pospeševanju prodaje, nemotenemu delovanju in ugledu organizacije (Gostič, 2014). Glede na njegovo pomembnost bi moral biti varnostni menedžer odgovoren neposredno upravi organizacije oziroma samemu predsedniku uprave (Dvojmoč, 2017a).

– Krizni menedžment

Krizni menedžment je relativno nova veda in pomeni upravljanje podjetja v okoliščinah, ko se je zaradi nepričakovanega večjega dogodka pojavila grožnja, ki lahko oškoduje in prizadene podjetje, zaposlene, lastnike ter druge deležnike, vključno s širšo družbeno skupnostjo (Dvojmoč, 2020).

Prav tako je vnaprej imenovan krizni štab, ki ima funkcijo načrtovanja in izvajanja ukrepov za pripravljenost, preprečevanje, odzivanje in sanacijo pred in med pojavom ter po pojavu izrednega dogodka. Naloge kriznega štaba: zagotavljanje informacij za vodenje, postavljanje mehanizmov za zgodnje odkrivanje simptomov krize, priprava kriznih scenarijev, priprava specialistov in tehnoloških sredstev, strateško načrtovanje dejavnosti za vzpostavitev prvotnega stanja in podobno (Gostič, 2014).

Krizno načrtovanje: Lahko ga členimo na načrtovanje neprekinjenega poslovanja oz. načrtovanje poslovanja ob nesreči, načrtovanje takojšnjega odziva na nesrečo in načrtovanje ponovne vzpostavitve poslovnih procesov in podobno, kar predstavlja celovitost kriznega menedžmenta.

– Reševanje sporov

Konflikti in spori so del vsakdana, zato je pomembno, kako se z njimi spopadamo in jih rešujemo. Reševanje sporov je zelo pomemben dejavnik tudi pri uspešnosti samega podjetja oziroma organizacije.

V delovnem okolju poznamo različne vrste konfliktov.

- Osebnostni konflikti so spori, do katerih pride zaradi različnih osebnostnih tipov zaposlenih in so najpogostejši. Koristno je, da se zaposleni naučijo sodelovati med seboj, saj imajo različni ljudje različne pristope in perspektive.
- Medsebojno odvisni konflikti na podlagi skupnih nalog predstavljajo spore, do katerih pride, ko se različni oddelki v organizaciji pozabijo obvestiti o pomembnih dogodkih, podatkih in obvestilih, kar lahko privede do konfliktov. Pri tem je izredno pomembna komunikacija.
- Konflikti, ki temeljijo na slogu, so spori, do katerih pride zaradi različnih slogov opravljanja dela, ki jih imajo ljudje. Pomembno je, da se nadrejeni tega zavedajo in so na to pripravljeni ter pri skupinskih sodelovanjih uporabljajo različne strategije.
- Konflikti stilov vodenja so spori, do katerih pride zaradi različnih stilov vodenja. Pri tem je pomembno, da se vodja tega zaveda in da svojim zaposlenim vseeno zna sporočiti, kako najbolje sodelovati (Bizjak, 2022).

Pri reševanju sporov so pomembni pristopi, s katerimi menedžer ali vodja poskuša rešiti nastalo situacijo. Najprej je treba priti do temeljnega vzroka za spor. Pri tem mora vodja dovoliti vsaki strani, da deli svojo plat zgodbe, pri čemer je pomembno, da se pridobi čim več informacij in da je vodja pri tem nevtralni mediator. Za reševanje konfliktov si je treba vzeti čas. Najboljše je, če vodja skliče sestanek, pri čemer ga določi v terminu, do katerega imata obe strani možnost, da se na to pripravita. Priporočljivo je, da je lokacija srečanja oz. pogovora nevtralna, tako da je okolje udobno za vse. Po tem, ko vodja sliši obe strani, mora pomagati vpletenim in najti rešitve ter naslednje korake, s katerimi se strinjata obe strani. Določiti je treba medsebojno dogovorjeno rešitev, pri čemer morajo vse osebe razumeti, kaj se od njih pričakuje in katere korake morajo sprejeti. Če rešitve ni mogoče doseči, mora vodja pomoč poiskati pri za to usposobljenih svetovalnih strokovnjakih (Bizjak, 2022).

14.5 Standardizacija varnosti

14.5.1 Mednarodna, evropska in slovenska standardizacija

Standardi tehničnega varovanja gospodarsko-poslovnih objektov so standardi, ki zmanjšujejo pogoje za kriminalne napade. Sprejeti so standardi s področja vlomnega odkrivanja in javljanja; požarnega odkrivanja in javljanja ter mehanskega varovanja.

– **Standard SIST EN ISO 9001:2000**

Glavni deli standarda so: sistem vodenja kakovosti, odgovornost vodstva, merjenje, analize in izboljševanje, realizacija proizvoda ter vodenje virov.

Uvajanje standarda ISO 9001 pomeni: določiti politiko in cilje kakovosti; identificirati in določiti ključne procese za doseganje ciljev; določiti in uporabiti merila za ocenjevanje uspešnosti procesov glede na cilj; iskati priložnosti za izboljševanje uspešnosti, učinkovitosti in poenostavitev procesov; določiti metode za preprečevanje napak, zmanjševati neskladnosti in zmanjševati delo ter stroške zaradi napak; nadzorovati učinkovitost izboljšav; ocenjevati rezultate glede na planirane rezultate. Pomeni tudi, da je sistem vodenja prožen; temelji na procesu in ne na postopkih; spodbuja nenehno izboljševanje; vidi v zadovoljstvu odjemalca merilo za uspešnost sistema; vsakogar motivira s skupnim ciljem in zagotavlja sodelovanje; v širokem obsegu vključuje najvišje vodstvo, saj poslovne odličnosti ni mogoče delegirati; se navezuje na zakonske in regulativne zahteve; zahteva postavitev izmerljivih ciljev na različnih ravneh sistema; se osredotoči na učinkovito notranje komuniciranje; usmerja pozornost na razpoložljive vire; zahteva vrednotenje učinkovitosti usposabljanja in vodenja kakovosti (Dvojmoč, 2020).

– **Standard BS 7799**

Osnovni cilj standarda je zagotavljanje: *zaupnosti* – občutljive informacije so dostopne samo pooblaščenim uporabnikom, *celovitosti* – informacije oz. druge dobrine informacijskega sistema niso bile nepooblaščeno spremenjene; informacije kakor tudi postopki za njihovo obdelavo so točni in popolni; *razpoložljivosti* – informacije oziroma druge dobrine informacijskega sistema so dostopne pooblaščenim uporabnikom, kjer koli in kadar koli jih ti potrebujejo. Standard temelji na principu PDCA, ki pomeni *Plan* – Načrtuj, *Do* – Izvedi, *Check* – Preveri, *Act* – Ukrepaj. Njegove koristi so celovito pokrivanje področja zagotavljanja informacijske varnosti; neprestano izboljševanje ravni informacijske varnosti na podlagi nepristranskega merjenja; zmanjševanje verjetnosti za

uresničitev groženj varnosti in/ali ublažitev posledic, ki jih te lahko povzročijo; povečanje ugleda organizacije, zaupanja poslovnih partnerjev in strank; povečanje konkurenčnosti; pripravljenost na bodoče zahteve zakonodajalca ali poslovnih partnerjev (Dvojmoč, 2020).

– Standard ISO/PAS 28001:2006

Standard ISO/PAS 28001:2006 uveljavlja zahteve in smernice za subjekte, ki sodelujejo v mednarodnih logističnih verigah, in sicer: razvijanje in uporabo varnostnih procesov v logističnih verigah; vzpostavljanje in dokumentiranje minimalne stopnje varnosti znotraj verige ali njenem delu; podporo prosilcem pooblaščenega gospodarskega subjekta pri izpolnjevanju meril v okviru svetovne carinske organizacije in prilagajanju nacionalnih programov varnosti logističnih verig. Rezultati uporabe določil standarda so izdelava varnostnega načrta z opisom ukrepov, namenjenih upravljanju z obstoječimi varnostnimi tveganji; določitev meja v logistični verigi in okoli nje, ki morajo biti zajete z varnostnim načrtom; varnostna ocena, ki opredeljuje tveganja in ranljivosti logistične verige, določa tudi scenarije postopanja, če bi se katero od tveganj uresničilo; načrt usposabljanja osebja v logistični verigi je izdelan tako, da zaposleni poznajo svoje naloge v zvezi z varnostjo (Dvojmoč, 2020).

Odgovorite na vprašanja

Kaj je poslovna skrivnost?

Kako se lahko zaščitijo poslovne skrivnosti?

Zakaj je »Zakon o poslovni skrivnosti (ZPosS)« (2019) pomemben?

Katere podsisteme mora vključevati celovit sistem varovanja poslovne skrivnosti? Naštejte in vsakega na kratko predstavite/opišite.

Na katere načine je poslovna skrivnost lahko ogrožena? Pojasnite.

Kaj spada pod intelektualno lastnino?

Zakaj je zaščita intelektualne lastnine pomembna? Pojasnite.

Razmislite in zapišite, kaj lahko pomeni izguba podatkov za organizacijo?

Na katere načine se preprečuje izguba podatkov?

S katerim zakonom je urejeno področje izgube podatkov v Sloveniji in kaj določa?

Kaj je varnostno svetovanje in kaj se z njim zagotavlja? Pojasnite.

Katere vrste menedžmenta varovanja poznamo? Naštejte in vsako na kratko predstavite.

Katere odgovornosti ima menedžer?

Kaj je krizni menedžment?

Katero funkcijo ima krizni štab?

Kako v organizaciji poteka reševanje sporov?

Kaj je pri reševanju sporov pomembno? Razmislite in zapišite.

Predstavite standarde tehničnega varovanja gospodarsko-poslovnih objektov in jih na kratko predstavite.

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

15 Posebne teme korporativne varnosti

Pri samem upravljanju korporativne varnosti v podjetju in organizaciji je zelo pomembno tudi sodelovanje med oddelki in zunanjimi partnerji. Konvergenčna obravnava organizacijskih tveganj in groženj je učinkovitejša kot reševanje fizičnih in informacijskih sistemov, če se le-to rešuje ločeno, saj so meje pogosto nejasne. Ločevanje oddelkov za korporativno varnost od drugih lahko za organizacijo predstavlja oviro ali celo grožnjo (Schneller idr., 2022).

15.1 Vloga policije in drugih pravosodnih organov

Sodelovanje policije s subjekti, ki zagotavljajo korporativno varnost, je zelo pomembno predvsem pri učinkovitejšem obvladovanju varnostnih tveganj. Tudi »Zakon o organiziranosti in delu policije (ZODPol)« (2013) več pozornosti namenja partnerskemu sodelovanju policije z drugimi subjekti. Razlog za to je predvsem zagotavljanje večje varnosti (Veniger, 2013).

Tako med seboj sodelujejo policija, organi lokalne skupnosti, organizacije in institucije, civilna družba in drugi organi, katerih dejavnost je usmerjena k spodbujanju samozaščitnega ravnanja in varnostnega samoorganiziranja ter pomoči. Spodbujajo se tudi skupno preprečevanje varnostne problematike, odkrivanje in odstranjevanje vzrokov ter pogojev za nastanek kaznivih dejanj. Sodelovanja med različnimi organi in organizacijami so ključni element pri zagotavljanju javne varnosti (Veniger, 2013).

Policija deluje tudi v sodelovanju z zasebnovarnostnimi podjetji, kamor spada tudi detektivska dejavnost. V Sloveniji v »pluralno policijsko družino« uvrščamo policiste, zasebne varnostnike, carinike, pravosodne policiste, občinske redarje in detektive (Modic idr., 2014). V primerjavi z državno oz. javno policijsko dejavnostjo je zasebno varovanje deležno veliko manj pozornosti (Dvojmoč idr., 2020).

Pomemben dogodek, pri katerem lahko izpostavimo delovanje zasebnovarnostnih podjetij in korporativne varnosti, je bilo omejevanje epidemije covida-19. Kot je bilo že omenjeno, se korporativna varnost zagotavlja tudi z zasebnimi varnostniki in detektivi, zato je v času epidemije potreba po ustreznem usposabljanju zasebnovarnostnega osebja in s tem tudi korporativnih menedžerjev narasla. Omenili smo tudi, da zasebno varovanje lahko poteka v obliki pogodbenega varovanja ali kot interno varovanje oziroma varovanje za lastne potrebe. Zasebnovarnostna podjetja varujejo različne naročnike, med katere spadajo tudi državni organi in ustanove, zasebni gospodarski subjekti in zasebniki posamezniki. Pri varovanju gospodarskih subjektov se podjetje sreča s korporativno varnostjo. S tem se vzpostavi njuna soodvisnost, sodelovanje in součinkovanje pri zagotavljanju varnosti. V času epidemije smo tako opazili, da so zasebni varnostniki prevzeli pomembno vlogo pri zagotavljanju varnosti v najbolj izpostavljenih dejavnostih, kot so na primer zdravstvene ustanove, banke, trgovine, in tudi v gospodarskih subjektih, da so ti lahko nemoteno poslovali in delovali. Zaradi tega se je morala reorganizirati tudi funkcija korporativne varnosti predvsem tam, kjer je šlo za kritično infrastrukturo, ki mora nemoteno in neprekinjeno delovati v kakršni koli situaciji. Na podlagi tega lahko povzamemo, da so varnostni menedžerji zasebne varnosti in menedžerji korporativne varnosti delovali usklajeno, saj je bil njihov skupni cilj neprekinjeno delovanje gospodarskih subjektov in izvajanje varnostnih funkcij v njih (Sotlar in Dvojmoč, 2021).

15.2 Sodelovanje z varnostnimi svetovalci

Večina menedžerjev za varnost in preprečevanje izgub je zelo usposobljenih za opravljanje svojega dela. Mnogi imajo dolgoletne izkušnje v organih kazenskega pregona ali vojski in se imajo za strokovnjake za varnostne zadeve. Ti varnostni menedžerji pogosto nočejo privabiti zunanjega varnostnega svetovalca, pri čemer pogosto navajajo naslednje razloge (Silva Consultants, 2023):

»Nihče ni bolj seznanjen z varnostnimi potrebami mojega podjetja kot jaz – ni možnosti, da bi mi zunanji svetovalec povedal kar koli, česar še ne vem.«

»Jaz naj bi bil varnostni strokovnjak podjetja. Ali ne bo moj šef mislil, da sem nesposoben, če bom prosil za pomoč od zunaj?«

»Svetovalci so dragi – ne moremo si privoščiti, da bi ga najeli, ne glede na naš varnostni proračun.«

Nenaklonjenost varnostnega menedžerja uporabi zunanje pomoči je zanimiva glede na to, da večina praktikov v vseh drugih poklicih redno uporablja svetovalce za zagotavljanje specializiranega strokovnega znanja ali podajanje zunanjega mnenja. Na primer, zdravniki skoraj vedno privabijo druge strokovnjake, kot so radiologi, hematologi in drugi specialisti, ko bolnikovo stanje to upravičuje, in niti v sanjah ne bi poskušali vsega narediti sami. Podobno najbolje ocenjeni odvetniki skoraj vedno privabijo druge odvetnike s posebnim strokovnim znanjem, ko začnejo soditi zapletene pravne zadeve (Silva Consultants, 2023).

Prednosti, ki jih varnostni svetovalec doprinese organizaciji, so naslednje (Matryx, 2023):

- Varnostni svetovalec bo strokovnjak za osebno varnost vaše organizacije, nekdo, s katerim se lahko zaupno pogovorite o svojih poslovnih operacijah in zahtevah na visoki ravni.
- Svoje podjetje poznate bolje kot kdor koli. Varnostni svetovalec si bo vzel čas, da bo razumel vaše poslovanje in morebitna tveganja za vaše ljudi in lastnino. Prepoznali in opredelili bodo vaše tveganje ter najboljše načine za njegovo ublažitev.
- Varnostni svetovalec bo ocenil vse vaše obstoječe operacijske sisteme in poslovne procese, da bi ugotovil, ali je tisto, kar imate, primerno za vaše trenutno poslovno okolje. Pregled bi moral oceniti dostop do stavbe, pošto in komunikacije, upravljanje v sili, nadzor dostopa in alarmne sisteme, CCTV in sisteme za upravljanje stavbe ter vse druge spremenljivke, specifične za primer.
- Ko je poslovno tveganje ugotovljeno, ga je treba opredeliti s finančnega vidika, to bo vaš svetovalec naredil za vas. Ko je to končano, je mogoče sprejemati kvalificirane odločitve o strategijah za zmanjševanje tveganja. Tu pridejo v poštev izkušnje varnostnega svetovalca, saj pozna posledice slabih strategij, tveganj in rezultatov, do katerih lahko pride ob odsotnosti svetovalca v podjetju.
- Dobra varnost izhaja iz kombinacije sistemov in procesov, ki delujejo v harmoniji. Resnično neodvisni svetovalec ne bo priporočal izdelka ali storitve, pri nakupu katere prejme podkupnine ali provizije, priporočil bo izdelke in storitve, ki bodo dali najboljše rezultate za njihovo stranko.

- S poznavanjem vašega podjetja in morebitnega poslovnega tveganja bo varnostni svetovalec zaščitil vaš rezultat. O izdatkih za varnost se redko razmišlja kot o naložbi, ki se bo vašemu podjetju povrnila, vendar s tehnološko učinkovitostjo ne boste uživali le v izboljšavah varnosti, temveč boste lahko videli tudi, da se bodo vaše varnostne nadgradnje sčasoma povrnile.
- Če zapravljate denar za nove varnostne tehnologije, bo varnostni svetovalec poskrbel, da boste dobili tisto, kar ste plačali. Vaš varnostni svetovalec bo prevzel odgovornost za podpis vseh kapitalskih nakupov, tako da boste lahko brez skrbi, da vam ne prodajajo slabših, napačnih ali neprimernih izdelkov. To ščiti vašo naložbo in zagotavlja raven odgovornosti do tistih, ki so zadolženi za delo za vas.
- Varnostnega svetovalca skrbijo le vaši interesi. Naredite si uslugo tako, da nekdo drug – strokovnjak – premisli o varnosti vašega podjetja. (Matryx, 2023)

15.3 Pomen mednarodnega sodelovanja v korporativni varnosti

Mednarodno sodelovanje je v zadnjih letih pomembno predvsem pri ukrepanju zoper digitalne napade in kibernetsko kriminaliteto ter grožnje. Potreba po globalnem sodelovanju za spopadanje z različnimi perečimi grožnjami, od elektronskega vohunjenja do napadov z izsiljevalsko programsko opremo na kritično infrastrukturo, je nujna za preprečevanje gospodarskih in družbenih katastrof, kot navajajo vrhunski strokovnjaki za kibernetsko varnost in vladni uradniki (Brumfield, 2022).

Skoraj popolna digitalizacija vseh vidikov družbe, ki izpostavlja skoraj vse storitve javnega in zasebnega sektorja naraščajočim kibernetskim grožnjam, narekuje močnejšo, kolektivno obrambo. Poleg tega, ko se kibernetska tveganja stopnjujejo in množijo, vlade po vsem svetu krepijo lastna neodvisna prizadevanja za zaščito pred naraščajočim valom digitalnih groženj (Brumfield, 2022).

Odgovorite na vprašanja

Zakaj je sodelovanje z zunanjimi varnostnimi organi pomembno?

Predstavite vlogo policije in drugih sodnih organov.

Pojasnite sodelovanje z zasebnovarnostnimi podjetji.

Kdo so varnostni svetovalci in zakaj je sodelovanje z njimi pomembno?

Kakšne prednosti predstavlja varnostni svetovalec za organizacijo?

Kako mednarodno sodelovanje vpliva na korporativno varnost?

ZAPISKI

Univerzitetna založba
Univerze v Mariboru

Literatura

Abdullah, M., Shukor, Z. A. in Rahmat, M. M. (2017). The influences of risk management committee and audit committee towards voluntary risk management disclosure. *Journal pengurusan, 50*, 83–95.

Akasaka, Y. (2023). External threats: The definitive guide to detection and remediation. *Flare.* https://flare.io/learn/resources/blog/external-threats/

Al-Fedaghi, S. in Alsumait, O. (2019). Towards a conceptual foundation for physical security: Case study of an it department. *International Journal of Safety and Security Engineering, 9*(2), 137–156.

Andales, J. (2023). Risk assessment. *Safety Culture.* https://safetyculture.com/topics/risk-assessment/

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308–313.

Anžič, A. (1997). *Varnostni sistem Republike Slovenije.* Uradni list Republike Slovenije.

Arain, M. A., Tarraf, R. in Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare*, *12,* 73–81. doi: https://doi.org/10.2147/JMDH.S183275

Arion, S. (2010). 21st century security manager. *Annals of the Academy of romanian scientists, 2*(2), 65–76.

Ashenden, D. (2008). Information security management: A human challenge? *Information security technical report, 13*(4), 195–201.

Baldwin, A. D. (2001). *The concept of security*. Cambridge University Press.

Barney, N. (2023). Crisis management plan (CMP). *Tech Target.* https://www.techtarget.com/searchdisasterrecovery/definition/crisis-management-plan-CMP

Bdc. (n. d.). *Phishing, malware and online pop-ups: 8 major technology security risks for your business.* https://www.bdc.ca/en/articles-tools/technology/invest-technology/phishing-malware-online-pop-ups-8-major-technology-security-risks-business

Belič, I. in Lesjak, B. (2006). Varovanje informacijskih sistemov pred kriminalnimi napadi. V A. Dvoršek in L. Selinšek (ur.), *Kriminalni napadi na premoženje gospodarskih subjektov (varnostni, pravni in zavarovalni vidik)* (str. 117–128). Pravna fakulteta in Fakulteta za policijsko-varnostne vede.

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Bizjak, J. (2022). Konflikti v podjetju in kako jih razrešiti. *Svet kapitala.* https://svetkapitala.delo.si/b2b/konflikti-v-podjetju-in-kako-jih-razresiti/

Breznik, M. (2012). Za učinkovito zaščito pred vlomilci ni dovolj le mehansko varovanje. *Revija Varnost, 60*(3), 27–31.

British Safety Council. (2023). *What is a risk assessment?*. https://www.britsafe.org/training-and-learning/informational-resources/risk-assessments-what-they-are-why-they-re-important-and-how-to-complete-them

Britovšek, J. (2019). Predlog modela ocen ogroženosti in ocen tveganj za področje obveščevalnovarnostne dejavnosti v Republiki Sloveniji. *Varstvoslovje*, 21(1), 73–86.

Britovšek, J., Tičar, B. in Sotlar, A. (2017). Private intelligence in the Republic of Slovenia: Theoretical, legal, and practical aspects. *Security Journal, 31*(2), 410–427.

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. *Security Journal, 23*(3), 225–239. https://link.springer.com/article/10.1057/sj.2008.18

Brumfield, C. (2022). *International cooperation is key to fighting threat actors and cybercrime.* CSO. https://www.csoonline.com/article/573649/international-cooperation-is-key-to-fighting-threat-actors-and-cybercrime.html

Buckbee, M. (2015). How to create a good security policy. *Varonis.* https://www.varonis.com/blog/how-to-create-a-good-security-policy

Button, M. (2014). Foreword. V K. Walby in R. K. Lippert (ur.), *Corporate security in the 21st century* (str. VIII–IX). Palgrave Macmillan.
Cabric, M. (2015). *Corporate security management: challenges, risks, and strategies*. Butterworth-Heinemann. https://dl.acm.org/doi/pdf/10.5555/2843502
Cassidy, A. K. (2021). Corporate security. V L. R. Shapiro in M. H. Maras (ur.), *Encyclopedia of security and emergency management* (str. 67–73). Springer.
Castagna, R. (n. d.). *3-2-1 backup strategy*. TechTarget. https://www.techtarget.com/searchdatabackup/definition/3-2-1-Backup-Strategy
CFI Team. (2023). *Transaction risk*. CFI. https://corporatefinanceinstitute.com/resources/valuation/transaction-risk/
CG Team. (2023). *Six strategies for fraud prevention in your business*. https://www.cgteam.com/six-strategies-for-fraud-prevention-in-your-business/
Chan, B. S. B. (2014). A human rights debate on physical security, political liberty, and the confucian tradition. *Dao, 13*(4), 567–588. https://link.springer.com/article/10.1007/s11712-014-9403-0
Chang, S. E. in Lin, C.-S. (2017). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438–458. https://doi.org/10.1108/02635570710734316
Christiánm L. in Sotlar, A. (2018). Private Security Regulation in Hungary and Slovenia – A Comparative Study Based on Legislation and Societal Foundations. *Varstvoslovje, 20*(2), 143 – 162.
Concentra. (2023). *Occupational medicine*. https://www.concentra.com/occupational-health/occupational-medicine/
Coole, M. P. in Brooks D. J. (2021). Physical security: best practices. V V L. R. Shapiro in M. H. Maras (ur.), *Encyclopedia of security and emergency management* (str. 730–737). Springer.
Cubbage, C. J. in Brooks, D. J. (2012). *Corporate security in the Asia-Pacific region: Crisis, crime, fraud, and misconduct*. CRC Press.
Čaleta, D. (2005). Varovanje poslovne tajnosti – priložnost za zasebno varnostne subjekte. V B. Lobnikar (ur.), *Zbornik prispevkov. 6. Slovenski dnevi varstvoslovja, Bled, 2.-4. junij 2005*. Fakulteta za policijsko-varnostne vede.
Čaleta, D. (2011). *Varnost mojega podjetja*. Podjetnik. http://www.podjetnik.si/clanek/varnost-mojega-podjetja-20110710
Čaleta, D. (2017). *Korporativna varnost – intervju*. Podjetnik.net. https://podjetnik.aktualno.si/korporativna-varnost-dr-denis-caleta-intervju/
Čaleta, D. (2018). Korporativna varnost je še v iskanju ustreznega mesta v poslovnem svetu. *Korporativna varnost*, 17, 5–8.
Čas – Zasebna šola za varnostno izobraževanje. (n. d.). *Varnostno svetovanje*. https://www.varnostnoizobrazevanje-cas.si/sl/content/svetovanje-in-izvedenstvo/varnostno-svetovanje.html
Čas, T. (2006). *Zasebno varovanje za uporabnike varnostnih storitev*. Atelje Kresnik.
Čeč, F. (2020). Učinkovito vodenje zdravstvene organizacije v času koronavirusa. *HR&M: strokovna revija za področje razvoja organizacij in vodenja ljudi pri delu* , *6*(28), 47–48. https://www.hrm-revija.si/ucinkovito-vodenje-zdravstvene-organizacije-vcasu-koronavirusa
Črnčec, D. (2009). *Obveščevalna dejavnost v informacijski dobi*. Defensor.
Data d.o.o. (2018). *Obveznosti zaposlenih – jih poznate?*. https://data.si/blog/obveznosti-zaposlenih-jih-poznate/
Data d.o.o. (2023). *Varstvo pri delu – kakšne so obveznosti delodajalcev?*. https://data.si/blog/varstvo-pri-delu/
Datalab. (23. 3. 2022). *Varnost programa in preprečevanje napadov*. https://www.datalab.si/blog/varnost-poslovnega-programa-in-preprecevanje-kibernetskih-napadov/
Davis, M. (2023). Identifying and managing business risks. V *Investopedia*. https://www.investopedia.com/articles/financial-theory/09/risk-management-business.asp
De Visser, S. (1. 11. 2022). 17 Actionable fraud prevention tips for your financial institution. *FPS Gold*. https://www.fpsgold.com/blog/fraud-prevention-for-financial-institutions
Direktiva z dne 12. junija 1989 o uvajanju ukrepov za spodbujanje izboljšav varnosti in zdravja delavcev pri delu (89/391/EGS). (1989). *Uradni list,* (L 183). https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:31989L0391
Dobrovoljc, A. (2018). Odkrivanje potencialnih groženj za informacijski sistem. *Revija za univerzalno odličnost, 7*(4), 334–346.
Dombora, S. (2016). *Characteristics of information security implementation methods*. Obuda University. https://kgk.uniobuda.hu/sites/default/files/04_Dombora.pdf
Drata. (2023a). *Semi-Quantitative risk assessment*. https://drata.com/glossary/semi-quantitative-risk-assessment
Drata. (2023b). *Vulnerability-Based risk assesment*. https://drata.com/glossary/vulnerability-based-risk-assessment

Dublino, J. (2. 11. 2023). Does your business need a code of ethics or conduct? *B.* https://www.business.com/articles/does-your-business-need-a-code-of-ethics-or-conduct/

Duigan, A. (8. 10. 2003). 10 steps to successful security policy. *Computerworld.* https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html

Duplain, R. (2023). Understanding, writing, & communicating crisis management plans. *Podium.* https://www.podium.com/article/crisis-management-plan/

Duvnjak, N. (2004). Fizičko-tehnička zaštita organizacija u službi obezbeđenja. *Defendologija, 7*(15–16), 55–61.

Dvojmoč, M. (2017a). Integralna korporativna varnost. *Varstvoslovje, 19*(3), 252–272.

Dvojmoč, M. (2017b). Detektivska dejavnost v Sloveniji – (normativen) razvoj dejavnosti in pogled v prihodnost. *Revija za kriminalistiko in kriminologijo, 68*(3), 280–297.

Dvojmoč, M. (2019). Korporativna obveščevalna dejavnost kot nova realnost: nujnost korporativne varnosti v sodobnem globalnem podjetništvu. *Varstvoslovje*, *21*(2), 205–223.

Dvojmoč, M. (2020). *Integralna korporativna varnost: 2. letnik: magistrski študijski program Varstvoslovje: zbrano študijsko gradivo.* Fakulteta za varnostne vede.

Dvojmoč, M. (2021). Corporate intelligence as the new reality: The necessity of corporate security in modern global business. *Varstvoslovje*, *21*(2), 205–223. https://www.fvv.um.si/rv/arhiv/2019-2/06_Dvojmoc_rV_2019-2.pdf

Dvojmoč, M. in Sotlar, A. (2018). Profesionalizacija zasebnega varstva v Sloveniji. *Varstvoslovje, 20*(3), 358–380.

Dvojmoč, M., Lobnikar, B., Sotlar, A. in Prislan, K. (2020). *CRP: Primerjava ureditve dejavnosti zasebnovarnostnih subjektov v Sloveniji in državah članicah EU*. Fakulteta za varnostne vede.

Fakiha, B. (2021). Business organization security strategies to cyber security threats. *International Journal of Safety and Security Engineering, 11*(1), 101–104. https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.110111

Farooq, M., Waseem, M. K. in Sadia, M. (2015). Critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*(7). doi: 10.5120/19547-1280

Fefer, D. (2013). *Sistemi tehničnega varovanja*. Zbornica za razvoj slovenskega zasebnega varovanja.

Fermin, J. (2023). What to include in your company's code of ethics. *Allvoices.* https://www.allvoices.co/blog/what-is-code-of-ethics

Finance PR. (21. 5. 2019). Pomembna novost, ki jo za podjetja uvaja novi Zakon o poslovni skrivnosti. *Finance.* https://www.finance.si/8948239?cctest

Frandsen, F. in Johansen W. (2017). Strategic communication. V C. R. Scott in L. Lewis (ur.), *The international encyclopedia of organizational communication*. https://doi.org/10.1002/9781118955567.wbieoc194

Georgescu, E. (2023). *Internal threats: A major risk to any business*. Heimdal. https://heimdalsecurity.com/blog/internal-threats/

Gerginova, T. (2016). Role of corporate security. V G. Meško in B. Lobnikar (ur.), *Criminal justice and security in Central and Eastern Europe: Safety, security, and social control in local communities: Conference proceedings* (str. 490–497). Faculty of Criminal Justice and Security.

Gerginova, T. (2018). Policy for Effective Realization of Corporate Security. V. G. Meško, B. Lobnikar, K. Prislan in R. Hacin (ur.), *Criminal Justice and Security in Central and Eastern Europe: From Common Sense to Evidence-based Policy-making* (str. 381–392). Faculty of Criminal Justice and Security.

Gill, R. (2023). *Whait is Open-Source Intelligence*?. SANS. *https://www.sans.org/blog/what-is-open-source-intelligence/*

Golob, R. (2013). *Varnostni sistem – Ocena varnostnih tveganj in varnostni ukrepi*. Samozaložba.

Gospodarska zbornica Slovenije. (n. d.). *Zakaj ščititi intelektualno lastnino?* https://www.gzs.si/skupne_naloge/inovativna_slovenija/vsebina/Intelektualna-lastnina/zakaj-scititi-intelektualno-lastnino

Gostič, Š. (2008). Osnovni principi organizacije korporativne varnosti. V J. Šifrer (ur.), *Javna in zasebna varnost: zbornik prispevkov, 9. slovenski dnevi varstvoslovja, Bled, 5. in 6. junij 2008*. Fakulteta za varnostne vede.

Gostič, Š. (2014). Odgovornost korporativno varnostnega menedžerja. *Korporativna varnost,* (9), 16–19.

Graham, J., Howard, R. in Olson, R. (2011). *Cyber security essentials*. Taylor and Francis Group.

Gupta, R. in Agarwal, S. P. (2017). A comparative study of cyber threats in emerging economies. *Globus: An International Journal of Management & IT: A Refereed Research Journal, 8*(2), 24–28.

Haimes, Y. Y. (2009). On the complex definition of risk: A systems-based approach. *Risk Analysis: An International Journal, 29*(12), 1647–1654.

Hajtnik, T. (21. 12. 2020). *Fizično in tehnično varovanje prostorov, opreme in gradiva kot eden od vidikov zagotavljanja informacijske varnosti*. Forum-Media. https://www.e-dokumentacija.si/vsebine/informacijska-varnost-e-hrambe-in-poslovanja/informacijska-varnost/zahteve-za-zagotavljanje-informacijske-varnosti-pri-zajemu-e-hrambi/fizi%C4%8Dno-in-tehni%C4%8Dno-varovanje-prostorov-opreme-in-gradiva-kot-eden-od-vidikov-zagotavljanja-informacijske-varnosti/

Hayes, A. (2023). Code of ethics: Understading its types, uses through examples. V *Investopedia*. https://www.investopedia.com/terms/c/code-of-ethics.asp
Herrity, J. (11. 3. 2023). Management roles and responsibilities. *Indeed*. https://www.indeed.com/career-advice/finding-a-job/management-roles
Hewlett Packard. (2023). *What is infrastucture security?* https://www.hpe.com/us/en/what-is/infrastructure-security.html
Höne, K. in Eloff, J. H. P. (2002). What makes an effective information security policy? *Network Security,* (6), 14–16. https://doi.org/10.1016/S1353-4858(02)06011-7
Horvath, I. (2023). *Top 5 risk analysis methods that you should know*. Invensis. https://www.invensislearning.com/blog/risk-analysis-methods/
Hribar, G., Ivanuša, T. in Podbregar, I. (2012). Protiobveščevalna dejavnost – znano, neznano. V T. Pavšič Mrevlje (ur.), *Zbornik prispevkov: 13. Slovenski dnevi varstvoslovja, 7.–8. junij 2012, Portotož*. Fakulteta za varnostne vede. http://www.fvv.uni-mb.si/DV2012/zbornik/varnostno_obvescevalna_dejavnost/hribar_podbregar_ivanusa.pdf
Hrovat, R. in Gorše, K. (ur.). (2000). *Požarna varnost v cestnih predorih.* Uprava Republike Slovenije za zaščito in reševanje pri Ministrstvu za obrambo: Družba za avtoceste v Republiki Sloveniji.
Hunter, J. M. D. (2001). Physical security. V J. M. D. Hunter (ur.), *An information security handbook*. (str. 29–34). Springer. https://link.springer.com/chapter/10.1007/978-1-4471-0261-8_3
IBM. (2021). *Developing a security policy*. https://www.ibm.com/docs/en/i/7.2?topic=strategy-developing-security-policy
ICS, Institut za korporativne varnostne študije. (2019). *Neprekinjeno poslovanje*. https://www.ics-institut.si/korporativna-varnost/neprekinjeno-poslovanje
Indeed. (2023a). *How to create a business code of ethics*. https://www.indeed.com/hire/c/info/code-of-ethics-and-professional-conduct
Indeed. (2023b). *What are external threats to a business? (With examples)*. https://uk.indeed.com/career-advice/career-development/external-threats
Infocenter. (2023). *Ocena tveganja za varnost in zaščito organizacij pred tveganji in neželenimi posledicami.* https://infocenter.si/ocena-tveganja-za-varnost-in-zascito-organizacij-pred-tveganji-in-nezelenimi-posledicami/
Infocenter. (n. d. a). *Posodobitev pravilnika o postopkih in ukrepih za zavarovanje osebnih podatkov.* https://infocenter.si/posodobitev-pravilnika-o-postopkih-in-ukrepih-za-zavarovanje-osebnih-podatkov/
Infocenter. (n. d. b). *Neprekinjeno poslovanje.* https://infocenter.si/neprekinjeno-poslovanje/
Infocenter. (n. d. c). *Varstvo osebnih podatkov. https://infocenter.si/varstvo-osebnih-podatkov-v-danasnjem-casu/*
Informacijski pooblaščenec. (n. d.). *Varnost osebnih podatkov*. https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/zavarovanje-oz-varnost-osebnih-podatkov
Inšpektorat Republike Slovenije za delo. (2020). *Obveznosti delodajalcev, pravice in dolžnosti delavcev ter samozaposlenih oseb.* GOV.SI. https://www.gov.si/teme/obveznosti-delodajalcev-pravice-in-dolznosti-delavcev-ter-samozaposlenih-oseb/
iReport Source. (2022). *8 key components of a successful safety management program.* https://ireportsource.com/blog/safety-management-program/
Irwin, L. (23. 9. 2022). *Conducting an asset-based risk assessment in ISO 27001*. Vigilant Software. https://www.vigilantsoftware.co.uk/blog/conducting-an-asset-based-risk-assessment-in-iso-270012013
ISACA. (2023). *State of Cybersecurity 2023 report*. https://www.isaca.org/resources/reports/state-of-cybersecurity-2023
Ivandić Vidović, D., Karlović L. in Ostojić, A. (2011). *Korporativna sigurnost*. Udruga hrvatskih menadžera.
Kandžič, A. (2021). Korporativna varnost je pomemben dejavnik za zagotavljanje ustrezne odpornosti delovanja organizacije. *Korporativna varnost, 22*(28), 30–32.
Kastelic, Z. (2016). Izobraževanja znotraj organizacije. *Revija za univerzalno odličnost, 5*(3), 233–241.
Kenton, W. (2023). SWOT analysis: How to with table and example. V *Investopedia.* https://www.investopedia.com/terms/s/swot.asp
Khodarahmi, E. (2009). Crisis management. *Disaster Prevention and Management: An International Journal, 18*(5), 523–528.
Kinzer, K. (2022). What is password management? *Jumpcloud.* https://jumpcloud.com/blog/what-is-password-management
Kirkham, A. (2022). Top workplace security policies and procedured that safeguard your organization. *Envoy*. https://envoy.com/blog/workplace-security-policy-and-procedures/
Kirn, A. (1995). Tveganje kot družbenovrednotna kategorija. *Teorija in praksa*, *32*(3/4), 212–219.

Kodeks. (n. d.). V *Slovar slovenskega knjižnega jezika*. https://fran.si/iskanje?View=2&Query=kodeks
Kohont, A. (2019). Menedžment človeških virov: stično področje za svetovanje v izobraževanju in usposabljanju zaposlenih. V T. Vilič Klenovšek (ur.), *S svetovanjem za zaposlene do večje vključenosti v izobraževanje in usposabljanje* (str. 16–44). Andragoški center Slovenije.
Kompare, J. (2014). *Obveznosti delavca*. Atama. https://atama.si/aktualno/novosti-v-zaposlovanju/obveznosti-delavca
Kop, I. (1995). *Varovanje in zaščita poslovnih skrivnosti*. Gospodarski vestnik.
Kovačič, A. in Podvršič, A. (2014). Korporativni varnostni management – nujnost sodobnih organizacij. *Korporativna varnost,* (7), 9–11.
Kriza. (n. d.). V *Slovar slovenskega knjižnega jezika*. https://fran.si/iskanje?View=1&Query=kriza
Kubale, V., Lobnikar, T., Gabrovec, B. in Dvojmoč, M. (2023). Ensuring corporate security and its strategic communication in healthcare institutions in Slovenia. *Healthcare, 11*(11)*,* 1578. https://doi.org/10.3390/healthcare11111578
Kumar, S. (18. 6. 2014). *The challenges of corporate security?*. Linkedin. https://www.linkedin.com/pulse/20140618052131-41375523-the-challenges-of-corporate-security
Lapuh Bele, J. (2021). *Informacijska varnost*. Visoka šola za poslovne vede.
Lee Seungmug, Z. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology, 14*(1), 203–219.
Lesjak, R. M. (2020). Krizne situacije razkrijejo vse. *Urednica*. https://www.urednica.si/strokovne-vsebine/krizne-situacije-razkrijejo-vse/
Lichte, D., Witte, D., Termin, T. in Wolf, K.-D. (2021). Representing uncertainty in physical security risk assessment. *European Journal for Security Research, 6*, 189–209. https://link.springer.com/article/10.1007/s41125-021-00075-3
Lincke, S. (2015). Desining physical security. V S. Lincke (ur.), *Security planning* (str. 159–170) Springer. https://link.springer.com/chapter/10.1007/978-3-319-16027-6_9
Liu, A. X. in Gouda, M. G. (2008). Diverse firewall design. *IEEE Transactions on Parallel and Distributed Systems, 19*(8), 1237–1251.
Lobnikar, B. in Sotlar, A. (2006). Celovito upravljanje z varnostnimi tveganji kot dejavnik dolgoročne uspešnosti podjetja. V A. Dvoršek in L. Selinšek (ur.), *Kriminalni napadi na premoženje gospodarskih subjektov (varnostni, pravni in zavarovalni vidik)* (str. 9–20). Pravna fakulteta; Fakulteta za policijsko-varnostne vede.
Ludbey, C. (2016). *The corporate security stratum of work: Identifying levels of work in the domain*. Edith Cowan University. https://ro.ecu.edu.au/theses_hons/1489/
Madureira, L., Popovič, A. in Castelli, M. (2021). Competitive intelligence: A unified view and modular definition. *Technological Forecasting and Social Change*, *173*. https://doi.org/10.1016/j.techfore.2021.121086
Markelj, B. in Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: Zavedanje uporabnikov v Sloveniji. *Revija za kriminalistiko in kriminologijo, 67*(1), 44–60.
Markelj, B. in Zgaga, S. (2018). Kibernetska varnost in kibernetska kriminaliteta uporabnikov mobilnih naprav v Sloveniji. *Revija za kriminalistiko in kriminologijo, 69*(1), 15–29.
Matryx. (2023). *Eight thing your security consultant can do for you*. https://matryxconsulting.com.au/eight-things-security-consultant-can/
Merkač Skok, M. (2013). Mentorstvo, trenerstvo, karierno svetovanje: vplivni dejavniki razvoja kariere. V V. Dermol (ur.), *Sodobni izzivi managementa človeških virov* (str. 153–165). Mednarodna fakulteta za družbene in poslovne študije.
Meyer, K. (2023). *Facing the unexpected: Mastering crisis communications*. Business wire. https://blog.businesswire.com/facing-the-unexpected-mastering-crisis-communications
Michelle. (2023). Five steps to effective qualitative risk assessment. *Nifty*. https://niftypm.com/blog/qualitative-risk-assessment/
Mihalič, R. (2006). *Management človeškega kapitala*. Mihalič in Partner.
Mind Tools Content Team. (2023). *Swot analysis: Understanding your business, informing your strategy*. MindTools. https://www.mindtools.com/amtbj63/swot-analysis
Ministrstvo za digitalno preobrazbo. (2023). *Načrtovanje sistemov tehničnega varovanja*. https://spot.gov.si/sl/dejavnosti-in-poklici/dejavnosti/nacrtovanje-sistemov-tehnicnega-varovanja/
Ministrstvo za javno upravo. (2020). *CAF 2020: priročnik za uporabo modela CAF 2020*. https://www.gov.si/assets/ministrstva/MJU/Kakovost-in-inovativnost-v-javni-upravi/CAF/CAF-prirocnik_A4_WEB.pdf
Modic, M., Lobnikar, B. in Dvojmoč, M. (2014). Policijska dejavnost v Sloveniji: Analiza procesov transformacije, pluralizacije in privatizacije. *Varstvoslovje, 16*(3), 217–241.

Molak, V. (1997). *Fundamentals of risk analysis and risk management*. CRC Press.
Molinaro, D. (4. 11. 2022). *What is biometrics and how secure is biometric data*? Avast. https://www.avast.com/c-what-is-biometricdata#topic-1
Možina, S. (2009). Učenje, izobraževanje, usposabljanje in razvoj kadrov. V I. Svetlik in N. Zupan (ur.), *Menedžment človeških virov* (str. 467–520). Fakulteta za družbene vede.
Nanda. (2023). *How can companies protect their assets?* https://www.nanda.ca/how-can-companies-protect-their-assets/
National Cyber Security Centre. (2021). *Device security guidance*. https://www.ncsc.gov.uk/collection/device-securityguidance/policies-and-settings/antivirus-and-other-security-software
Ollivier, P. in De Leon, V. N. (2021). Business secrets are at the heart of a good intangible asset strategy for comapny executives. *Les Nouvelles – Journal of the Licensing Executives Society, LVI*(4), 316–320.
Online manipal editorial team. (11. 5. 2023). Importance of management in an organization. *Online Manipal*. https://www.onlinemanipal.com/blogs/importance-of-management-in-an-organization
Paltrinieri, N., Comfort, L. in Reiniers, G. (2019). Learning about risk: Machine learning for risk assessment. *Safety Science, 118*, 475–486. https://doi.org/10.1016/j.ssci.2019.06.001
Parsons, N. (2021). What is a SWOT analysis and how to do it right (with examples). *LivePlan*. https://www.liveplan.com/blog/what-is-a-swot-analysis-and-how-to-do-it-right-with-examples/
Patentni biro. (n. d.). *Intelektualna lastnina*. https://www.patentni-biro-af.si/kaj-je-intelektualna-lastnina.html
Pečar, J. (2000). Nadzorovanje – temelj in vsebina varovanja in varnosti (Kaj z »varstvoslovjem«?). *Revija za kriminalistiko in kriminologijo, 51*(2), 105–114.
Podbregar, I. (2007). *Varnostni in varstveni standardi v podjetju: Skripta za usposabljanje za pridobitev pooblaščenega gospodarskega subjekta AEO po standardih AXUD/2006/1450*. Samozaložba.
Podbregar, I., Mulej, M., Pečan, S., Podbregar, N. in Ivanuša, T. (2010). *Informacije kot »bojna« podpora kriznemu odločanju, krizni komunikaciji in delovanju*. Zavod za varnostne strategije pri Univerzi Maribor.
Policija. (n. d. a). *Varovanje oseb in objektov*. https://www.policija.si/index.php/component/content/article/188-varovanje-oseb-in-objektov/69999-varovanje-oseb-in-objektov
Policija. (n. d. b). *Sedem vrst spletnih finančnih prevar, ki jim uporabniki najpogosteje nasedejo*. https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/sedem-vrst-spletnih-financnih-prevar-ki-jim-uporabniki-najpogosteje-nasedejo
Pranggono, B. in Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Journal of Internet Technology Letters, 4*(2), 1−6. https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/itl2.247
Pravilnik o izdelavi ocen požarne ogroženosti. (2020). *Uradni list RS*, (180/20).
Pravilnik o požarnem redu. (2007). *Uradni list RS*, (52/07).
Pravilnik o usposabljanju in pooblastilih za izvajanje ukrepov varstva pred požarom. (2011). *Uradni list RS*, (32/11).
Primc, Ž. (2021). The use of tools for obtaining data from publicly accessible sources for the purpose of competitive intelligence in enterprises. *Varstvoslovje, 23*(4), 425 – 446.
Prislan, K. (2016). *Večkriterijski model učinkovitosti informacijske varnosti v organizacijah* [Doktorska disertacija]. Fakulteta za varnostne vede. https://dk.um.si/Dokument.php?id=108821&lang=slv
Prislan, K. in Bernik, I. (2014). Trendi informacijske varnosti v sodobni organizaciji. *Uporabna informatika, 22*(1), 25–37.
Prislan, K. in Bernik, I. (2019). *Informacijska varnost in organizacije*. Fakulteta za varnostne vede.
Purpura, P. P. (2017). Internal threats and countermeasures. V L. J. Fennelly (ur.), *Effective physical security* (fifth edition) (str. 181–218). Butterworth-Heinemann.
Putra, I. H. in Purba, E. D. (2020). Effects of satisfaction, subjective norms, and self-efficacy on job application intentions of student interns. *PRoUST, Psychological research on urban society, 3*(2), art. 9. https://doi.org/10.7454/proust.v3i2.92
Rakar, A. (2006). Upravljanje z varnostnim tveganjem informacijskih sistemov. V A. Novaković, M. Indihar Štemberger, M. Bajec in J. Poženel (ur.), *V partnerstvu z informatiko do poslovne odličnosti: zbornik posvetovanja: Dnevi slovenske informatike 2006 – DSI, Portorož, Slovenija, 19.–21. april* (str. 1–7). Slovensko društvo Informatika.
Rashid, R. M., Zakaria, O. in Zulhemay, N. M. (2013). The relationship of information security knowledge (isk) and human factors: Challenges and solution. *Journal of Theoretical and Applied Information Technology, 57*(1), 67–75.
Reed, C. (2021). Internal threats: Everything you need to know. *Firewall Times*. https://firewalltimes.com/internal-threats/

Reid, M. B. (2021). Business continuity plan. V L. R. Shapiro in M.-H. Maras (ur.), *Encyclopedia of security and emergency management*. (str. 52–57). Springer. https://link.springer.com/referenceworkentry/10.1007/978-3-319-70488-3_112

Reinfelder, L., Landwirth, R. in Benenson, Z. (2019). Security managers are not the enemy either. V S. Brewster in G. Fitzpatrick (ur.), *Proceedings of the 2019 CHI conference on human factors in computing systems* (str. 1–7). Association for Computing Machinery.

Resolucija o nacionalnem programu varnosti in zdravja pri delu 2018–2027. (ReNPVZD18–27). (2018). *Uradni list RS*, (23/18).

Riantini Supriadi, L. S. in Sui Pheng, L. (2016). *Business continuity management in construction*. Springer.

RiskOptics. (2023). *What is technology risk?*. Reciprocity. https://reciprocity.com/resources/what-is-technology-risk/

Rouse, M. (2015). Technical security. V *Techopedia*. https://www.techopedia.com/definition/31429/technical-security-techsec

Rumelili, B. (2015). Identity and desecuritisation: the pitfalls of conflating ontological and physical security. *Journal of International Relations and Development, 18*, 52–74. https://link.springer.com/article/10.1057/jird.2013.22

Sapiński, A., Ciupka, S. in Tomanik, R. (2020). Emotional intelligence in the professional life of a security manager. *Social Development & Security, 10*(1), 79–83.

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

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K-K. R. in Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics, 9*(9). https://doi.org/10.3390/electronics9091460

Schaurer, F. in Störger, J. (2013). The evolution of open source intelligence (OSINT). *Journal of U.S. Intelligence Studies, 19*(3), 53–56.

Schermerhorn, J. (2002). *Management*. Wiley.

Schneller, L., Porter, C. N. in Wakefield, A. (2022). Implementing converged security risk management: Drivers, barriers, and facilitators. *Security Journal, 36*, 333–349.

Schweighofer, T. (2010) *Vpeljava varnostne politike v srednje velikem podjetju* [Diplomsko delo]. Fakulteta za elektrotehniko, računalništvo in informatiko.

Sektor za varnost in zdravje pri delu. (n. d.). *Obveznosti delodajalcev, pravice in dolžnosti delavcev ter samozaposlenih oseb*. GOV.SI. https://www.gov.si/teme/obveznosti-delodajalcev-pravice-in-dolznosti-delavcev-ter-samozaposlenih-oseb/

Shaw, C. (2020). *Why phishing works and the detection needed to prevent it* [Dissertation]. Faculty of Utica College.

SHRM. (2024). *Developing effective safety management programs*. https://www.shrm.org/topics-tools/tools/toolkits/developing-effective-safety-management-programs

Silva Consultants. (2023). *Why would an expirienced security manager hire a security consultant*. https://www.silvaconsultants.com/new-security-tips/why-would-an-experienced-security-manager-hire-a-security-consultant

Slovar slovenskega knjižnega jezika (Druga, dopolnjena in deloma prenovljena izdaja). (2014). Inštitut za slovenski jezik Frana Ramovša ZRC SAZU.

Sood, P. in Bhushan, P. (2020). A structured review and theme analysis of financial frauds in the banking industry. *Asian Journal of Business Ethics, 9*(2), 305–321.

Sotlar, A. in Čas, T. (2011). Analiza dosedanjega razvoja zasebnega varovanja v Sloveniji – med prakso, teorijo in empirijo. *Revija za kriminalistiko in kriminologijo, 62*(3), 227–241.

Sotlar, A. in Dvojmoč, M. (2021). Zasebno varovanje in korporativna varnost v času epidemije covida-19 v Sloveniji. *Revija za kriminalistiko in kriminologijo, 72*(1), 79–90.

Stankovski, L. (2012). Role of the security manager in managing with risks, threats and emergencies in toplifikacija A.D Skopje. V C. Mojanski (ur.), *International scientific conference: security and euroatlantic perspectives of the Balkans: police science and police profession (states and perspectives)* (str. 217–224). University St. Kliment Ohridski – Bitola.

Stevenson, R. (21. 07. 2022). *6 Types of risk assessment methodologies + How to choose*. Drata. https://drata.com/blog/risk-assessment-methodologies

Stvarnopravni zakonik (SPZ). (2003). *Uradni list RS*, (87/02).

Šaponja, V. (1999). *Taktika dela obveščevalnovarnostnih služb*. Visoka policijsko-varnostna šola.

Španinger, V. (2006). *Varovanje poslovnih skrivnosti v gospodarskih družbah: specialistično delo*. Fakulteta za organizacijske vede.

Team Asana. (2022). What is crisis management plan? (6 steps to create one). *Asana.* https://asana.com/resources/crisis-management-plan

Thinkcurity. (2022). *How to Perform a SWOT Analysis on Your Security Firm.* https://www.thinkcurity.com/articles/how-to-perform-a-swot-analysis-on-your-security-firm

Trivan, D. (2013). The influence of corporate security on national security = Vpliv korporativne varnosti na nacionalno varnost. *Sodobni vojaški izzivi, 15*(3), 69–98. 10.33179/BSV.99.SVI.11.CMC.15.3.5

Trivan, D. (2017). *Osnove korporativnega varovanja.* Fakulteta za poslovne studije i pravo.

Urad Republike Slovenije za intelektualno lastnino. (n. d.). *Intelektualna lastnina.* GOV.SI. https://www.gov.si/podrocja/podjetnistvo-in-gospodarstvo/intelektualna-lastnina/

Urbach, N. in Ahlemann, F. (2019). Digitalization as a risk: security and business continuity management are central cross-divisional functions of the company. V N. Urbach, F. Ahlemann (ur.), *IT Management in the Digital Age: A Roadmap for the IT Department of the Future.* (str. 85–92). Springer.

Uredba (EU) 2016/679 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP). (2016). *Uradni list Evropske unije,* (L 119/1).

Ustava Republike Slovenije (URS). (1991). Uradni list RS, (33/91-I, 42/97- UZS68, 66/00-UZ80, 24/03-UZ3a, 47,68, 69/04-UZ14, 69/04-UZ50, 68/06-UZ121, 140, 143, 47/13-UZ148, 47/13-UZ90, 97, 99, 75/16-UZ70a in 92/21-UZ62a).

Vadnjal, J. (2014). Korporativna varnost in poslovna etika. *Korporativna varnost,* (6), 27–30.

Van Deventer, L. (2023). *What to know about a security procedure.* Essential Data Corporation. https://essentialdata.com/the-principles-about-a-security-procedure/

van Zadelhof, M. (19. 9. 2016). The biggest cybersecurity threaths are inside your company. *Harvard Business Review.* https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Varnost Ljubljana. (2020). *Varovanje.* https://www.varnostljubljana.si/storitve/varovanje/

Veniger, S. (2013). Policija je pomemben partner pri zagotavljanju korporativne varnosti v organizacijah. *Korporativna varnost,* (4), 5–9.

Vidic, J. (2008). Krizni management kot sestavni del managementa neprekinjenega poslovanja gospodarske družbe. V J. Šifrer (ur.), *Javna in zasebna varnost: zbornik prispevkov: 9. slovenski dnevi varstvoslovja, Bled, 5. in 6. junij 2008*. Fakulteta za varnostne vede. http://www.fvv.uni-mb.si/dv2008/zbornik/clanki/Vidic.pdf

Vršec, M. (1993). *Varnost podjetja – tokrat drugače*. Viharnik.

Vršec, M. (2014). Strateško načrtovanje procesov korporativne varnosti. *Korporativna varnost,* (6), 23–26.

Vršec, M. in Vršec, M. (2006). Vzpostavljanje celovitega varovanja kot preventivnega dejavnika v gospodarskih družbah. V A. Dvoršek in L. Selinšek (ur.), *Kriminalni napadi na premoženje gospodarskih subjektov: (varnostni, pravni in zavarovalni vidiki)* (str. 83–101). Pravna fakulteta in Fakulteta za policijsko-varnostne vede.

Vršec, M. in Vršec, M. (2015). Kaj sploh je korporativna varnost. *Korporativna varnost*, (9), 5–9.

Will, M. in Brauweiler, W. (2020). Business continuity management (BCM). V W. L. Filho, A. M. Azul, L. Brandli, P. Gökçin Özuyar in T. Wall (ur.), *Sustainable cities and communities* (str. 33–44). Springer. https://doi.org/10.1007/978-3-319-95717-3_2

Wright, L. (2017). Business continuity planning. V L. Wright, *People, risk, and security: How to prevent your greatest asset from becoming your greatest liability* (str. 107–120). https://link.springer.com/chapter/10.1057/978-1-349-95093-5_8

Wu, W. N. (2021). Organizational resilience: examining the influence of information cost and organizational capacity on business continuity management. V F. F. H. Nah in K. Siau (ur.), *International conference on human-computer interaction.* (str. 444–455). Springer International Publishing.

Yasar, K. (2023). *Risk analysis*. TechTarget. https://www.techtarget.com/searchsecurity/definition/risk-analysis

Zagorc, A. (2016). *Interno izobraževanje*. Fakulteta za organizacijske študije. https://www.fos-unm.si/media/pdf/RUO/2016-5-3/RUO_046_koncni_2.pdf

Zakon o avtorski in sorodnih pravicah (ZASP). (1995). *Uradni list RS*, (21/95).

Zakon o avtorski in sorodnih pravicah (ZASP-UPB3). (2007). *Uradni list RS*, (16/07).

Zakon o delovnih razmerjih (ZDR-1). (2013). *Uradni list RS*, (21/13).

Zakon o detektivski dejavnosti (ZDD-1). (2011). *Uradni list RS*, (17/11).

Zakon o detektivski dejavnosti (ZDD). (1994). *Uradni list RS*, (32/94).

Zakon o gospodarskih družbah (ZGD-1). (2006, 2008, 2009, 2011, 2012, 2013, 2015, 2017, 2019). *Uradni list RS*, (42/06, 60/06, 10/08, 68/08, 42/09, 33/11, 91/11, 32/12, 57/12, 82/13, 55/15, 15/17, 22/19).

Zakon o industrijski lastnini (ZIL-1). (2001, 2002, 2004, 2006, 2013). *Uradni list RS*, (45/01, 96/02, 37/04, 20/06, 100/13).

Zakon o kritični infrastrukturi. (ZKI). (2017). *Uradni list RS*, (75/17).

Zakon o organiziranosti in delu v policiji (ZODPol). (2013). *Uradni list RS*, (15/13).
Zakon o podjetjih (Zpod). (1988, 1989, 1990). *Uradni list RS*, (77/88, 40/89, 46/90).
Zakon o poslovni skrivnosti (ZPosS). (2019). *Uradni list RS*, (22/19).
Zakon o tajnih podatkih (ZTP). (2001, 2003, 2006, 2010, 2011). *Uradni list RS*, (87/01, 101/03, 28/06, 9/10, 60/11).
Zakon o varstvu osebnih podatkov (ZVOP-2). (2022). *Uradni list RS*, (163/22).
Zakon o varstvu pred požarom (ZVPoz-UPB1). (2007). *Uradni list RS*, (3/07).
Zakon o zasebnem varovanju (ZZasV-1). (2011). *Uradni list RS*, (17/11).
Zakon o zasebnem varovanju in o obveznem organiziranju varnostnih služb (ZZVO). (1994). *Uradni list RS*, (32/94).
Združenje notranjih revizorjev. (n. d.). *Več o notranji reviziji.* https://www.iia.si/vec-o-notranji-reviziji/#toggle-id-18
Zimmerman, R. in Restrepo, C. E. (2021). Physical security: exterior application. V L. R. Shapiro in M. H. Maras (ur.), *Encyclopedia of security and emergency management*. (str. 737–747). Springer.
Žirovnik, J. in Podbregar, I. (2006). Obveščevalno-varnostni vidiki ogrožanj pomembnih gospodarsko poslovnih subjektov. V A. Dvoršek in L. Selinšek (ur.), *Kriminalni napadi na premoženje gospodarskih subjektov: (varnostni, pravni in zavarovalni vidiki)* (str. 47–66). Pravna fakulteta in Fakulteta za policijsko-varnostne vede.

INTEGRALNA KORPORATIVNA VARNOST: PRAKTIKUM

MIHA DVOJMOČ
Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
miha.dvojmoc@um.si

Varnost je na splošno ena izmed najpomembnejših prvin človeštva, zato se je tudi v organizacijah razvila dejavnost, imenovana korporativna varnost, ki zagotavlja varnost na različnih področjih. Ne glede na njeno pomembnost, se ji še vedno ne posveča dovolj pozornosti, zato praktikum predstavlja različne poglede na sam pojem, njene začetke oz. zgodovino in vse, kar dejansko sestavlja celovit proces zagotavljanja varnosti v organizacijah. Skozi praktikum se bralec seznani z vsem, kar je pomembno pri zagotavljanju varnosti oseb, premoženja, infrastrukture in vsega drugega, kar tvori korporativno varnost. S predstavitvijo vseh pojmov, definicij, postopkov in procesov postane razumevanje temeljnega pojma precej lažje, kar pripomore k enostavnejšemu odgovarjanju na vprašanja, ki so zastavljena po vsakem poglavju. Preko vprašanj bralec utrdi svoje znanje, hkrati pa upamo, da v njem vzbudi še večje zanimanje za področje korporativne varnosti.

DOI
https://doi.org/
10.18690/um.fvv.3.2024

ISBN
978-961-286-850-5

Ključne besede:
integralna korporativna varnost,
organizacije,
varnostni menedžer,
varnost,
tveganja

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.3.2024

ISBN
978-961-286-850-5

Ključne besede:
integral corporate security,
organizations,
security manager,
security,
risks

University of Maribor Press

Integral Corporate Security: Practicum

Miha Dvojmoč
University of Maribori, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
miha.dvojmoc@um.si

Security is generally one of the most important elements of humanity, so an activity called corporate security has also developed in organizations, which ensures security in various areas. Regardless of its importance, it is still not given enough attention. That is why the practicum presents different views on the concept itself, its beginnings or history and everything that actually makes up the complete process of ensuring security in organizations. Through the practicum, the reader gets acquainted with everything that is important in ensuring the safety of persons, property, infrastructure and everything else that makes up corporate security. By presenting all concepts, definitions, procedures and processes, the understanding of the basic concept becomes much easier, which helps to answer more easily the questions that are asked after each chapter. Through the questions, the reader consolidates his knowledge, and at the same time we hope that it arouses in him an even greater interest in the field of corporate security.

Praktikum "Integralna korporativna varnost" avtorja Miha Dvojmoča predstavlja dragocen vir informacij in znanj za vse, ki se ali se bodo poklicno ukvarjali z vprašanji korporativne varnosti, in prispeva k boljšemu razumevanju ter učinkovitejšemu upravljanju varnostnih tveganj v organizacijah.

Branko LOBNIKAR
Univerza v Mariboru, Fakulteta za varnostne vede

Integralna korporativna varnost: praktikum ni zgolj gradivo za študente, ki se z dotičnimi vsebinami srečujejo, temveč je zelo dobrodošel pripomoček tudi za vse tiste, ki se s temi vsebinami dnevno srečujejo v delovnem ali strokovnem procesu, saj je iz praktikuma mogoče razbrati, da ima avtor številne in dolgoletne izkušnje s tega področja, tako teoretične kot tudi praktične.

Dragan TRIVAN
Univrzitet »Uninon – Nikola Tesla«, Fakultet za poslovne studije i pravo

Univerza v Mariboru
Fakulteta za varnostne vede