Sigurnost korporacija u vremenu pandemije bolesti Covid-19

Brletić, Kristina

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zagreb

Specijalistički diplomski stručni studij

Menadžment javnog sektora

KRISTINA BRLETIĆ

SIGURNOST KORPORACIJA U VREMENU PANDEMIJE BOLESTI COVID-19

SPECIJALISTIČKI ZAVRŠNI RAD

Zaprešić, 2021. godine

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zagreb

Specijalistički diplomski stručni studij

Menadžment javnog sektora

SPECIJALISTIČKI ZAVRŠNI RAD

SIGURNOST KORPORACIJA U VREMENU PANDEMIJE BOLESTI COVID-19

Mentor:
dr.sc. Dragutin Funda, prof. v. š.

Studentica:
Kristina Brletić

Naziv kolegija:
Upravljanje kriznim situacijama

JMBAG studentice:
0066139469

SAŽETAK

Tema ovog rada je korporativna sigurnost u vremenu pandemije virusa Covid-19. Kako su korporacije svojom veličinom veliki poslovni objekti, za očekivati je da će one biti jedna od žarišta širenja virusa. S obzirom na naglo širenje bolesti odjeli korporativne sigurnosti morali su se prilagoditi trenutnoj situaciji.

Tako je u ovome radu teorijski obrađena materija od samog pojma krize i kriznog komuniciranja do implementacije korporativne sigurnosti unutar korporacija. Posebna pozornost je posvećena organizaciji procesa rada i implementaciji odgovarajućih mjera kao odgovor na pandemiju virusa Covid-19, kako zdravstvenih tako i mjera cyber sigurnosti.

Ključne riječi: **korporativna sigurnost, bolest Covid-19, kriza, krizno komuniciranje, ugroze**

TITLE IN ENGLISH: CORPORATE SECURITY DURING THE COVID-19 DISEASE PANDEMIC

ABSTRACT

The topic of this paper is corporate security during the pandemic of Covid-19 virus. As corporations are large business objects by their size, it is to be expected that they will be one of the spread centers of the virus. Given the rapid spread of the disease, corporate security departments had to adapt to the current situation.

Thus, this paper theoretically deals with the concept of crisis, crisis communication and the implementation of corporate security within corporations. Special attention is paid to the work processes within organization and the implementation of appropriate health and cyber security measures and response to the Covid-19 virus pandemic.

Key words: **corporate security, disease Covid-19, crisis, crisis communication, threats**

1. UVOD

U ovome radu su detaljno opisani izazovi, rješenja i smjernice sa kojima se korporacije susreću u periodu tijekom trajanja pandemije bolesti Covid-19, a posebno organizacijski dijelovi koji se bave korporativnom sigurnošću. Korporacije odnosno timovi korporativne sigurnosti se već dugi niz godina susreću sa raznim krizama, rješavanjem istih te komuniciranjem u kriznim situacijama unutar i van organizacije. Kako je pandemija bolesti Covid-19 bila nepredvidivi problem, timovi korporativne sigurnosti su se primarno bavili sprječavanjem širenja bolesti unutar organizacije te primjenama mjera koje su se donosile na državnoj i lokalnoj razini. Upravo je proučavanje primjena mjera i pregled sigurnosnih izazova unutar korporacija bio primarni istraživački problem ovog rada.

Svrha ovog rada je cjelovita teorijska obrada ponašanja korporacija u vremenu bolesti Covid-19 dok je cilj rada istražiti važnost i položaj tima korporativne sigurnosti unutar korporacije.

Rad je strukturiran na način da osim uvoda i zaključka sadrži još šest poglavlja. U drugom poglavlju je obrađen pojam krize i kriznog upravljanja u domeni korporacija. U trećem poglavlju je obrađena teorija kriznog komuniciranja i njena važnost u nepredvidivim situacijama te u očuvanju reputacije kompanije. U sljedećem, četvrtom poglavlju je obrađena tematika korporativne sigurnosti, njen razvoj i pravni status unutar Republike Hrvatske. U petom poglavlju su obrađeni razni oblici ugroza korporacija i njenih resursa. U šestom poglavlju je obrađena sigurnost i zaštita radnika unutar korporacija za vrijeme trajanja pandemije virusa Covid-19 te izazovi i radnje koje se moraju napraviti pod upravljanjem tima korporativne sigurnosti. U sedmom poglavlju su obrađene prijetnje koje imaju primarni cilj ugrozu informacijskih sustava unutar korporacija. U posljednjem, osmom poglavlju su prikazani koraci i planovi za oporavak poslovanja radi utjecaja krize uzrokovane pandemijom bolesti Covid-19.

2. KRIZA

Kriza je nepredvidiv događaj koji može imati negativni ishod koji utječe na organizaciju (na njihove usluge, proizvode ili ugled), cijelu ili dio industrije. Svaka kriza zahtijeva kvalitetnu i efikasnu komunikaciju kako bi se potencijalna šteta povezana sa nepredvidivim događajem u što većoj mjeri smanjila. Jedan od primjera nepredvidivih događaja je pandemija koja je uzrokovana virusom Covid-19.

Posljedice krize su vidljive kako u financijskom smislu tako i u području efikasnosti rada i procesa organizacije. Neki od simptoma u financijskom smislu su sljedeći:

- Povećanje stope zaduženosti,
- Smanjenje likvidnosti,
- Smanjenje rentabilnosti,
- Smanjenje prometa,
- Smanjenje novčanog toka.

Simptomi krize koji su vidljivi u području efikasnosti rada i procesa organizacije:

- Područje prodaje: smanjenje tržišnog udjela, smanjenje narudžbi, kašnjenje u rokovima,
- Područje zaposlenika: visoka stopa fluktuacije, nezadovoljstvo radnika i štrajkovi,
- Područje nabave: porast kašnjenja isporuke, povećanje dana vezivanja zaliha, povećanje učestalosti grešaka,
- Područje proizvodnje gdje se smanjuje proizvodnost, porast otpada i škarta, smanjenje stupnja iskorištenja kapaciteta,
- Tehnološko područje: smanjenje stupnja investiranja, istraživanja i razvoja, smanjenje efikasnosti poslovnog procesa. (Osmanagić Bedenik, 2007: 21-22)

2.1.Tipologija krize

Svaka kriza u poslovnom svijetu ima vlastitu povijest koja je bila pod internim i eksternim utjecajima i njihovim međusobnim odnosima. Kriza je obilježena višeslojnim aspektima, a sama tipologija omogućava analizu pojedinih aspekata i njihovo dublje razumijevanje. Kriteriji koji se uzimaju za diferenciranje tipologije kriza u poslovnom svijetu:

- Uzrok krize: eksterno i/ili interno uzrokovane krize,

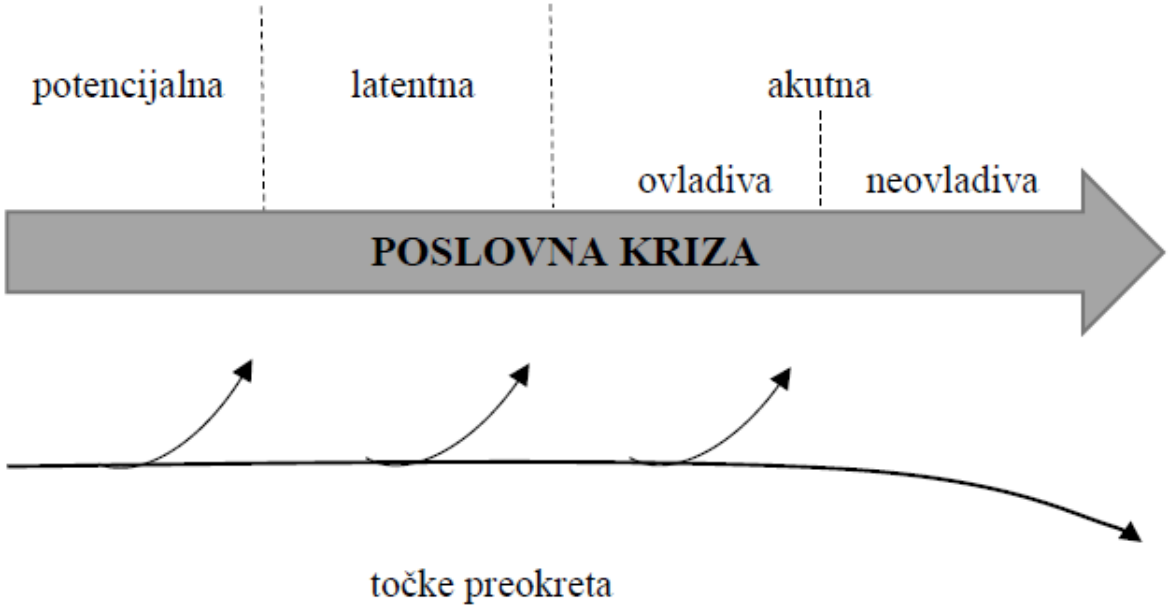
- Broj uzroka same krize: Uni kauzalno i multi kauzalno uzrokovane krize,
- Duljina krize: kratkotrajne i dugotrajne krize,
- Stupanj opažanja: potencijalne, latentne i akutne krize,
- Mogućnost vladanja kriznim procesom: konačno, privremeno i ne ovladive poslovne krize,
- S obzirom na posljedicu: krize s većinski destruktivnim posljedicama ili pretežito konstruktivnim posljedicama,
- Lokalizacija posljedica: krize s pretežito internim ili pretežito eksternim posljedicama,
- Ciljevi korporacije: strategijska kriza, kriza uspjeha ili kriza likvidnosti,
- Stadij krize: kriza koja je opasna za sami opstanak poduzeća te kriza koja uništava korporaciju te ona više ne postoji u postojećem obliku,
- Predvidivost krize: nepredvidiva i predvidiva kriza.

Kada se uključi stupanj opažanja, posljedica te vremenske dimenzije u pojam krize, moguće je razlikovanje na: potencijalne, latentne i akutne krize. (ibidem, 2007: 17,19)

Potencijalna kriza - to stanje još nije kriza nego postoji mogućnost pojave same krize zbog određenih nedostataka u poslovanju. Jedan primjer bi bio hotelski lanac u vrijeme pandemije virusa Covid-19 gdje bi potencijalnim zatvaranjem granica nastao veliki problem za samu korporaciju koja ima lanac hotela.

Latentna kriza - stanje gdje opasnost već postoji, ali tu opasnost je teško uočiti standardnim ekonomskim instrumentima. Primjer takove krize je korporacija koja financira rast na račun povećanja duga prema dobavljačima. Menadžment takvih poduzeća često nije ni svjestan činjenice da posluju na teret dobavljača. (Sučević, 2010: 12)

Akutna kriza - treći stupanj razvoja krize gdje su simptomi vidljivi u poslovnim procesima te u poslovnim podacima. Akutna kriza podrazumijeva relativno visok pritisak za brzo djelovanje u kratkom vremenskom roku; kad su potrebne jako brze i prave odluke uz istodobno veoma ograničene mogućnosti samog djelovanja pa su akutne krize veliki generator promjena.



Slika 1. Faze kriznog procesa

Izvor: Sučević, 2010

Korporacija koja je u krizi ne mora prolaziti kroz sve prije navedene faze krize. U pojedinim okolnostima korporacija može preskočiti fazu latentne krize te iz potencijalne krize ući u akutnu fazu krize, ovladivu ili neovladivu. U posljednjem slučaju se govori o poslovnoj katastrofi, pogotovo ako je uzrok krize neki vanjski događaj.

Trenutak kada kriza počne bilo u jednom ili drugom smjeru se naziva točkom preokreta. Točka preokreta nije objektivan trenutak s obzirom da ovisi o načinu gledanja, stoga je subjektivna. Sami početak procesa krize se još teže utvrđuje, uzroci krize se nalaze u puno ranijem stadiju. Radi toga je veoma važno sprječavanje krize, što je više moguće ranijim uočavanjem potencijalnih uzroka krize.

2.2.Vrste i uzroci kriza

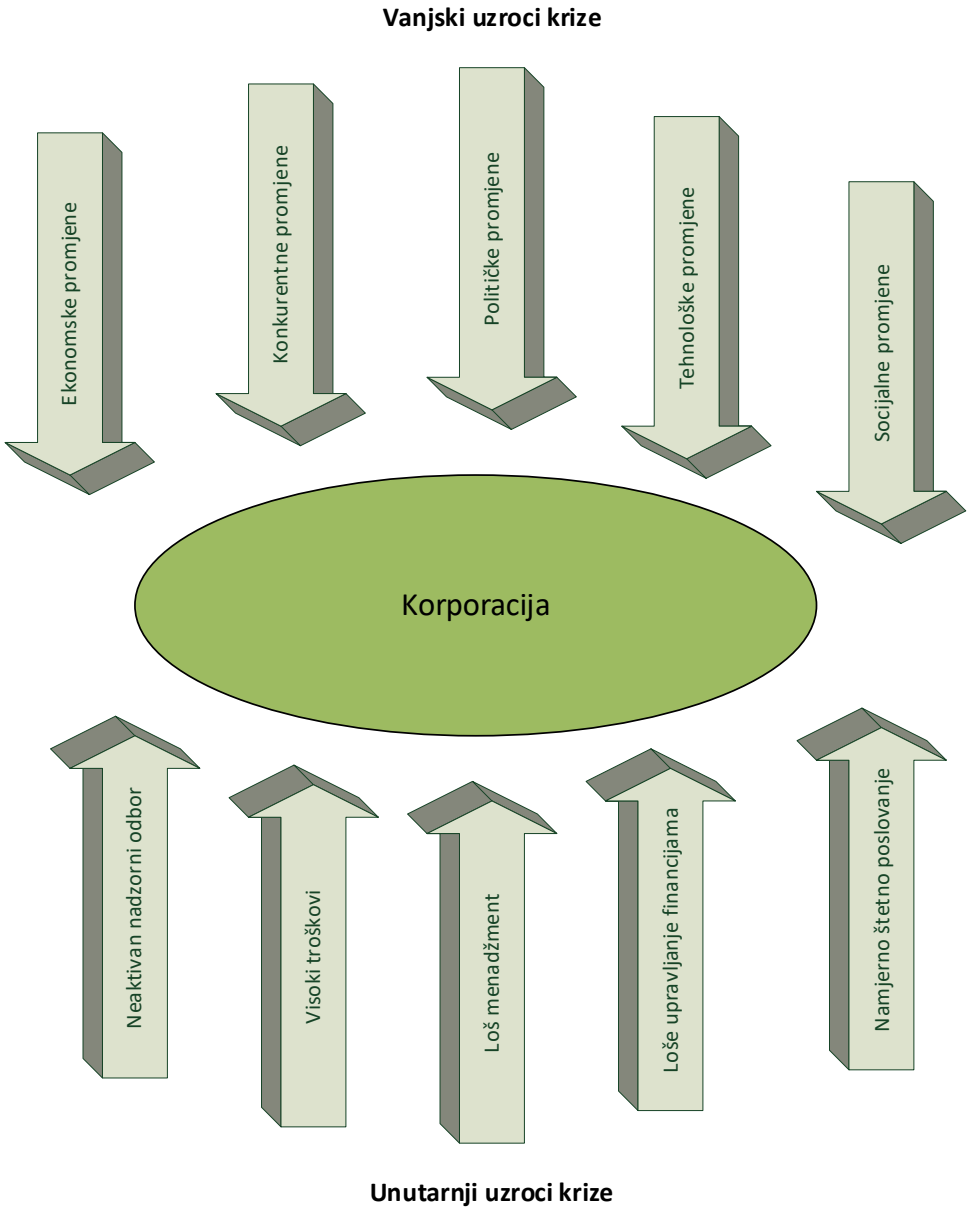
U velikom broju situacija nije moguće u dovoljno dobroj mjeri uvidjeti jesu li krizu uzrokovali vanjski ili unutarnji čimbenici. Mnogi vanjski događaji su predvidivi, ali isto tako mnogi nisu predvidivi. Veoma je važno razlikovati dvije kategorije vanjskih utjecaja.

Prva kategorija su ekonomske, političke ili regulatorne karakteristike tržišta koje su van utjecaja menadžmenta, i bitno ograničavaju njegove akcije. To su ograničenja na koje ne treba trošiti

puno resursa i energije već ih treba prihvatiti i pokušati poslovati po „zacrtanim“ pravilima unutar njih.

Drugu kategoriju sadrže promjene u okolini koje su mnogo više značajnije s menadžerskog gledišta. To su promjene za koje je menadžment morao znati i predvidjeti ih te je na te promjene korporacija morala biti spremna s odgovarajućim akcijskim planom smanjenja rizika. U ovu kategoriju spadaju pojave normalnih poslovnih rizika do nesretne i nepredvidive kombinacije zbivanja na koje niti jedna korporacija nije imuna niti zaštićena.

Unutarnji uzroci krize su posljedica lošeg djelovanja odnosno potpunog nedjelovanja menadžmenta. Nadzorni odbor u svojim definiranim ovlastima može bitno usmjeriti, odnosno ograničiti rad menadžmenta te sa svojim zahtjevima uvelike utjecati na daljnje produbljivanje krizne situacije. Prema raznim provedenim istraživanjima postotak direktne ili indirektne krivnje menadžmenta uvijek iznosi oko 80 %. Loše upravljanje financijama, veliki troškovi poslovanja, namjerno štetno ponašanje kupaca, zaposlenih i uprave spada u unutarnje uzroke krize. (ibidem, 2010: 21 - 27)



Slika 2. Unutarnji i vanjski uzroci krize,

Izvor: uradak autorice

Prema autoru Coombs-u postoje sljedeći tipovi kriza (Jugo, 2017: 69,70):

- Minimalna odgovornost korporacije: To su krize koje podrazumijevaju postojanje elementa žrtve kao direktna posljedice krize. Ona uključuje zlostavljanje, glasine, prirodne katastrofe ili namjerno izazivanje kvarova te nasilje na radnome mjestu

- Niska odgovornost organizacije: To su krize koje podrazumijevaju faktor nesreće ili nezgode te u nju spadaju izazovi, povlačenje proizvoda zbog velikih kvarova i štete te nesreće s tehničkim kvarovima kao posljedice.
- Visoka odgovornost organizacije: U ovoj skupini je uključena mogućnost sprječavanja krize. U nju spadaju ljudske greške, organizacijsko odnosno korporacijsko nedjelovanje bez ozljeda te neprimjereno ponašanje vodstva

Osim gore navedenih podjela, Coombs spominje i druge podjele kriza različitih autora.

Tablica 1: Podjela krize prema autoru Cooms-u

Izvor: Jugo, 2017

Prirodne katastrofe	Potres, tornado, poplava, uragani ili snažne oluje
Nasilje na radnome mjestu	Zaposlenik ili bivši zaposlenik počini nasilje nad drugim zaposlenikom ili zaposlenicima u prostorima u kojima organizacija posluje.
Glasine	Netočne informacije o organizaciji ili njezinim proizvodima namjerno su puštene u opticaj da naštete organizaciji, njezinu poslovanju i ugledu.
Zlonamjernost	Vanjski pojedinac ili suparnik koristi se ekstremnim taktikama, poput sabotiranja proizvoda, otmice, terorizma ili hakiranja radi nanošenja štete organizaciji.
Izazov	Organizacija je suočena s nezadovoljnim sudionicima koji tvrde da se organizacija ponaša ili djeluje neprikladno ili štetno.
Tehničke greške	Tehnologija koju je organizacija osigurala ili se njome koristila zataji ili prouzroči težak industrijski incident ili kvar.
Tehničke greške na proizvodima	Tehnologija koju je organizacija osigurala ili se njome koristila zataji ili prouzroči teški nedostatak ili potencijalno štetan i opasan proizvod.
Ljudske pogreške	Pogreška pojedinca ili skupine pojedinaca uzrokuje nesreću koja posljedično utječe na ugled ili poslovanje organizacije.
Ljudske pogreške na proizvodima	Pogreška pojedinca ili skupine pojedinaca uzrokuje nesreću koja se odražava na proizvodima organizacije.
Organizacijsko nedjelo	Menadžment organizacije poduzima aktivnosti za koje zna da mogu dionike izložiti riziku ili pak svjesno krši zakonske propise.

2.3. Krizno upravljanje

U široj populaciji krizno upravljanje je najčešće poistovjećeno sa pojmom lošeg upravljanja, što ne mora biti slučaj. To vidimo na primjeru kriznog stožera civilne zaštite Republike Hrvatske, koji je osnovan od strane vlade Republike Hrvatske u vrijeme pandemije bolesti Covid-19 radi sprječvanja eksponencijalnog širenja bolesti.

Slika 3. Stožer civilne zaštite RH[1]

Sami pojam kriznog upravljanja se odnosi na sprječavanje i smanjivanje neželjenih posljedica krize kako bi se zaštitila korporacija i njezini članovi od moguće štete.

Krizno upravljanje također ima zadatak aktivnog upravljanja kriznom situacijom. Efikasno krizno upravljanje podrazumijeva i proaktivno upravljanje, odnosno upravljanje koje predviđa potencijalne krizne situacije i planiranje radnji koje će smanjiti neke od mogućih posljedica krizne situacije. Uključenosti svih zainteresiranih dionika u kriznu komunikaciju i dijalog veoma olakšava upravljanje u vremenu krize i pregled te ocjenu donesenih mjera. Dvosmjerna komunikacija je ključni element efikasnog upravljanja u vremenu krize. (Mihaljević, Mihalinčić, 2011: 223)

Krizno upravljanje podrazumijeva:

- Postaviti cilj,
- Napraviti strategiju vođenja krize,
- Napraviti plan djelovanje:

[1] https://vlada.gov.hr/vijesti/nacionalni-stozer-nema-novih-preminulih-osoba-veseli-nas-sto-najveci-dio-gradjana-postuje-mjere-samozastite/29115 , pristupano 1.4.2021

    - Što i kada napraviti te,
    - Gdje i kako napraviti,
- Stvaranje odnosno izazivanje krize,
- Vođenje i upravljanje krizom,
- Rješavanje krize ili njeno neželjeno produbljivanje,
- Ostvarenje planiranog cilja ili njegovo neostvarenje.

Upravljanje u situacijama krize predstavlja veoma složene operacije te suradnju raznih tijela korporacije i pojedinaca s ciljem ostvarivanja sigurne i brze komunikacije, ali i razmjenu stručnih znanja. Može se zaključiti da ljudski faktor predstavlja presudnu ulogu za pozitivno savladavanje stanja krize i sanaciju posljedica krize. (Tatalović, 2015: 15)

Prema samome smislu djelovanja krizno upravljanje možemo razdvojiti na:

1. Krizno upravljanje u širem smislu
2. Krizno upravljanje u užem smislu

U širem smislu krizno upravljanje se odnosi na ukupno djelovanje korporacije usmjereno na krizu. Prema kronološkom slijedu to su sljedeća djelovanja:

    - preventivnog djelovanja prije pojave krize,
    - upravljanje krizom u užem smislu,
    - učenje novih načina djelovanja u prevenciji krize.

U užem smislu krizno upravljanje predstavlja radnje ovladavanja krizom unutar kojih se ublažavaju posljedica krize i trajno ograničavanje posljedica nakon njezine pojave.

3. KRIZNO KOMUNICIRANJE

Komunikacija u vrijeme krize predstavlja dijalog između korporacije i njene javnosti neposredno prije same krizne situacije, ali i tijekom te nakon neželjene situacije ili događaja. Komunikacija se odnosi na stvaranje taktike i raznih strategija koje imaju osnovni cilj smanjiti nastalu štetu na imidž korporacije.

Krizno komuniciranje predstavlja jednu vrstu odnosa sa javnošću jer ima za cilj zaštita ugleda korporacije i održavanje njene pozitivne slike u javnosti. Postoji niz različitih čimbenika koji mogu umanjiti ugled korporacije kao što su:

- kriminalni napadi,
- vladine istrage,
- medijske istrage,
- koruptivne radnje zaposlenika.

Organizacije teže da u vlastitim kadrovima imaju stručnjake za komunikaciju u oblicima raznih kriznih timova kako bi uspješno savladali teške krizne situacije na najbolji mogući i najbrži način u datom trenutku.[2]

Unutar same korporacije krizna komunikacija ima za ulogu smanjenje nesigurnosti pružanjem raznih podataka i činjenica iz povijesti te potvrđivanjem psihološke veze između zaposlenika i kompanije. Tim za krizno komuniciranje komunikaciju mora proširiti do najnižih razina zaposlenika kako bi se izbjegao dojam da se nešto skriva. (Slatter, Lovett, 2011: 176)

Kvalitetno i učinkovito komuniciranje za vrijeme krize podiže moral i zadovoljstvo zaposlenika te zaustavlja raznorazne glasine i nepouzdane informacije. Isto vrijedi i za eksterno komuniciranje čime se zaustavljaju predrasude i predstavlja se svjesnost problema te rješenje istog od strane menadžmenta.

3.1. Teorije kriznog komuniciranje

Kroz različite pristupe krizi definirano je pet teorija kriznog komuniciranja:

1. Apologija – obrambeni govor. Reakcija korporacije na optužbe

[2] https://www.managementstudyguide.com/crisis-communication.htm , pristupano 24.03.2021.

2. Teorija obnove imidža – Kroz ovu teoriju korporacija prati što sve šteti njenom imidžu te radi na popravljanju štetnih stvari
3. Teorija difuzije – Svaka kriza ima za posljedicu veliku potražnju za informacijama i rast potrebe za širenjem informacija. Ova teorija se odnosi na širenje inovacija i ideja te analizira kako korporacije prihvaćaju nove inovacije i ideje
4. Teorija dionika – Dionici su publika sa kojom korporacija uspostavlja dijalog i prema kojima širi poruke. Ova teorija definira kako dionici djeluju na korporaciju, ti dionici mogu biti pojedinci ili vanjske organizacije
5. Situacijska krizna teorija - Ova teorija je jedna od često upotrebljivih teorija u kriznom komuniciranju. Cilj joj je proučavanje percepcije javnosti i odobravanje postupaka korporacije koja je u kriznoj situaciji. Ova teorija ima za pretpostavku da se menadžment u situacijama krize koristi strategijama (poricanje, umanjivanje, ponovna izgradnja, pojačavanje) kao odgovorom na situaciju krize s ciljem očuvanja ugleda korporacije. (Jugo, 2017: 52-54) Dodatno je potrebno naglasiti kako ova teorija komunikacije teži razumjeti, objasniti i ponuditi moguće akcije za krizno komuniciranje. Situacijska krizna teorija se temelji na razumijevanju prijetnje krize koji bi narušila reputaciju korporacije te kako bi iznjedrila odgovarajuću strategiju kao prihvatljiv odgovor na kriznu situaciju. (Tomić, Milas, 2006: 7)

3.2. Strateško komuniciranje

Strateška komunikacija je sredstvo kojim se definiraju ciljevi koje korporacija želi postići u komunikaciji sa javnošću. Ona predstavlja temelj za izradu svih planova aktivnosti koji će se izvoditi tijekom određenog vremena kako bi se široj javnosti kroz medijske kanale pružile sve potrebne informacije i kako bi se stvorila odgovarajuća prepoznatljiva slika u javnosti. Dobro definirana strategija u komunikaciji s javnošću stvara pozitivnu sliku o korporaciji. (Mihaljević, Mihalinčić, 2011: 228)

Korporacije bi trebale biti sposobne komunicirati sve pozitivne elemente krize s ciljem da kriza može predstavljati jedan produktivan proces u organizacijskom smislu. Strategije kojom se krize savladavaju moraju uključivati kako sadašnji tako i budući razvoj. Također teže uvođenjem inovacija koje zahtijevaju visoku spremnost i motiviranost menadžmenta u svim potrebnim aktivnostima i zahtijevaju napuštanje svakodnevnih rutinskih aktivnosti.

Korporacije imaju na raspolaganju dvije temeljenje strategije: aktivna – ofenzivan i pasivna - defenzivna. Kombinacija tih dviju strategije nije nikako preporučljiva jer može stvoriti negativne ishode nakon krize i za njihovo popravljanje je potrebno uložiti mnogo napora i resursa.

3.3. Koncept i važnost komunikacije

Koncept same komunikacije je veoma bitan za uspješno upravljanje tijekom krizne situacije jer daje odgovore na bitna pitanja: Kada se treba koga informirati? Tko to mora učinit? Što se koga traži? Dobar koncept obuhvaća sve razine korporacije, dokumentira kada je što kome preneseno i definira kada tko dalje dobiva informacije. Menadžment mora definirati sve te procese (kada, tko, gdje, kome i kako daje informacije). Ovisno o agilnosti same korporacije stvaranje koncepta i definiranje procesa komunikacije može iziskivati velike resurse. Radi postojanja neformalne organizacije unutar same organizacije dobra praksa je organizacijska snimka stanja same korporacije i traženje pomoći vanjskih suradnika u kreiranju koncepta komunikacije.

Sama komunikacija se dešava na tri razine:

- Menadžment - Sastanci kriznog menadžmenta i uprave, na tim sastancima se upravlja procesom izlaska iz krize, donose se odluke i definira se koje sve informacije mogu slati i točno na koji način.
- Menadžment sa najbližim suradnicima – Sastanak čine uprava i najbliži suradnici. Nakon toga menadžment pojedinih vertikalnih jedinica dalje obavještavaju linijske rukovoditelje.
- Menadžment i svi zaposleni – širenje informacija svim zaposlenima (zbor radnika ili na neki drugi način). Takvi sastanci trebaju prenijeti informacije o trenutnom stanju i napredovanju upravljanja kriznom situacijom. Najčešće su kratki te informativni i stvaraju osjećaj zajedništva. (Osmanagić Bedenik, 2007: 233,234)

Osim komunikacije u vrijeme krize važna je komunikacija i nakon krize, sve s ciljem prevencije posljedica krize. Tako sve poruke prije svega moraju biti dosljedne te moraju biti prilagođene interesima, ciljanim skupinama i odgovarajućim medijima. Platforma za uspješnu prevenciju posljedica krize je osiguranje kontinuirane funkcionalne komunikacije bilo u vidu raznih internih tjednika i mjesečnika ili tzv. „newsletter“ email-ova. Komunikacija za vrijeme trajanja

krize mora biti iskrena, pravovremena s objavom informacija, mora se razgovarati sa ugroženim skupinama, mora dati rješenje problema i iskazivati empatiju te žaljenje.

Najčešće greške u kriznom komuniciranju su nedostatak komunikacijske platforme, nepripremljenost na krize, manjak agilnosti u brzini reakcije te nejasno prenošenje poruka.

3.4. Odnos kriznog komuniciranja i reputacije

Krizna komunikacija ima veliki utjecaj na očuvanje reputacije. Reputacija je status korporacije u javnom prostoru. Ona se vrlo teško i dugo gradi, a vrlo se lako i brzo gubi. U današnje vrijeme reputacija je jako važan element svake korporacije i uvelike utječe na tržišnu vrijednost korporacije. Kada se korporacija nađe u krizi reputacija je pod udarom te može doći do cjelokupnog gubitka reputacije što može rezultirati padom vrijednosti dionica korporacije. Kako bi korporacije zaštitile svoju reputaciju, posebno u vrijeme krize, potreban je jasni kanal komunikacije s javnosti. Također potrebno je napraviti analizu postojećeg stanja kompanije i otpornosti na rizike sve sa ciljem za smanjenjem potencijalnih posljedica krize i očuvanja reputacije. (Anthonissen, 2008)

Kako je spomenuto reputacija je status koji se dugo gradi, tako je prethodno redovno kvalitetno komuniciranje sa javnosti temelj kriznog komuniciranja. Poznata lica u javnosti stvaraju poveznicu i određeni stupanj povjerenja što automatski zadržava dulje vrijeme reputaciju na višoj razini.

Krizno komuniciranje se ne smije samo koncentrirati na očuvanje reputacije već mora odavati i dojam da menadžment ima jasno ucrtan put ka savladavanju krize, u suprotnome će se izgubiti vjerodostojnost.

Iz svega spomenutog jasno je da svaki nedostatak komuniciranja smanjuje reputaciju korporacije i vjerodostojnost u rješavanju krizne situacije.

4. KORPORATIVNA SIGURNOST

Jedna od prikladnih definicija korporativne sigurnosti bi bila: ukupnost i zbroj svih aktivnosti usmjerenih na prevenciju i otklanjanje posljedica ugrožavanja koje bi na bilo koji način dovodile u pitanje normalno funkcioniranje korporacije ili njenog jednog dijela. (Djurkin Konig i sur., 2020: 22)

Pojam korporativne sigurnosti je u današnje vrijeme vezan uz ova tri značenja:

1. Planska aktivnost koju provode korporacije s ciljem zaštite imovine, osoba te poslovanja,
2. Kolegij koji se proučava na raznim studijskim programima,
3. Posebna znanstvena disciplina.

Korporativna sigurnost je mlada znanstvena disciplina koja je nastala simbiozom iz ostalih više usko specijaliziranih znanstvenih disciplina. U Republici Hrvatskoj još nije potpuno konstituirana. U zemljama zapadnog svijeta korporativna sigurnost ima bogatu i dugu tradiciju kako u akademskom smislu tako i u samoj primjeni u praksi. Tako je u nekim zemljama korporativna sigurnost dobila strateško značenje.

U počecima formiranja znanstvene discipline korporativne sigurnosti ostatak akademske zajednice je pružao otpor u daljnjem akademskom razvoju te discipline pošto je dio te tematike pokriven kroz nacionalnu i ekonomsku sigurnost. (ibidem, 2020:22) Druga primjedba akademske zajednice je ta što za obavljanje djelatnosti u sferi korporativne sigurnosti nisu potrebna znanstvena znanja već su potrebne odgovarajuće vještine i umijeće. Međutim razvojem privatnog vlasničkog odnosa i dolaskom novih oblika kapitala kao i razvojem korporacija javile su se potrebe znanstvenog pristupa problematici korporativne sigurnosti.

Za prikladnu provedbu sigurnosti potrebno je napraviti niz aktivnosti i prethodnih radnji koje dosta korporacija i investitora preskače smatrajući da je to gubitak novca i vremena. Dakle u trenutku planiranja neke korporacije nužno je definirati i određene sustavne mjere zaštite. Sama sigurnost bi trebala štititi cjelokupnost korporacije ali na način da ne „razbija“ ustaljeni načina rad osim ako je to neophodno. Preduvjet za razvoj svih drugih oblika sigurnosti unutar korporacije.

4.1. Suvremeni pristup konceptu korporacijske sigurnosti

Kroz lateralno širenje pojma sigurnosti u 90-im godinama prošlog stoljeća postaje sve veća potreba za korporacijskom sigurnošću. U novijim literaturama korporativan sigurnost se smatra jednim od pet novih sektora (pored vojnog, političkog, socijalnog i ekološkog). U velikom broju zemalja korporacijska sigurnost se tretira kao pod cjelina ekonomske sigurnosti te u globaliziranom svijetu ima sve značajniju ulogu.

Novi konceptualni okvir koji se razvija unazad godinama, utemeljen je na zahtjevima koji teže ka minimiziranju prijetnji i ka maksimiziranju mogućnosti u sferi korporativne sigurnosti. Slojevita više disciplinarna priroda međunarodne ekonomije čini korporativnu sigurnost upotrebljivom zbog mogućnosti povezivanja i sinteze uvida iz različitih disciplina u holistički okvir analize. U Hrvatskoj koncept suvremene korporacijske sigurnosti nije još potpuno razrađen iako je formaliziran kao integralna sigurnost i kao dio nacionalne sigurnosti. (Djurkin Konig i sur., 2020:28)

Suvremeni koncept danas polazi od tri postavke:

- Nedostajanje svijesti o postojanju ugroze korporacija i mogućnost uspostave pripadajućih sigurnosnih mehanizama,
- Sigurnost nije jednostavno već je strategijsko pitanje unutar svake korporacije,
- Nedostatak koncentracije na unutarnje uzroke narušavanja sigurnosnih procedura.

Jedan od primjera proboja unutarnjih sigurnosnih procedura je curenje podataka iz američke NSA agencije od strane vanjskog računalnog konzultanta pod imenom Edward Snowden.

Slika 4. Edward Jospeh Snowden – afera curenja NSA podataka[3]

[3] https://www.pcmag.com/news/the-10-most-disturbing-snowden-revelations , pristupano 1.4.2021

Dosadašnji koncept je primarno usmjeren na fizičku zaštitu osoba i imovine u korporacijama te na mehanizme sigurnosti informacijskih sustava dok novi koncept sigurnosti se definira kao ukupnost sigurnosti poslovnih sustava koja se ostvaruje sa više mehanizama, postupaka, procedura, mjera i aktivnosti u sferi zaštitnog i sigurnosnog karaktera. ((Djurkin Konig i sur., 2020:28)

Suvremeni koncept korporativne sigurnosti mora zadovoljiti sve moderne zahtjeve u korporativnom okruženju kao i zahtjeve koji se odnose na korištenje modernih i visoko sofisticiranih tehnologija, digitalizaciju poslovnih sustava i procesa te na nove sigurnosne prijetnje i rizike koji mogu ugroziti korporaciju.

4.2. Razvoj i oblikovanje korporativne sigurnosti

Danas niti jedna korporacija koliko god bila moćna i stabilna nije imuna na iznenadne događaje i sva moguća eksterna i interna iznenađenja. Kako bi poslovanje korporacije bilo uspješno i stabilno menadžment mora biti sposoban predvidjeti i procijeniti sve prijetnje i događaje kao i njihove posljedice te definirati poslovni odgovor na te događaje. Instrument za takvo stabilno poslovanje je upravo korporacijska sigurnost. (Djurkin Konig i sur., 2020:29)

U Hrvatskoj se korporativna sigurnost trenutno tek institucionalizira te se radi razvoj i ispostava svih elemenata sustava zaštite i sigurnosti unutar korporacija.

Kako je trenutno vrijeme intenzivnog uvođenja novih tehnologija pojavile su se nove prijetnje i rizici, infrastruktura postaje jedan od važnijih stupova zaštite. To su razlozi radi kojih menadžment mora prepoznati važnost razvoja sigurnosno – zaštitne komponente u korporaciji bez obzira ne temeljnu djelatnost korporacije. Tako je u posljednje vrijeme zabilježen rast investiranja u razvoj sustava za korporativnu sigurnost. Kako je sve teže razlučiti granicu javnog i privatnog interesa kada se radi o potrebama zaštite poslovanja, imovine i osoba sve više i više se uspostavlja suradnja između korporativne i javne sigurnosti. Spomenuto se vidi i na primjeru pravila stožera civilne zaštite RH kada se propisana epidemiološka pravila primjenjuju preko internih timova za korporativnu sigurnost. Također je u posljednje vrijeme vidljiva sve veća edukacija i profesionalno usavršavanje kako zaposlenika tako i menadžmenta radi usvajanja zvanja i procedura adekvatnog sigurnosnog ponašanja i razvijanja kulture sigurnosnog ponašanja. (ibidem, 2020:30)

Kako svaki poslovni sustav tako i sustav korporativne sigurnosti ima svoja osnovna obilježja, karakteristike i posebnosti koje ga razlikuju od drugih organizacijskih dijelova korporacije. Temeljno obilježje sustava korporativne sigurnosti je to da predstavlja cjelokupnu integriranu zaštitu korporacije, dakle zaštita svih vrijednosti i resursa. Tako niti jedan subjekt, mehanizam ili procedura iz domene sigurnosti ne može biti izvan okvira sustava za zaštitu korporacije već predstavlja njegov integralni dio. Iz navedenog proizlazi da sigurnosne i zaštitne aktivnosti moraju biti planirane, uređene, podržane materijalno i logistički te zaposlenici educirani. U suprotnome će se pojaviti ne efikasnost i loša reakcija na detekciju prijetnji i saniranje štete i gubitaka. Dakle unutar procesa upravljanja mora postojati element sigurnosti.

Cilj svake korporacije je sigurnost poslovnog uspjeha tako se sve više i više ulaže u korporativnu sigurnost te se pred urede korporativne sigurnosti postavljaju sljedeći ciljevi: (ibidem, 2020:31)

- Svesti faktore ugroze na minimum,
- Eliminirati rizike i ugroze koji bi mogli utjecati na poslovne aktivnosti i uspjeh,
- Osigurati poslovno funkcioniranje u bilo kojim uvjetima krize, bez obzira na obim i vrstu,
- Sanirati sve posljedice nepredvidivih događaja i normaliziranje poslovnih procesa.

Ako korporacija ima složenu organizacijsku strukturu tada će i struktura sustava korporacijske sigurnosti biti usklađena sa tim zahtjevima te potrebama i funkcionirat će kao jedinstveni sustav sa ostalim elementima korporacije. Dakle sustavnim pristupom sustav korporativne sigurnosti mora obuhvatiti sve organizacijske dijelove korporacije.

4.3. Pravno uređenje korporativne sigurnosti u Republici Hrvatskoj

Osim poslovnih i organizacijskih osnova potrebno je urediti i normativno pravne osnove korporativne sigurnosti. Kako je prije spomenuto, koncept korporativne sigurnosti je napravljen ali postoje određena neslaganja po pitanju sadržaja i širine djelovanja poslova koje bi korporacije trebale raditi same te koji bi se poslovi radili preko kompanija za pružanje sigurnosnih usluga. (Djurkin Konig i sur., 2020:33)

Strategijom nacionalne sigurnosti RH napravljena je veza između korporativne odnosno privatne sigurnosti i javne sigurnosti. Cilj je sinergija djelovanja, brze reakcija na krizu,

sprječavanje i uklanjanje posljedica krize te što brži povratak u stanje prihvatljivog poslovnog funkcioniranja.

Kako poslovno nestaju granice koje definiraju osobno, nacionalno i međunarodno sigurnosno djelovanje Republika Hrvatska u strategiji nacionalne sigurnosti navodi da treba napraviti partnerstvo za složene rizike te da će iz tog partnerstva izaći učinkovit sustav domovinske sigurnosti. Taj sustav bi trebao biti sve obuhvatan, suvremen, racionalan i učinkovit. Dakle paradigma pristupa koji sadrži pristup kroz obranu, policiju i sigurnosno obavještajni sustav zamijenit će pristup koji će dodatno uključiti gospodarske subjekte, i akademske i stručne institucije, javni i privatni sektor te razne organizacije iz civilnog društva.

Ono što je krucijalno je nedostatak nekog od propisa koji bi što preciznije uredio sustav korporativne sigurnosti. Tako korporacije iz ustava i propisa koji su prestali vrijediti a u kojima se navodi pravo na zaštitu imovine i drugih vrijednosti vuku temelje i metodologiju za sigurnosnu djelatnost. (ibidem, 2020:34)

U zemljama gdje postoji duga tradicija korporativne sigurnosti to područje je regulirano kroz posebne zakone ili su u okviru šireg područja ekonomske sigurnosti.

5. OBLICI UGROŽAVANJA POSLOVANJA, IMOVINE I OSOBA

5.1. Suvremeni izazovi u sigurnosti korporacija

Sve veća globalizacija, otvaranje granica, integracije i migracije stvaraju potpuno novu poslovnu okolinu kako na nacionalnom tako i na internacionalnom poslovanju te se kompanije susreću sa velikim spektrom prijetnji, sigurnosnih izazova i nesigurnosti. S obzirom na sve spomenute prijetnje koje konstantno utječu na rad, kompanije moraju imati implementiranu sigurnosnu komponentu u svim procesima poslovanja te u funkcijama upravljanja.

Prema istraživanjima provedenim u SAD-u spominje se šteta od okvirno 300 milijardi američkih dolara kao posljedica gubitka poslovnih informacija. U današnje vrijeme upravo poslovne informacije i nematerijalni resursi čine oko 80 posto vrijednosti kompanija. (Djurkin Konig i sur., 2020:37)

Kako je razvoj informacijsko-informatičkih tehnologija informacije pretvorio u vrijedan resurs tako su one postale roba vrijedna kao dobro poput, kapitala, radne snage i zemlje. Upravo zbog spomenutog informacijska sigurnost je postala kritična komponenta i odgovornost izvršnog menadžmenta i uprave te se podrazumijeva da ima organizacijsku strukturu i odgovarajuće procese. Tehnološke kompanije koje se bave razvojem aplikacija u čijoj domeni postaje ograničenja na autorsko pravo najvažnije resurse smatraju poslovnom tajnom i posebnu pozornost obraćaju na takove resurse.

Mnogi istraživački podaci govore da dosta kompanija nema adekvatan odgovor na razne oblike opasnosti, rizika i ugroza te su zbog toga razni poslovni procesi i sustavi postali ugroženi. Da bi kompanije spriječile posljedice tih opasnosti, rizika i ugroza s ciljem očuvanja stabilnosti, konkurentnosti i profitabilnosti kompanije sve veću pažnju posvećuju korporativnoj sigurnosti. Tako korporativna sigurnost u sve većem broju kompanija postaje ne samo strateško pitanje već strateška funkcija. Tako inercija razvoja korporativne sigurnosti u kompanijama uzrokuje i sve veću suglasnost države i poslovnih subjekata u domeni rješavanja sigurnosnih pitanja.

5.2. Stvarne prijetnje i oblici ugroza korporacija

Svaki sustav posjeduje imovinu čija stvarna vrijednost ovisi o nizu faktora (tržišni uvjeti, kapital, infrastruktura), posljedično vrste ugroza možemo klasificirati prema teritorijalnoj ili

prostornoj dimenziji na ugroze koje imaju izvor unutar kompanije, izvan kompanije ili kombinirano. ((Djurkin Konig i sur., 2020:39)

Oblici prijetnje koji imaju uzrok unutar kompanije su najčešće sljedeći:

- Materijalna šteta,
- Razna oštećenja,
- Disfunkcije koje su nastale slučajno nemarom, nehatom ili neznanje.

Unutarnji oblici prijetnji su najčešći i za posljedicu stvaraju velike štete za kompanije i rijetko se za njih snosi odgovornost. U manjem obimu se javljaju štetna djelovanja koja su uzrokovana namjerno te je u tim slučajevima opseg štete veoma velik. Neki od primjera namjernog djelovanja su:

- Krađa materijala, opreme ili predmeta,
- Razni oblici ekonomskog kriminala,
- Diverzija i sabotaža.

Ponekad su izvori unutarnjih prijetnji nesavjesno i nelojalno ponašanje zaposlenika prema kompaniji i kršenje raznih propisanih sigurnosnih i pisanih procedura. Ali s obzirom na posljedice djelovanja najveću štetu izaziva korupcija.

Vanjske oblike ugroza se vidi kroz različite načine djelovanja, a najčešći su imovinski kriminal i različite vrste političkog kriminala. Ponekad su vidljive i nezakonite i neprimjerene radnje koje direktno i indirektno nanose štetu drugim kompanijama poput:

- Nelojalne konkurencije,
- Ugroza poslovanja i imovine,
- Bojkot drugih kompanija.

U vanjske oblike ugroze spadaju i događaji koji su izravna posljedica prirodnih katastrofa i raznih tehničko tehnoloških nesreća.

Osim spomenutog, podjela s obzirom na izvor ugroze, u nekim stručnim literaturama je vidljiva i sljedeća podjela prijetnji i ugroza: (ibidem, 2020:41)

- Prirodne nesreće: potresi, poplave, požari,

- Tehnološko – tehnike nezgode,
- Društvene prijetnje: to su one koje su direktna posljedica djelovanja čovjeka.

Vidljivo je da je mogući katalog prijetnji dosta velik stoga kompanije moraju imati spremne odgovore na bilo koji vid prijetnji makar to bile i prijetnje koje imaju čisto ekonomski karakter (restrikcije, sankcije i razna ograničenja)

5.3. Oblici ugroze poslovanja

Svaki poslovni sustav i proces je izložen raznim ugrozama. Tako su moguće ugroze u području proizvodnje, trgovine, deviznog poslovanja, blagajničko poslovanja, .itd. U posljednje vrijeme umjesto pojma gospodarski kriminal sve češće vidimo pojam korporacijski kriminal. Glavna karakteristika mu je dinamičnost odnosno prilagodljivost okolini. Stručnjaci iz domene kriminalistike smatraju da je takova vrste kriminala sve više multinacionalna.

Vidljivo je da je osim prevara i krivotvorenja javnih isprava zabilježen rast kriminalnih radnji u području fiskalnih obaveza, poreza na promet, isplata plaća, dnevnica, pranja novca i slično.

Jedan primjer iz ugroze poslovanja je „Afera Dnevnice“:

Slika 5. Afera dnevnice[4]

5.4. Oblici ugroze imovine

Neke vrste imovine koje mogu biti pod ugrozom su: proizvodni pogoni, infrastrukturni objekti, gotovi proizvodi i sl., a neke od ugroza koje mogu djelovati su požari, potresi, poplave ili razni

[4] https://www.tportal.hr/vijesti/clanak/nepravomocno-je-okoncana-socna-afera-dnevnice-podsjecamo-na-bizarne-detalje-sa-sudenja-od-touretteova-sindroma-do-kolekcije-cipela-foto-20201216 , pristupano 1.4.2021

tehničko - tehnološki faktori. Ovisno o udaljenosti od izvora negativnog događaja razlikuje se stupanj oštećenja imovine i vrijednost nastale štete te iznos gubitaka. Spomenuti izvori ugroze imovine nisu toliko učestali, imovina je učestalije pod ugrozom od ljudskog djelovanja radi nemara, nehata i nesavjesnog djelovanja.

Jedan od primjera ugroza imovine je bio požar unutar Data Centra tvrtke OVHcloud koji je za posljedicu imao nedostupnost velikog broja web stranica na području Europe.

Slika 6. Požar OVHCloud Data Centra[5]

5.5. Oblici ugroza osoba

Postoji niz ugroza na radnom mjestu koje mogu ugroziti sigurnost i zdravlje radnika. Prema zakonodavstvu Republike Hrvatske svaki poslodavac mora osigurati siguran radni proces i mora provoditi sve potrebne mjere zaštita na radu i zaštite zdravlja na radu. Kroz podzakonske propise odnosno pravilnike o procjeni rizika razrađene su sve opasnosti koje dovode u pitanje sigurnost i zdravlje radnika. Na temelju procjena rizika poslodavac mora primjenjivati mjere i postupke za smanjenje rizika i mora osigurati visoku razinu zaštite na radu. Pri izradi procjene

[5] https://www.jutarnji.hr/vijesti/svijet/pozar-unistio-servere-tehnoloske-tvrtke-ovhcloud-najvece-europske-tvrtke-za-spremanje-podataka-15056771, pristupano 1.4.2021

rizika moraju biti uključeni radnici ili njihovi predstavnici, poslodavac te razni stručnjaci iz raznih područja. Prema Pravilniku o izradi rizika razlikujemo: (ibidem, 2020:44)

- Opasnosti: mehaničke, od padova, od električne struje, od požara, od eksplozija, …,
- Štetnosti: fizikalne, biološke i kemijske,
- Napore: napor govora, napor vida, psihofizički napor te statodinamički napor.

Osim spomenutog sigurnost radnika može biti narušena kroz razne kriminalne radnje, to je posebno vidljivo na radnim mjestima gdje je pohranjena veća količina novca.

Jedan od primjera ugroze osoba je pljačka banke:

Slika 7. Ilustracija pljačke banke[6]

5.6. Cyber kriminal

Cyber kriminal je najčešće usmjeren na zloupotrebu ili krađu informacija koje su pohranjene digitalno. Neke definicije računalni ili cyber kriminal određuju kao zloupotreba računala u bilo kojem smislu gdje se korištenjem računalne tehnologije žrtva ili trpi ili bi mogla trpjeti štetu a počinitelj djeluje sebi u korist.

[6] https://www.nbcconnecticut.com/news/local/woodbridge-police-seek-gun-wielding-bank-robber/2202504/ , pristupano 1.4.2021

Prema Europskoj konvenciji o računalnom kriminalitetu razlikujemo četiri grupe djela: (Djurkin Konig i sur., 2020:45)

- Djela protiv povjerljivosti, integriteta i dostupnosti računalnih podataka,
- Djela vezana uz računala,
- Djela vezana uz sadržaj,
- Djela vezana uz kršenje autorskih prava.

Nadalje računalni kriminal možemo još podijeliti na politički, ekonomski, proizvodnju i distribuciju nedozvoljenih i štetnih sadržaja te na povredu računalne privatnosti.

Jedan od primjera cyber kriminala je lažiranje „web shop“ prodaje:

Slika 8. Ilustracija lažnog web shopa[7]

5.7. Ekološki kriminal

Prema teoriji pod ekološki kriminalom se smatraju sve kriminalne radnje koje imaju za štetne posljedice zagađenje zraka, vode, zemljišta i ekosistema. To su dakle sve radnje koje ugrožavaju okoliš i zdravlje ljudi.

Najčešći primjeri ekološkog kriminala su: (Djurkin Konig i sur., 2020:46)

[7] https://www.tedxdharavi.com/list-of-fake-timberland-sites , pristupano 22.3.2021

- Nelegalne emisije supstanci u okoliš,
- Nelegalna trgovina životinjama ili biljkama,
- Nelegalna trgovina supstancama koje uništavaju ozonski omotač,
- Nelegalna trgovina opasnim otpadom.

S obzirom na globalne potrebe za resursima i mogućnosti visokog profita radnje iz ekološkog kriminala su u velikom porastu.

Jedan od primjera ekološkog kriminala je ilegalna sječa šuma:

Slika 9. Ilustracija ilegalne sječe šuma[8]

[8] https://www.24sata.hr/news/kazna-420000-kn-za-sjecu-sume-bez-potrebne-dozvole-167972 , pristupano 15.3.2021

6. SIGURNOST I ZAŠTITA RADNIKA UNUTAR KORPORACIJA POD RIZICIMA BOLESTI COVID-19

Nakon pojave epidemije koja je uzrokovana bolesti Covid-19, države članice EU-a su uvele postepeno niz mjera koje utječu na radna mjesta a sve s ciljem daljnjeg sprječavanja širenja bolesti. Sami opseg djelovanja mjera nije unificiran za sve zemlje članice EU, tako su u nekim zemljama potpuno zatvorene djelatnosti koje nisu nužne (najčešće uz neki zamjenski dohodak) te je u nekim djelatnostima preporuka čim većeg opsega rada od kuće.

Nakon što mjere pokažu dovoljno smanjenje zaraženih osoba po danu, najčešće se uvodi postepeno popuštanje mjera i vraćanje radnih djelatnosti koje nisu nužne u ponovni rad.

Kriza koju je generirala bolest Covid-19 stvara veliki pritisak i na poslodavce i na radnike, bilo u provedbi mjera u kratkom vremenu bilo u potpunoj obustavi poslovnih aktivnosti.

Kao i pri normalnim radnim uvjetima, identificiranje i procjena rizika u radnom okruženju je početna točka za upravljanjem korporativnom sigurnosti i zdravljem radnika u okviru mjera protiv bolesti uzrokovane virusom Covid-19. Pri svakoj promjeni radnih uvjeta poslodavac mora nanovo evaluirati rizike a posebno one koji utječu na mentalno zdravlje. (ibidem str 78) Nakon procjene rizika opet se izrađuje odgovarajući akcijski plan sa primjenom pripadajućih mjera.

U Republici Hrvatskoj poslodavac je dužan pratiti preporuke Stožera civilne zaštite RH i drugih nadležnih organa te je dužan pratiti upute HZJZ-a. Osim spomenutih preporuka i uputa te općih načela prevencije utvrđene Zakonom o radu poslodavci se moraju pridržavati i posebnih mjera.

Prema Zakonu o radu poslodavac mora: (Zakon o radu, Narodne novine, broj 93/14, 127/17, 98/19)

- Poslodavac mora radniku osigurati sve uvjete za rad na siguran način te na način koji ne ugrožava zdravlje radnike, u skladu s posebnim zakonom i drugim propisima,
- Prilikom rada na izdvojenom mjestu, poslodavac je dužan radniku osigurati sigurne uvjete rada, a radnik se mora pridržavati svih zdravstvenih i sigurnosnih mjera u skladu s posebnim zakonom i drugim propisima,
- Prilikom sklapanja ugovora o radu i tijekom trajanja radnog odnosa radnik je dužan obavijestiti poslodavca o bolesti ili bilo kojoj drugoj okolnosti koja ga onemogućuje ili

ometa u većoj mjeri za obavljanje svih obavezan definirane ugovorom o radu ili o okolnosti koja ugrožava život ili zdravlje osoba s kojima radnik dolazi u kontakt,

- Uputiti radnika na liječnički pregled radi utvrđivanja zdravstvene sposobnosti zbog obavljanja određenih poslova.

Osim zakona o radu poslodavac ima i određene obaveze sukladno Zakonu o zaštiti na radu, a te obveze su: (Zakon o zaštiti na radu, Narodne novine, broj 7/14, 118/1, 154/14, 94/18, 96/18)

- Organiziranje i provedba zaštite na radu, vodeći pri tome brigu o prevenciji rizika i obavještavanju, osposobljavanju, organizaciji i sredstvima,
- Imati procjenu rizika izrađenu u pisanome ili elektroničkom obliku, koja odgovara postojećim rizicima na radu i vezano s radom te koja je dostupna radniku na samome mjestu rada,
- Pravovremeno dati zaposlenicima upute o načinu postupanja u slučaju nastanka neposrednog rizika za život i zdravlje kojemu je radnik ili izložen ili bi mogao biti izložen, kao i o mogućim mjerama koje je potrebno provesti radi sprječavanja ili smanjenju rizika. Poslodavac je obvezan provoditi davanje obavijesti i podataka na način da čuva privatnost radnika u skladu sa posebnim propisom o zaštiti osobnih podataka.

6.1. Pripravnost korporacija na pandemiju Covid-19

Da bi kompanija išla zdravim korakom prema naprijed te da bi bila uspješna potreban joj je plan i program kako funkcionirati u normalnim situacijama, Ali također joj je potreban plan i program za nepredvidive i iznenadne situacije poput pandemije uzrokovane virusom Covid-19.

Kako se niti jedna korporacija dosad nije susrela sa bolesti Covid-19 skoro sve kompanije bilo u manjem ili većem obimu su po utjecajem posljedica bolesti Covid-19.

Najbolji način za umanjivanje rizika je spremnost, umjesto panike i improvizacije. U nastavku je dan primjer tablice spremnosti koju koriste korporacije u Kanadi. (Djurkin Konig i sur., 2020: 80)

Tablica 2. Pripravnost korporacija na pandemiju

Izvor: Djurkin Konig i sur., 2020: 81

POSTUPAK	STVARI KOJE TREBA RAZMOTRITI
Razviti / ažurirati planove kontinuiteta poslovanja i krizne planove	• Kakav je postupak donošenja odluka u vrijeme krize? • Kako identificirate i štite osnovne korporativne evidencije i dokumente vaše tvrtke? • Koje su kritične usluge, pozicije i vještine potrebne za održavanje vašeg poslovanja? • Kako i kada komunicirate s unutarnjim i vanjskim dionicima i kako upravljate protokom informacija? • Kakav je vaš plan za oporavak?
Imajte u planu potencijalni utjecaj pandemije na vage poslovanje.	• Koliki je rizik od pandemije za vaše zaposlenike, partnere, dobavljače i kupce • Tko su članovi tima za odgovor na pandemiju i koje su njihove uloge i odgovornosti? • Koji su okidači i postupci za aktiviranje i ukidanje plana odgovora na pandemiju? • Kakav je postupak odlučivanja povezan s pandemijom i izvršavanjem plana za kontinuitet poslovanja? • Tko su vaši najvažniji zaposlenici i koji su drugi resursi (npr. sirovine, dobavljati, usluge/ proizvodi podizvođača i logistika) potrebni za održavanje poslovanja prema lokaciji i funkcijama tijekom pandemije? • Kako se pripremate za značajnu odsutnosti osoblja? • Imate li alate i tehnologiju koja radnicima omogućuje rad na daljinu? • Jeste li obučavali i pripremali radnu snagu i pričuvne resurse? • Budete li prisiljeni zatvoriti vrata na dva ili više tjedana, imate li pristup kreditnoj liniji koja će vam pokriti tekuće troškove sve dok se ne mognete ponovo otvoriti i dok se novčani tok ne nastavi? • Kakav je vaš plan za scenarije koji će vjerojatno rezultirati povećanjem ili smanjenjem potražnje za vašim proizvodima i/ili uslugama tijekom pandemije (npr. znak zabrana okupljanja većeg broja ljudi, potreba za higijenskim potrepštinama)? • Kako procjenjujete i upravljate potencijalnim utjecajem pandemije na vaše financije koristeći više mogućih scenarija? • Kakav je utjecaj pandemije na domaća i međunarodna poslovna putovanja? • Koji su vaši Izvori relevantnih, vjerodostojnih ažurnih podataka o pandemiji iz saveznog, pokrajinskoga lokalnog javnog zdravstva, kriznog stožera I drugih izvora? • Je li vaš plan komunikacije u Izvanrednim situacijama ažuriran i jesu Ii utvrđene i priopćene ključne uloge i odgovornosti? Taj plan bi trebao uključivati identifikaciju ključnih kontakata (s pričuvama), lanac komunikacije (uključujući dobavljače i kupce) i procese za praćenje I dojavljivanje o statusu poslovanja i zaposlenika. • Kakva je vaša trenutna putna politika i je li ju potrebno ažurirati? • Je li vaš plan testiran?
Imajte u planu potencijalni utjecaj pandemije na vaše ljude	• Koje korake možete poduzeti kako biste zaštitili zdravlje i sigurnost osoblja i posjetitelja vašeg radnog mjesta? • Koje su prakse kontrole infekcije na vašem radnom mjestu? • Koju zaštitnu i preventivnu opremu te alate trebate postaviti kako biste spriječili širenje infekcije? • Kako i koliko često komunicirate sa zaposlenicima, kupcima i dobavljačima? • Kako pratite i upravljate strahom, tjeskobom, glasinama i dezinformacijama medu zaposlenicima? • Imate li uspostavljene platforme (npr. pozivni centar, web stranica itd.) prema zaposlenicima, dobavljačima, kupcima itd. preko kojih prenosite podatke o statusu i djelovanju pandemije i odgovarate na njihova pitanja? • Postoje li, ako je potrebno, smjernice i prakse koje možete izmijeniti ili uspostaviti kako biste umanjili izravan kontakt s javnošću? • Trebaju li se ažurirati propisi o dopustu zaposlenika kako bi odražavali jedinstvene okolnosti zbog pandemije? Jesu li u skladu s vašim provincijskim propisima o radu? • Imate uspostavljenu politiku radnih mjesta i radnog vremena? • Imate Ii uspostavljenu politiku prema zaposlenicima koji su možda bili ili misle da su možda bili izloženi virusu? • Koje su zdravstvene usluge dostupne zaposlenima? • Koje usluge zaštite mentalnog zdravlja mogu biti pružene tijekom pandemije i moguće karantene? • Postoje li zaposlenici i klijenti s posebnim potrebama kojima se treba prilagoditi?

6.2. Uloga korporativne sigurnosti u sprječavanju širenja bolesti Covid-19

Korporativna sigurnost je operativna i strateška funkcija korporacije koja upravlja svim vrstama incidenata koji mogu na bilo koji način ugroziti sigurnost organizacije i njene najvrijednije imovine – zaposlenika. (Djurkin Konig i sur., 2020:84)

Voditelji korporativne sigurnosti moraju anticipirati nove rizike za korporaciju. Da bi to mogli, moraju biti u toku sa globalnim ranjivostima. Korporativna sigurnost je primarno usmjerena na sigurnost i zaštitu zdravlja zaposlenika a zatim i na sve preventivne radnje radi sprječavanja gubitka informacija , cyber zaštitu, tehničku i tjelesnu zaštitu, zaštitu od požara i dr. Voditelji korporativne sigurnosti su zaduženi za cjelokupno vođenje svim sigurnosnim procesima od procjene rizika do provedbe određenih mjera.

Voditelji kroz multidisciplinarno iskustvo te poznavanje više vrsti rizika i prijetnji će doprinijeti tome da će njihova korporacija biti sigurnosno bolje otpornija i pripremljenija od ostalih korporacija. (ibidem, 2020:84)

S obzirom na situaciju sa širenjem bolesti Covid-19, unutar samih korporacija korporativna sigurnost je preuzela operativno provođenje mjera stožera civilne zaštite RH i HZJZ-a sve s ciljem daljnjeg sprječavanja daljnjeg širenja bolesti.

6.3. Minimiziranje širenja bolesti Covid-19 na radnome mjestu

Sudjelovanje predstavnika radnika u procesu upravljanja zdravljem na radu i sigurnosti je ključno za obranu od bolesti na radnome mjestu a ujedno je i zakonska obaveza. Spomenuti korak je ključan za brzu reakciju u vremenu velike tjeskobe i nesigurnosti među zaposlenima.

Također uključivanje radnika u procese procjena rizika je dobra praksa za zdravstvenu i sigurnosnu preventivu radi što bolje operativnog provođenja mjera, pošto se same mjere najviše reflektiraju na zaposlenike.

Dakle sinergija poslodavca i zaposlenike je prijeko nužna. Neki od primjera mjera koji se odnose na poslodavca i zaposlenike su dani u narednim tablicama

Tablica 3. Mjere za poslodavce

Izvor: Djurkin Konig i sur., 2020: 85

Postavljanje važnih obavijesti: na vidljivim mjestima na ulazu u prostor tvrtke postaviti edukacijske plakate i sve važne upute o zaštiti zdravlja Stožera civilne zaštite Republike Hrvatske, Hrvatskog zavoda za javno zdravstvo i Epidemiološke službe (upute o pravilnom pranju i dezinfekciji ruku, zadržavanju razmaka medu osobama i druge mjere).
Uvođenje obveze radnicima da prije dolaska na posao izmjere tjelesnu temperaturu. U slučaju povišene tjelesne temperature od 37,2 stupnja i viša, ne dolaze na posao već se javljaju svom obiteljskom liječniku i pretpostavljenom.
Osiguranje osobne zaštitne opreme: osigurati dovoljan broj jednokratnih zaštitnih rukavica i maski, zaštitnih odijela za tijelo, nanogica, zaštitnih kapa i sl. u ovisnosti o procesima rada i staviti na raspolaganje radnicima te nadzirati njihovu uporabu.
Olakšajte radnicima dolazak na posao osobnim vozilima radije nego javnim prijevozom, primjerice, omogućite im parkirna mjesta za automobile ili sigurnu pohranu bicikala i potičite ih da pješke dolaze na posao, ako je to moguće.
Za odlaganje korištene jednokratne zaštitne opreme na vidljivim i dostupnim mjestima postavite spremnike s poklopcem koji imaju oznaku za odlaganje korištene zaštitne opreme.
Postavite dezinfekcijske barijere za obuću na ulazu(ima) u organizaciju.
Postavljanje fizičkih barijera: gdje je moguće postaviti zaštitne pregrade u vidu stakla, pleksiglasa ili sličnog materijala, kako bi se smanjio kontakt radnika i stranke, a samim time i rizik širenja zaraze.
Potičite pojačano pranje ruku tekućim sapunom i tekućom toplom vodom slijedom preporuka HZJZ i Hrvatskog Crvenog, križa.
Osiguranje mjesta za dezinfekciju ruku. Postavite dezinfekcijska sredstva za ruke već kod samog ulaza u organizaciju.
Osiguranje udaljenosti između osoba od najmanje 2 metra: preraspodjelom prostora, preraspodjelom radnog vremena/rad u smjenama, smanjenjem broja osoba koje istovremeno borave u prostoriji ili na prostoru, omogućiti rad od kuće ili u iznimnim situacijama postavljanjem pregrada.
Minimiziranje prijema vanjskih stranaka uz obvezu njihova beskontaktnog mjerenja tjelesne temperature. U slučaju postojanja povišene tjelesne temperature od 37,2 i više stupnjeva strankama se ne omogućuje ulazak u organizaciju.
Sprječavanje okupljanja više od 5 osoba: sastanke održavati online, a komunikaciju na mjestima rada održavati putem telefona, e-maila i sl., ograničiti broj radnika koji istovremeno koriste pauzu na način da ju koriste u različitim vremenskim intervalima.
Kada je sastanak neophodan i neodgodiv, organizirajte ga do 5 sudionika u što većim prostorijama uz cik cak raspored sjedenja. Prethodno dezinficirajte sve radne i podne površine prostorije kao i uredske uređaje.
Održavanje čistoće objekta i mjesta rada: čistiti i dezinficirati mjesta rada koliko je god moguće više puta (dezinfekciju obavljaju stručne osobe s propisanim i učinkovitim kemijskim sredstvima), a posebnu pažnju posvetiti čistoći sanitarnih čvorova i označavanju istih, ukoliko je moguće omogućiti korištenje većeg broja primjerenih kemijskih WC-a.
Najmanje dva puta dnevno čistiti sve dodirne površine: radne površine, dizala za prijevoz osoba, pametne i druge telefone, POS ureduje, tipkovnice, konzole, računala te druge dodirne površine koje koristi veći broj osoba.
Provjetravanje radnih prostorija i prostora: potrebno je što je moguće češće osigurati dotok svježeg zraka te omogućiti izmjene zraka provjetravanjem radnih prostora i prostorija.
Izradite i protokol dijeljenja službenih vozila koji se odnose na maksimalan broj osoba u automobilu, načinu njihova sjedenja, uvjetima nošenja maski i dezinfekcije unutrašnjosti automobila.
Osigurati posebnu zaštitu kroničnim i onkološkim bolesnicima: svim kroničnim i onkološkim bolesnicima omogućiti obavljanje rada od kuće gdje god je to moguće.
Osigurati nesmetani rad stručnjacima zaštite na radu i drugim osobama zaduženim za sigurnost: organizirati provedbu štetnih unutarnjih nadzora kao i provođenje nadzora pridržavanja mjera za sprječavanja širenja korona virusa.

Tablica 4. Mjere za zaposlenike

Izvor: Djurkin Konig i sur., 2020: 87

Provoditi mjere zaštite osigurane od strane poslodavca: primjenjivati upute o pravilnom pranju i dezinfekciji ruku, zadržavanju razmaka medu osobama i sl. te istu provoditi. Koristiti preuzetu jednokratnu zaštitnu opremu te istu prema uputi odlagati u kantu za otpad koja ima poklopac i propisano zbrinjavati takav otpad. Redovito provoditi osobnu higijenu.
Osobna zaštitna oprema: osobnu zaštitnu opremu koju koriste u skladu s propisima iz zaštite na radu potrebno je propisano odlagati na mjesta koja je odredio poslodavac.
Kašljanje i kihanje: prekriti usta i nos laktom ili papirnatom maramicom koju je poslije potrebno odbaciti u koš za otpad s poklopcem te obvezno nakon toga oprati ruke. Pri kašljanju i kihanju okrenuti lice od drugih osoba.
Izbjegavanje dodirivanja lica, usta i očiju rukama: lice, usta i nos dodirivati isključivo nakon dezinfekcije ruku ili pranja sapunom i vodom.
Izbjegavati rukovanje ili bilo kakve druge dodire ili diranje korištenih maramica ili korištenih osobnih zaštitnih sredstava i sl.
Socijalni kontakt: ostvarivati samo najnužnije socijalne kontakte unutar obitelji, a u kontaktu s kolegama držati propisani razmak bez rukovanja i sličnog kontakta.
Simptomi: postoji li sumnja na simptome zaraženosti korona virusom, ne dolaziti na posao te obavijestiti svog liječnika ili nadležnog epidemiologa te početi provoditi postupak samoizolacije i daljnje mjere u skladu sa stručnim medicinskim preporukama.
Hitnost: u slučaju hitnosti obratiti se svom stručnjaku zaštite na radu, poslodavcu, liječniku ili nazvati 112.

6.3.1. Osobna zaštitna oprema

U vremenu pandemije bolesti Covid-19 zahtijevaju se dodatne mjere opreza i zaštite zdravlja radi maksimalnog sprječavanja širenja bolesti. Mjere predostrožnosti koje se provode na radnim mjestima gdje se ostvaruje socijalni kontakt su upotreba osobne zaštitne opreme te njihov pravilan odabir i edukacija o samom korištenju opreme.[9]

Najčešća zaštitna oprema koja se koristi je jednokratna zaštitna maska i jednokratne zaštitne rukavice. Spomenuta oprema se nakon jednog nošenja mora odbaciti u kantu za otpad sa poklopcem. Prije i nakon korištenja opreme potrebno je oprati ruke.

[9] https://narodne-novine.nn.hr/clanci/sluzbeni/2021_01_5_111.html , pristupano 1.4.2021

Osim jednokratnih maski, još se koriste FFPP2 i FFPP3 zaštitne maske koje se mogu koristiti više puta te za tu opremu proizvođač mora napraviti određene radnje oko ocjenjivanja sukladnosti sa prikladnim normama i izraditi odgovarajuću dokumentaciju.

6.3.2. Čišćenje i dezinfekcija prostora

Čišćenje poslovnih prostora provode osobe zadužene od strane poslodavca. U tijeku pandemije preporuka je što češće čistiti radne prostore. Kod samih poslova čišćenja potrebna je briga sigurnosti i zaštiti zdravlja osoba koje obavljaju čišćenje.

Dezinfekciju radnih prostora moraju provoditi osobe koje su ovlaštene za to te moraju koristiti propisana sredstva i kemikalije a sve u skladu sa pripremljenim uputama i protokolima.[10]

6.3.3. Rad od kuće

Kako je u većini zemalja preporuka ili je za dio radnih mjesta propisana mjera fizičkog distanciranja, radnike se uveliko potiče na rad od kuće. Za većinu zaposlenika ta promjena je nova i postoji mnogo nedostataka u odnosu na radno mjesto. (Djurkin Konig i sur., 2020:91)

Da bi rad od kuće bio funkcionalan i da se postigne pozitivno iskustvo potrebno je uzeti u obzir par jednostavnih stvari:

- Odabir mikro lokacije za radni prostor,
- Osigurati dobro osvjetljenje,
- Izabrati dobar stol i stolicu,
- Razmišljati o zdravlju i sigurnosti.

6.3.4. Upravljanje aktivnostima radnika koji rade od kuće

Europska agencija za sigurnost i zdravlje na poslu predlaže niz smjernica za zaposlenike koji nisu mogli adekvatno mogli pripremiti radno mjesto kod kuće na odgovarajući način:[11]

- Potrebno je provesti procjenu rizika uključujući i radnike koji rade od kuće,

[10] https://zdravstvo.gov.hr/UserDocsImages/2020%20CORONAVIRUS/Korona-prostorije_.pdf , pristupano 1.4.2021

[11] https://uznr.mrms.hr/obavljanje-poslova-na-izdvojenom-mjestu-rada-i-oslobada-je-od-obveze-dokumentiranja-procjene-rizika/, pristupano 1.4.2021

- Potrebno je omogućiti zaposlenicima privremeno uzimanje opreme za rad kući,
- Osigurati radnicima upute za rad na ergonomičan i što zdraviji način,
- Potaknuti zaposlenike na redovito uzimanje stanke,
- Osigurati što kvalitetniju potporu u pogledu IT opreme i softvera,
- Pobrinuti se da postoji dobra horizontalna i vertikalna komunikacija,
- Kako postoji rizik da se zaposlenici osjećaju izolirano potiče se održavanje redovitih mrežnih sastanaka,
- Osigurati fleksibilnost radnog vremena radi ostalih članova obitelji. Uvijek postoji mogućnost da bračni partner također radi na daljinu ili da djeca pohađaju nastavu online,
- Pomoći zaposlenicima u definiranju i postavljanju ciljeva i zdravih granica s obzirom na nove okolnosti radnog mjesta.

6.4. Preporuke za projektiranje ureda i rad nakon Covid-19

Za sada je poznato da je jedini put prijenosa zaraze bolesti direktni kontakt s osobe na osobu kapljičnim putem pa je za očekivati da će centralizirani uredi biti glavna mjesta širenja bakterija i virusa.

Kako će se mjere smanjivati za očekivati je povratak zaposlenika na posao. Sukladno tome postojat će zabrinutost zbog moguće infekcije unutar ureda. Prema tome slijede neke od preporuka za što sigurniji rad u prostorima unutar korporacije: (Djurkin Konig i sur., 2020:93)

- Poželjno je koristiti klizna vrata za ulaz u zgradu radi nepotrebnog dodirivanja površine vrata,
- Zaštitari i osoblje recepcije bi trebalo biti zaštićeno zaštitnom pregradom od pleksiglasa,
- Preporučiti zaposlenima da koriste što više stepenice umjesto dizala,
- S obzirom na trend gušćeg smještaja ljudi u urede i smanjivanje radnih stolova za očekivati je rijeđenje ljudi unutar ureda i povećanje radnih stolova,
- Preporuka je zadržavanje kombiniranog rada, djelomično u uredu djelomično od kuće,
- Provoditi politiku čistog stola bez osobnih stvari,
- Uvođenje zabrane dijeljenja radnih stolova,
- Uvesti podne oznake s vidljivom distancom od 2 metra,
- Sobe za sastanke organizirati na način da je moguća kvalitetna ventilacija zraka i da je jasno vidljiv broj ljudi koji može biti prisutan na sastanku,

- Poticati korištenje virtualnih platformi za sastanke,
- Poticati što veću digitalizaciju poslovanja,
- Što češće čišćenje i držanje urednim prostora čajnih kuhinja.

6.5. Unutarnji nadzor za provođenje mjera sprječavanja širenja bolesti Covid-19

Prema uputama za poslodavce i zaposlenike za provođenje mjera sigurnosti i zaštite zdravlja izdanih od ministarstva rada i mirovinskog sustava napomenuto je: „ Kako bi se postigao visok stupanj sigurnosti i zaštite zdravlja radnika, u ovom trenutku potrebna je posebna angažiranost stručnjaka zaštite na radu“. (Djurkin Konig i sur., 2020:95)

Tako je tim zadužen za zaštitu na radu dužan svakodnevno provjeravati zaposlenike da li se pridržavaju propisanih mjera. Ukoliko se uoči da se zaposlenici ne pridržavaju propisanih mjera nužno je obavijestiti poslodavca i predložiti odgovarajuće mjere kako bi se u što kraćem roku otklonile nepravilnosti.

6.6. Moderna rješenja u funkciji smanjenja širenja bolesti Covid-19

Moderna rješenja mogu uključivati neke od ovih sustava a sve s ciljem što sigurnijeg rada:

- Aplikacija sa mikro lokacijama punktova za čišćenje ruku,
- Softverski sustav za brojanje dodira lica,
- Sustav za izdavanje vjerodajnica za sastanke i za kontrolu napućenosti prostorija,
- Korištenje umjetne inteligencije u kombinaciji sa termalnim kamerama i infracrvenim toplomjerima,
- Sustav za kontrolu socijalne distance temeljen na video analizi,
- RFID narukvice koje signaliziraju prebliske kontakte.

Sva spomenuta rješenja moraju biti implementirana u skladu sa ograničenjem GDPR-a.

7. CYBER PRIJETNJE U VREMENU PANDEMIJE COVID-19

U vrijeme pandemije vidljiva je briga za zdravlje zaposlenika i održavanje operativnog poslovanja. Međutim kako su informacijsko komunikacijske tehnologije postale važan resurs korporacija nije moguće zanemariti važnost cyber i informacijske sigurnosti. ((Djurkin Konig i sur., 2020:101)

Svaki odgovor na prijetnju bi trebao biti u okviru plana upravljanja incidentima te u okviru plana upravljanja kontinuitetom poslovanja, no u praksi su vidljivi aspekti koji utječu na sigurnost korporacija:

- Vidljiv je nesustavan porast broja ljudi sa udaljenim pristup na IT resurse korporacije bez prethodne ocjene rizika,
- Sukladno porastu rada od kuće porastao je i broj mjesta i mreža sa kojih zaposlenici pristupaju IT resursima,
- Sukladno spomenutom porastao je i mogući broj mjesta koji mogu biti ulazna točaka za kibernetički napad,
- Sigurnosni operativni centri zbog manjka svjesnosti korisnika gube nadzor nad radnim stanicama korisnika dok se nalaze na radu van prostorija korporacija,
- Naglo je i nesustavno porastao broj servisa koje korisnici koriste te je nastao razdor između stvarnog i dokumentiranog stanja po pitanju IT resursa.

Vidljivo je po raznim istraživanjima da je porastao broj napada i ranjivosti IT sustava u vremenu pandemije bolesti Covid-19.

Sigurnosni timovi bi trebali uspostaviti sustav koji će omogućiti prikupljanje informacija za forenziku i analizu prijetnji i rizika te bi trebali implementirati mjere koji će biti što manje invazivne u odnosu na postojeće poslovne procese. U takvim okolnostima osobe zadužene za sigurnost IT sustava unutar korporativne sigurnosti bi trebale osvijestiti ostale korporacijske funkcije o važnosti sigurnosti informacijskih sustava.

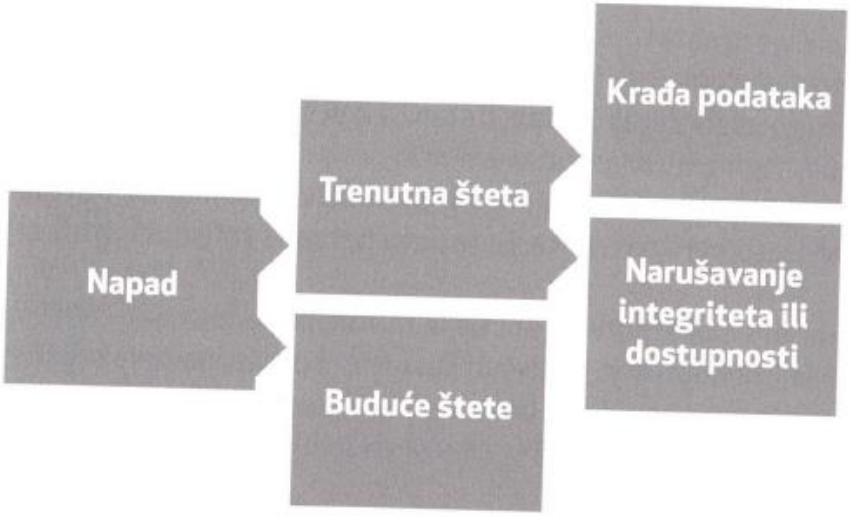
Slika 10. Uspostava sigurnosti IT sustava

Izvor: Djurkin Konig i sur., 2020: 102

7.1. Napadi na IT resurse

Vidljivo je da je za vrijeme pandemije Covid-19 povećan broj alata za napad i mehanizma napada na korporacijske IT resurse, posebno se to odnosi na vektor napada na korporacijska računala koje zaposlenici koriste kod kuće.

Cilj napad nije jednoznačan, ponekad je cilj napada samo računalo zaposlenika te informacije na njemu a ponekad je računalo zaposlenika samo iskorišteno za pristup na ostale IT resurse korporacije, bilo trenutno bilo u budućnosti.



Slika 11. Tijek i plan napada na IT resurse

Izvor: Djurkin Konig i sur., 2020: 102

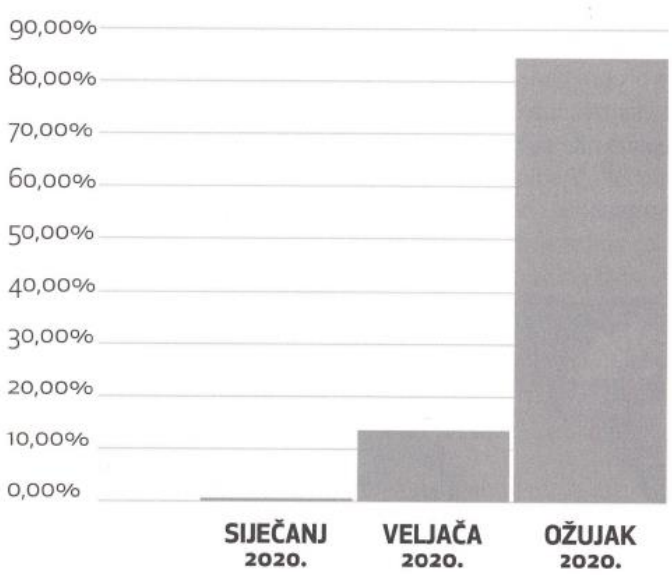
Jedan od značajnih napada na IT resurse u Republici Hrvatskoj je napad na korporaciju INA d.d., koji se desio početkom 2020. godine.

Slika 12. Primjer IT napada na korporaciju INA d.d.[12]

7.2. Phishing napadi

Phishing napad je napad zlonamjernom email porukom gdje se ili lažira pošiljatelj poruke ili je u tijelo poruke umetnut zlonamjeran link ili je korištena kombinacija oboje spomenutog radi prikupljanja i zloupotrebe informacija.

U 2020. godini je posebno porastao trend korištenja tematike virusa Covid-19 za Phishing napade što je vidljivo na slici u nastavku.

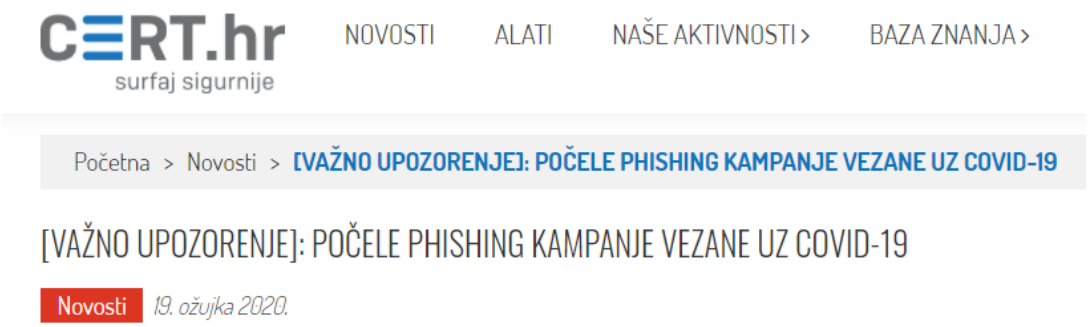


Slika 13. Postotak poruka vezanih uz Covid-19

Izvor: Djurkin Konig i sur., 2020: 103

[12] https://www.bug.hr/sigurnost/hakerski-napad-na-ina-u-provjerili-smo-neke-nesluzbene-navode-i-sto-se-trenutno-13938 , pristupano 24.3.2021

Čak je i svjetska zdravstvena organizacija upozorila da se njen identitet zloupotrebljava od strane hakera te da su i oni primili zlonamjerne email poruke. Također je i Hrvatski računalni tim za hitne slučajeve (CERT) upozorio na zlonamjerne email poruke s Covid-19 tematikom.



Slika 14. Objava CERT-a o phishing napadima[13]

7.3. Zlonamjerni programi

Hakerske skupine su po početku pandemije krenule prilagođavati zlonamjerne programe i kreirati nove sve s ciljem iskorištavanja trenutne situacije. Najveći vektor napada distribucije zlonamjernih programa je bio pomoću elektroničke pošte, a najveći izvori odnosno pošiljatelji poruka su bili iz SAD-a, Turske i Nizozemske.

Slika 15. Pregled izvora poruka sa zlonamjernim programima

Izvor: Djurkin Konig i sur., 2020: 104

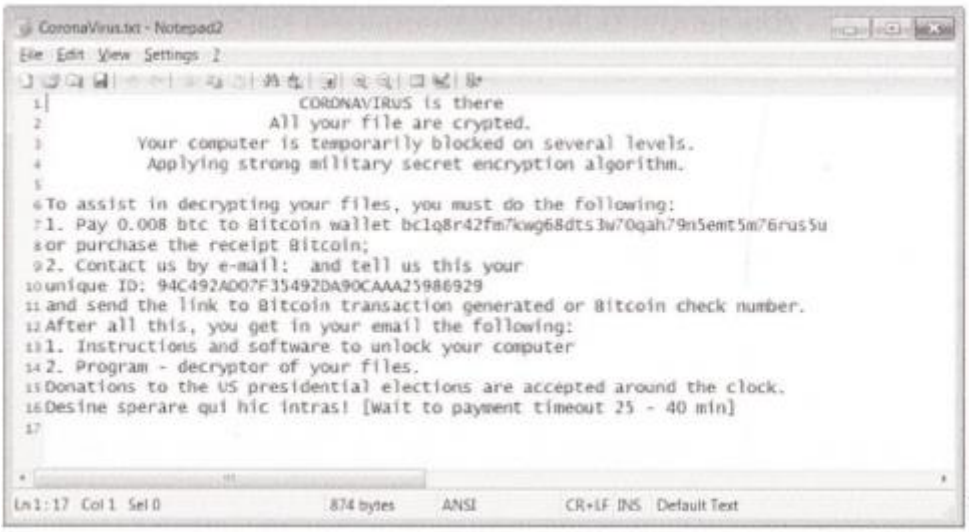
[13] https://www.cert.hr/PhishCoviD, pristupano 26.3.2021

U ožujku 2020. godine se pojavila zlonamjerna kampanja koja je promovirala zlonamjerni antivirusni program naziva „Corona Antivirus“.

Slika 16. Izgled zlonamjerno linka sa Corona antivirus programom

Izvor: Djurkin Konig i sur., 2020: 105

Također je vidljiva i upotreba Ransomware-a koji je prikazivao poruke vezane uz naziv „Covid“ i „Coronavirus“. Ransomaware-a je zlonamjerni program koji zaključava i kriptira datoteke na računalu nakon čega hakeri traže određeni iznos za otključavanje tih datoteka. U nastavku je dan prikaz jedne takove poruke.



Slika 17. Izgled poruke Ransomware programa nakon zaključavanja datoteka

Izvor: Djurkin Konig i sur., 2020: 105

8. PLANIRANJE OPORAVKA POSLOVANJA

„Svjetska zdravstvena organizacija (WHO) proglasila je COVID-19 javnozdravstvenom prijetnjom međunarodnog razmjera. COVID-19 je postao ljudska tragedija i podjednako utječe na vlade i tvrtke neviđenim izazovima i rizicima. Kriza je to koja ima duboke posljedice za tvrtke širom svijeta. Od potpunog ili djelomičnog zatvaranja tvornica, poremećaja u lancu opskrbe, otpuštanja radne snage do problema novčanog toka, tvrtke osjećaju poslovni i financijski šok od izbijanja pandemije.“[14]

Postoji niz pitanja i stvari o kojima bi poslovni lideri korporacija trebali razmišljati kao i niz koraka koje je preporučeno poduzeti radi promijene i oporavka svog poslovanja te radi utjecaja pandemije koja je nastala.

Slijedi pet koraka kao mogući način odgovora na utjecaj i oporavak poslovanja.

Prvi korak: Staviti prioritet na sigurnost ljudi i omogućavanje kontinuiranog angažmana

Potrebno je osigurati rješavanje briga oko ljudi na otvoren i nadasve transparentan način te ih je potrebno uvjeriti u kontinuitet poslovanja. Kako su ljudi nesigurni oni traže kvalitetne smjernice od korporacija, vlade i svoje bliže zajednice.

Drugi korak: Izmijeniti strategiju za kontinuitet poslovanja

Većina korporacija će doživjeti značajne promjene u odnosu na ustaljeni način poslovanja te će se suočiti s raznim oblicima neučinkovitosti poslovanja tijekom i neposredno nakon trajanja pandemije. Da bi korporacije što lakše prebrodile poteškoće preporuča se sljedeće:

- Procjena kratkoročne likvidnosti
  Korporacije će uvesti kratkoročno praćenje toka novca s ciljem pravovremenog predviđanja pritiska na novčani tijek i mogućnost brze intervencije. Htjeti će postaviti i održati disciplinu i konstantnost u pogledu radnog kapitala, poglavito oko naplate potraživanja i upravljanjem zaliha. U vrijeme krize naročito je bitno biti kreativan i proaktivan kako bi bio lakši ciklus radnog kapitala.
- Procjena operativnih i financijskih rizika

[14] https://www.ey.com/hr_hr/covid-19/covid-19-business-recovery-planning-for-private-businesses , pristupano 1.4.2021

Korporacije moraju detaljnije nadzirati razne eskalacije troškova i njihov utjecaj na ukupnu maržu proizvoda ili usluga, intervenirajući i pregovarati kada je to nužno. Korporacije također moraju biti svjesne svih pritisaka koji mogu djelovati na kupce, dobavljače, izvođače i partnere. Također potrebna je svjesnost kršenja sporazuma sa financijskim institucijama i bankama radi rizika umanjenja vrijednosti imovine i možebitnog utjecaja na zdravlje ukupne bilance.

- Razmotriti izmjenu duga i kreditnog ugovora
  Kako korporacije mogu imati problem sa tokom novca zbog krize u poslovanju, većih troškova nastalih kao izravna posljedica pandemije ili smanjenih prihoda, postoji mogućnost potrebe dodatnog financiranja, izmjene postojećih ugovora ili odricanja ako više nije moguće zadovoljavanje ugovora o dugu.
- Uzimanje u obzir alternative mogućnosti lanca opskrbe
  Tvrtke koje dobavljaju materijale ili dijelove od dobavljača koji su pod utjecajem Covid-a 19 morati će potražiti alternativne dobavljače
- Utjecaj krize pandemije na proračun i na poslovne planove
  Korporacije će testirati utjecaj pandemije na financijske planove u više mogućih scenarija i povećat će broj pregleda proračuna radi mogućeg utjecaja krize na financijske performanse i procjenu trajanja utjecaja krize.

Treći korak: Komunikacija sa relevantnim dionicima

„Jasna, transparentna i pravovremena komunikacija potrebne su prilikom stvaranja platforme za preoblikovanje poslovanja i osiguranja stalne podrške od kupaca, zaposlenika, dobavljača, kreditora, investitora i regulatornih tijela.“[15]

Kupci: Korporacije će obavijestiti kupce o bilo kojim utjecajima koji mogu promijeniti rok isporuke usluga ili proizvoda. Ako se uoči da obveze iz ugovora neće moći biti ispoštovane bitno je održati otvoreni i transparentni način komunikacije radi revidiranja vremenskih rokova ili mogućnosti pozivanja na klauzulu „više sile“. Ovakva proaktivnost će zasigurno smanjiti novčanu odštetu ili obveze koje su povezane s obećanjem prema kupcima.

Zaposlenici: Prema zaposlenicima treba komunicirati plan koji će imati balans opreza, zaštite zdravlja i redovnog poslovanja

[15] Ibidem, pristupano 1.4.2021

Dobavljači: Radi sposobnosti redovne isporuke robe i usluga tijekom pandemije Covid-19 korporacije moraju redovito komunicirati sa dobavljačima uzimajući u obzir plan rizika i oporavka u slučaju traženja alternativnih mogućnosti lanca opskrbe.

Vjerovnici i investitori: Tvrtke će željeti ispitati uvjete i odredbe raznih ugovora o zajmu radi identifikacije dugova da bi izbjegle tehničko kršenje duga. Takovi pregledi imaju dodatnu korist jer tvrtkama omogućuju proaktivni dijalog i komunikaciju sa kreditorima vezano uz potrebu izmjene trenutnih postojećih uvjeta i refinanciranja.

Vlada i regulatori: Korporacije će morati komunicirati sa internim pravnim timovima radi savjeta o potencijalnim obvezama prema vladi ili regulatorima te pojasniti način komunikacije u slučaju mogućih kršenja obveza.

Četvrti korak: Maksimizacija korištenja podrške države

„Vlade diljem svijeta ubrzano razvijaju nove mjere za rješavanje ekonomskih izazova s kojima su suočene industrije, tvrtke i zaposlenici. Mnoge su države već uvele fiskalne i / ili monetarne mjere namijenjene olakšavanju izazova nastalih u COVID-19.

Kako se razvijaju nove mjere, tvrtke bi trebale raditi na praćenju regulatornih i zakonodavnih promjena, analizirati kako se politike primjenjuju na njihovo poslovanje, dijeliti ekonomske probleme i prijedloge politika s vašim regulatorima i zakonodavcima, te komunicirati moguće nove prednosti zaposlenicima.“[16]

Peti korak: Izgradnja otpornosti

Nakon što se nova strategija poslovanja krene primjenjivati te nakon što se njene smjernice kvalitetno prenesu svim dionicima one će se morati krenuti provoditi uz temeljito praćenje. Rukovodstvo će morati pravodobno prijaviti svaka odstupanja od planiranih radi daljnjeg smanjenja negativnog utjecaja.

Nakon što se utjecaj pandemije stavi pod kontrolu potrebno je napraviti reviziju planova za kontinuitet poslovanja i prilagoditi ga novim uvjetima sve s ciljem otpornosti na postojeću te na daljnje moguće krize.

[16] Ibidem, pristupano 1.4.2021

9. ZAKLJUČAK

Razvojem poslovnih organizacija u velike cjeline poput korporacija, iste osim organizacijskih problema nailaze na razne predvidive i nepredvidive sigurnosne probleme, od kojih je jedan i bolest Covid-19. Tako organizacije osim standardnih organizacijskih dijelova iz ekonomskih i područja primarnog djelovanja radi kvalitetnog upravljanja i prevencije sigurnosnih incidenta osnivaju organizacijske cjeline za korporativnu sigurnost.

Korporativna sigurnost je relativno novi pojam i logički dio organizacije, a krasi ga multidisciplinarni pristup koji je prijeko potreban radi složenih sigurnosnih događaja pod čijem su utjecajem korporacije.

Da bi se dobro razumjelo djelovanje korporativne sigurnosti bitno je savladati i upoznati teoriju krize, kriznog komuniciranja te ugroza koje utječu na poslovanje i na sve vrste resursa koje korporacija posjeduje.

U ovome radu je vidljivo da dobro organizirani tim koji upravlja korporativnom sigurnošću može itekako doprinijeti osiguranju svih resursa korporacije, od ljudskih preko materijalnih do informacijskih. Također se zaključuje da korporativna sigurnost mora pratiti kompleksnost svih organizacijskih procesa da bi adekvatno mogla procijeniti, upravljati i spriječiti sve vrste sigurnosnih incidenata.

U budućnosti se očekuje jasnije definiranje pravnog položaja i dosege djelovanja timova za korporativnu sigurnost, pošto je u ovome trenutku nejasno koji doseg upravljanja rizicima i incidentima može korporacija obavljati sama a iznad kojeg dosega mora konzultirati ili obavijestiti vanjske organizacije ili službe.

10. LITERATURA

10.1. Popis knjiga, časopisa i članaka

1. Anthonissen, P. (2008). Crisis Communication: Practical PR Strategies for Reputation Management & Company Survival, Kogan Page Publishers, London.

2. Djurkin-Konig L., Ostojić A., Delić A., Mihaljević B. (2020). Korporativan sigurnost u vrijeme pandemije Covid-19, Business Security Academy, Zagreb.

3. Jugo, D. (2017): Menadžment kriznog komuniciranja, Udžbenici sveučilišta, Sveučilište u Dubrovniku, Školska knjiga, Zagreb.

4. Osmanagić- Bedenik, N. (2007): Kriza kao šansa-Kroz poslovnu krizu do poslovnog uspjeha, Udžbenici Sveučilišta u Zagrebu, Školska knjiga, Zagreb.

5. Slatter, S., Lovett, D. (2011): Kako svaku tvrtku izvući iz krize, Mozaik knjiga, Zagreb.

6. Sučević, D. (2010) : Krizni menadžment-Vodič kroz planiranje, prevenciju i oporavak s primjerima iz prakse, Lider, Zagreb.

7. Tomić Z., Milas Z. (2007): Strategija kao odgovor na krizu, Politička misao : časopis za politologiju, Vol. 44 No. 1, str. 137-149., Fakultet političkih znanosti, Zagreb.

8. Zakon o radu Narodne novine, broj 93/14, 127/17, 98/19

9. Zakon o zaštiti na radu, Narodne novine, broj 7/14, 118/1, 154/14, 94/18, 96/18

10.2. Popis internetski izvora

1. https://dku.hr/wp-content/uploads/2016/09/zbornik2011.pdf , 20.03.2021. g.

2. https://dku.hr/wp-content/uploads/2016/09/DKU-2015-VVG.pdf , 20.03.2021. g.

3. https://www.managementstudyguide.com/crisis-communication.htm , 22.03.2021 g.

4. https://vlada.gov.hr/vijesti/nacionalni-stozer-nema-novih-preminulih-osoba-veselinas-sto-najveci-dio-gradjana-postuje-mjere-samozastite/29115 , pristupano 1.4.2021 g.

5. https://www.pcmag.com/news/the-10-most-disturbing-snowden-revelations , pristupano 1.4.2021 g.

6. https://www.tportal.hr/vijesti/clanak/nepravomocno-je-okoncana-socna-afera-dnevnice-podsjecamo-na-bizarne-detalje-sa-sudenja-od-touretteova-sindroma-do-kolekcije-cipela-foto-20201216 , pristupano 1.4.2021 g.

7. https://www.jutarnji.hr/vijesti/svijet/pozar-unistio-servere-tehnoloske-tvrtke-ovhcloud-najvece-europske-tvrtke-za-spremanje-podataka-15056771 , pristupano 1.4.2021 g.

8. https://www.nbcconnecticut.com/news/local/woodbridge-police-seek-gun-wielding-bank-robber/2202504/ , pristupano 1.4.2021 g.

9. https://www.24sata.hr/news/kazna-420000-kn-za-sjecu-sume-bez-potrebne-dozvole-167972 , pristupano 15.3.2021 g.

10. https://www.tedxdharavi.com/list-of-fake-timberland-sites , pristupano 22.3.2021 g.

11. https://www.bug.hr/sigurnost/hakerski-napad-na-ina-u-provjerili-smo-neke-nesluzbene-navode-i-sto-se-trenutno-13938 , pristupano 24.3.2021 g.

12. https://www.cert.hr/PhishCoviD , pristupano 26.3.2021. g.

13. https://www.ey.com/hr_hr/covid-19/covid-19-business-recovery-planning-for-private-businesses , pristupano 1.4.2021

14. https://narodne-novine.nn.hr/clanci/sluzbeni/2021_01_5_111.html , pristupano 26.3.2021

15. https://zdravstvo.gov.hr/UserDocsImages/2020%20CORONAVIRUS/Korona-prostorije_.pdf , pristupano 26.3.2021

16. https://uznr.mrms.hr/obavljanje-poslova-na-izdvojenom-mjestu-rada-i-oslobada-je-od-obveze-dokumentiranja-procjene-rizika/ , pristupano 26.3.2021

POPIS TABLICA I SLIKA

11. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Kristina Brletić

Matični broj studenta: 07-62/19

Naslov rada: SIGURNOST KORPORACIJA U VREMENU PANDEMIJE BOLESTI COVID-19

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristila sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam navela autora i izvor te ih jasno označila znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spremna sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum **Potpis studenta**

_____ _____

12. ŽIVOTOPIS

Kristina Brletić

Ulica Antuna Arbanasa 11a

10020 Zagreb

095-1999-316

brekalo86@gmail.com

Datum rođenja: 25.prosinac 1986.g.

Sažetak i vještine:

- **Iskustvo u području proračunskog računovodstvo**
- **Organizirana, sistematična, spremna za timski rad**
- **Izražene komunikacijske vještine**
- **Samostalnost u radu**
- **Iskusna u radu s MS Office-om,**
- **Spremnost na nove izazove te na usvajanje novih vještina**
- **Engleski – B2 razina.**

Radno iskustvo:

Favorit d.o.o. 2008. – 2018.

Blagajnik

- **Blagajnički poslovi**
- **Izrada dnevnog obračuna prometa**
- **Narudžba potrošnog materijala**

Ekonomska škola Velika Gorica. 2018. – trenutno zaposlenje.

Voditelj računovodstva

- **Izrada obračuna plaća**
- **Financijska izvješća prema ministarstvu i osnivaču**

- **Financijski planovi**
- **Platni promet**

Obrazovanje

Specijalistički diplomski stručni studij – Menadžment javnog sektora

Veleučilište Baltazar u Zagreb **2019. – 2021.**

Preddiplomski stručni studij: Računovodstvo i financije

Sveučilište u Splitu, Sveučilišni odjel za stručne studije **2012 – 2015.**

Srednja škola Matije Antuna Reljkovića, I. Cankara 76, Slavonski Brod **2001. – 2005.**

Vozačka dozvola B kategorije