Стручни рад
УДК 004.056:351.862
DOI 10.7251/BPG2202067D

Рад запримљен: 13.10.2022. године
Рад прихваћен: 28.10. 2022. године

КРИЗНИ МЕНАЏМЕНТ У СИТУАЦИЈАМА УГРОЖАВАЊА САЈБЕР БЕЗБЈЕДНОСТИ

Мср[1] Душан Дакић

Апстракт: Према Тепавцу (2019), поуздане и провјерене информације представљају основ смисленог људског дјеловања, успостављања међуљудских, међународних и пословних односа. Информације нарочито добијају на значају са напретком информационо-комуникационих технологија и настајањем глобалних пословних мрежа, односно умрежавањем институција и присутношћу неког од видова информационо-комуникационих технологија у животу највећег дијела људске популације. Посебно мјесто и улогу у свијету информација имају пословне информације јер од њих зависи ефикасност функционисања информационо-комуникационог система (ИКС) националних држава али и привредних субјеката. Појава великог броја пословних информација намеће разна питања од којих су најзначајнија сљедећа: како из великог броја информација извући оне потребне и корисне, како расположиве информације употријебити тако да се постигне најбољи пословни резултат, како онемогућити злоупотребу информација и ИКС-а и како заштити информације и обезбиједити сигуран и несметан рад ИКС-а. Заштита пословних информација је активност која се реализује у циљу обезбјеђивања несметаног и континуираног рада ИКС-а, смањујући ризике и пријетње на минимум. Заштита пословних информација представља заједнички задатак пословних субјеката и државних институција. Квалитетна заштита пословних информација, између осталог, подразумјева стандардизацију информационе безбједности, а савремени стандарди који се данас употребљавају односе се на генерисање, пријем и чување података унутар ИКС-а.

Кључне ријечи: сајбер безбједност, интернет, ризик, криза, кризни менаџмент, сајбер простор, сајбер криминал.

1 *Министарство унутрашњих послова, имејл: dusan_dakic@hotmail.com*

УВОД

Савремено пословно окружење у којем организација остварује своје циљеве одликује се великим бројем интеракција међу учесницима. Восіј, Greasley и Hickie (2015, стр. 17) наводе да се главни фактори окружења који утичу на организацију могу груписати у три међусобно повезане цјелине: специфично окружење кога чине односи са запосленим, тренутним и будућим, односи са купцима и добављачима, као и конкуренција, опште окружење које чине економски фактори, технологија, правни оквир и јавно мнење и физичко окружење које чине локација и вријеме. Информациони системи, као модели стварних система имају за циљ да са таквим окружењем омогуће организацији да одржи везе путем размјене података, информација и знања, уз несметано обављање дневних операција, као и да омогуће довољно добру основу за доношење стратешких одлука. Окружење у којем организација остварује наведене интеракције је небезбједно, а при томе се јављају могућности интерних пријетњи, што доводи до тога да се проблем безбједности једне организације пројектује и на њен модел, тј. информациони систем. Због тога је потребно спровести одговарајући приступ по питању безбједности информационог система организације и тиме створити могућност за остварење њене мисије, визије и циљева. Такође, потребно је истаћи да тај процес није једнократан, већ се одвија континуирано, из разлога што се информациони системи и елементи окружења организације непрекидно мијењају, а самим тим и динамика, облици угрожавања и нивои пријетњи којима су изложени. Заступљеност ИКТ-а у савременом животу савременог човјека је достигла такав ниво, да је скоро па немогуће замислити да друштво уопште функционише без примјене савремених технологија овог типа. Пракса, односно свакодневна употреба информационих система је показала да савремене ИКТ-е поједностављују приватне и пословне обавезе човјека, омогућавају лакшу и бржу комуникацију и податке чине лакше доступним крајњим корисницима. Међутим приступ таквим подацима је омогућен и неким лицима која немају добре намјере када је у питању употреба осјетљивих и битних информација, односно лицима која настоје да злоупотријебе такве податке и информације. Управо такве информације погодују неким криминалним, екстремистичким и терористичким организацијама у развоју, које још увијек немају развијене начине за обуку лица и довољно сазнања о тим областима. Данас постоји велики број националних и међународних институција било због општости или преуског значења које се баве спречавањем и истрагама ове врсте криминала, који се најчешће назива високотехнолошким криминалом. У данашње вријеме када се свијет развија невиђеном брзином у сваком облику, а на-

рочито у сфери информационих технологија и безбједносних система, неминовно је да услијед тога дође до кризе. Изградња ефикасног система менаџмента ризика и кризног менаџмента је приоритет таквог слиједа догађаја. Сигурност информационих система - сајбер безбједност[2], је основа опстанка и пословања корпорација у данашњем савременом свијету, и због тога треба свакодневно и континуирано радити на унапријеђењу сајбер безбједности.

ПОЈАМ РИЗИКА И КРИЗА

Појам ризик потиче од грчке ријечи која означава постојање опасности на отвореном мору. Ризик представља могућност настајања ситуације која се може негативно одразити на пословање, што може довести до поремећаја у остваривању циљева предузећа. Постоје разне дефиниције ризика, међутим заједнички елементи свих дефиниција су: неодређеност исхода и потенцијални губитак као један од могућих исхода. Ризик представља вјероватноћу да се оно што се планира неће остварити, а изведено из неизвјесности будућих догађаја. Уз појам ризика веже се излагање опасности – у основи је перципиран као негативна појава. Vaughan E. и Vaughan T. (1995), кажу сљедеће: „Ризик је стање у којем постоји могућност негативног одступања од пожељног исхода који очекујемо или којем се надамо. У вези са тим можемо рећи да би ризик постојао у финансијском пословању, мора: бити могућ, изазивати економску штету, неизвјестан и бити случајан.“ Постоје различите дефиције ризика, али су оне често зависне од критеријума, принципа или теоријских упоришта на којима се израда типологије заснива. Није ријетка подјела ризика на оне чији су извори и облици природни догађаји и на оне условљене човјековим дјеловањем. Ризици условљени човјековим дјеловањем се даље дијеле на тзв. интенционалне (настали са намјером) и акцидентне (настали намјерном или случајном непажњом, директним или индиректним утицајем људског или других фактора). Са генералног становишта ризици се најчешће дијеле на природне и технолошке, а сваки од њих у себи садржи бројне подврсте. Међу њима може постојати неких сличности и преклапања, али у сваком случају много је више разлика. Природни ризици се испољавају углавном без људског утицаја, мада у неким случајевима као што је ситу-

2 Данас се за област сајбер безбједности али и уопште свих активности са овим префиксом, користе разни термини. Међутим, термини као што су „информациони“, „информатички“, „рачунарски“ појмовно не одговарају, било због општости или преуског значења, због чега је често у употреби префикс „сајбер“. У питању је облик неологизма, а познато је да се неологизми користе кроз историју и то најчешће у области технологије. Ријеч сајбер данас користимо јер је то један од најзаступљенијих неологизама у свијету, како код нас тако и у енглеском језику, чија се употреба веома брзо шири.

ација „глобалног затопљења“, може се говорити о индиректном утицају човјековог дјеловања. По интензитету, ширини и посљедицама ови ризици често имају карактер природних непогода и катастрофа. Најизраженији ризици ове врсте су поплаве, суше, земљотреси, олује и сл. За разлику од природних, технолошки ризици најчешће се јављају као производ људског дјеловања. Мада већина техничко – технолошких изума, постројења и процеса сама по себи нису ризична, ипак постоје и оне које самим својим постојањем или својим радом неспорно производе посљедице које су штетне, па и потенцијално опасне по људску и природну околину (нуклеарна постројења). У техничко – технолошке ризике спадају они попут пожара насталих на инсталацијама, објектима, постројењима и сл. Наведена подјела ризика на природне и техничко – технолошке обухвата значајан број извора и облика угрожавања који могу задесити људе, друштво, пословне организације, али се врсте и облици њих наведеном класификацијом не исцрпљују (Бошковић, 2017). У данашњем времену, гдје је присутна велика дигитализација и коришћење савремених технологија, све је већа присутност „сајбер“ ризика. Данашња сајбер безбједност много је више од једноставног технолошког ризика којим се бави ИТ одјељење. Нарушавање сајбер безбједности може умањити способност пословног дјеловања и узроковати милионске штете. Појам криза потиче од грчке ријечи krisis, што значи одлучна тачка и представља избор, преокрет, опасност и одлучивање, прекретницу у развоју или реализацији одређеног процеса. Ријеч криза данас је вјероватно једна од најчешће кориштених ријечи у свакодневном животу и говору. Користи се у описивању личне, односно приватне ситуације, али много чешће за опис стања са потенцијалним негативним консеквенцама у којима се налазе друштво као цјелина или поједине организације и системи у оквиру њега. Али и поред учестале примјене нема јасног и и једнозначног појмовног садржаја термина кризе, већ постоје многобројне и међусобно често различите интерпретације. Иако се под кризом подразумјева најчешће нестабилна ситуација у друштву, у политичким или економским односима, размотрићемо неколико схватања појма кризе. Према Политичкој енциклопедији (1975, стр. 494-495), нема одређења појма кризе, већ политичке кризе која се дефинише као „период који наступа између преласка једне владе и успостављања друге. (...) у свом пунијем социолошко-политичком појму политичка криза наступа кад се поставља проблем постојеће политичке власти или њене битне промјене. (...) многи фактори и низ објективних и субјективних околности, укључујући ту и историјско вријеме, међународне односе и способност нових и револуционарних снага, утичу на одговарајуће рјешење једне праве политичке кризе, кризе система и власти. Отуда су за политичку праксу и акцију од великог значаја научна и објек-

тивна анализа кризе и постојања способних друштвених и политичких група да кризу претворе у њену негацију и афирмацију." Као што видимо кризе представљају константу друштвене историје. Милашиновић (2009), наводи да су се са напретком људског сазнања повећале и способности за управљање кризама. Међутим, истовремено у савременом глобалном, повезаном, међузависном високотехнолошком окружењу у коме су сви процеси убрзани, мијења се природа кризе и оне добијају сасвим нове карактеристике. Било да се називају модерним или фундаменталним, ове кризе стављају кризне менаџере на озбиљан испит, показујући ограничене домете традиционалног промишљања, кризе и немоћ, па и контрапродуктивност класичних алата кризног менаџмента. Нужно се намеће потреба креативног мултидисциплинарног приступа и тражења нових одговора на ову врсту криза.

Како наводи Кешетовић (2008), свакодневно управљање активностима неке организације, односно пословање предузећа, разликује се од управљања пословањем у условима кризе. Према Ђукићу (2018), да би менаџери што боље управљали својим организацијама и предузећима, чак и у условима кризе, морају познавати главне карактеристике кризе. Њих све није могуће навести, будући да се кризе међусобно разликују по садржају, трајању, посљедицама и осталим карактеристикама. У литератури се најчешће као три карактеристике заједничке за све кризе наводе: пријетња, хитност (временски притисак) и несигурност. Уз ове карактеристике често се додаје као четврта основна карактеристика недовољност, односно неадекватност ресурса неопходних за одговор на кризу.

ПОЈАМ КРИЗНОГ МЕНАЏМЕНТА

Појам кризе, као одступања од нормалног поретка ствари, настао је релативно касно, односно тек када су људи схватили да у природи и друштву постоји ред и законитост тј. космос, а не хаос. Ђукић (2017), наводи да је криза као одступање од нормалности, односно нарушавање уобичајеног функционисања, дуго схватана као производ више силе или резултат божје воље, па су се људске активности у случајевима криза сводиле на магијске ритуале, религијске обреде. Са продором рационалног погледа на свијет и развојем науке јавила су се и прва настојања људи да опишу, класификују, разумију и објасне кризе и направе што адекватније начине за управљање кризама. Ипак, кризни менаџмент, као научно – теоријска дисциплина и рационално осмишљена пракса, озбиљно ступа на историјску сцену тек у другој половини XX вијека. Поријекло термина кризни менаџмент налази се у политичкој сфери. Наиме, тврди се

да је амерички предсједник Џ. Ф. Кенеди први употријебио овај израз током Кубанске кризе 1962. године, када је конфротација САД и СССР-а услијед инсталирања совјетских ракета са нуклеарним главама на Куби, довела свијет на ивицу Трећег свјетског рата. На тај начин Кенеди је описао управљање једном озбиљном, ванредном ситуацијом. Кризни менаџмент као функција, односно дјелатности кризног менаџмента, старији су од самог термина. Тако је управљање ванредним догађајима као формална одговорност владе САД настала са напорима да се одговори на растуће пријетње пожара у великим градовима у XIX вијеку. Касније, кризни менаџмент настаје и као организација, односно формирају се посебни органи, тијела и агенције које се баве управљањем кризама. Кризни менаџмент је врста апликативног (примјењеног) менаџмента, као уосталом менаџмент уопште, и не представља неку егзактну науку већ прије праксу у руковођењу теоријом. Кризни менаџмент може се одредити као скуп функција или процеса који имају за циљ да идентификују, изуче и предвиде могуће кризне ситуације и успоставе посебне начине који ће омогућити организацији да спријечи кризу или да се са њом избори и да је превазиђе уз минимизирање њених посљедица и што бржи повратак у нормално стање.

ИНТЕРНЕТ И САЈБЕР ПРОСТОР

У данашњем, назовимо, модерном времену, број корисника интернета расте великом брзином. Интернет користе сви, без обзира на старосну доб, ниво образовања, врсту посла којом се баве и сл., само је различита сврха кориштења. Неки га користе за забаву, други за обављање задатака из својих професија, стицање нових сазнања, комуникацију, док се са друге стране интернет може користити и за разне илегалне радње. У сваком случају можемо рећи да се интернет скоро преко ноћи увукао у све сфере нашег живота. Интернет је свјетска односно глобална рачунарска мрежа која повезује многе рачунаре и друге рачунарске мреже (академске, пословне, владине) у једну цјелину са намјером размјене података и кориштења разних садржаја, услуга и сервиса као што су www, електронска пошта и сл., док је сајбер простор – сајберспејс (енгл. cyberspace) у ствари замишљени простор у коме се одвија комуникација путем компјутера, нарочито преко интернета, виртуелни простор. Интернет нико не посједује, а називају га мрежом свих мрежа односно скупом глобалних мрежа, великих и малих. Те мреже с повезују заједно на много различитих начина тако да чине једну цјелину коју знамо под називом Интернет. „Интернет је дакле глобална рачунарска мрежа која се заснива на пакетном преносу података и клијент-сервер архитектури која повезује кориснике из ције-

лог свијета. Интернет повезује не само поједине рачунаре већ и читаве мреже. Осим компјутера на интернет се повезују мобилни телефони, видео камере, паметни телевизори итд. Као мрежа за пренос података, представља основу на коју се надограђују различити протоколи, па тако интернет данас омогућава комуникацију, размјену фајлова, видео и аудио репродукцију, забаву, апликације". (WEBnSTUDY.com., Појам и настанак интернета).

ПОЈАМ САЈБЕР ПРОСТОРА И САЈБЕР КРИМИНАЛА

Како наводе Ристић и Маринковић (2018), сајбер простор – сајберспејс (енгл. cyberspace) је у ствари замишљени простор у коме се одвија комуникација путем компјутера, нарочито преко интернета, виртуелни простор. Развој информационих технологија и компјутерски посредоване комуникације је допринио настанку сајбер простора, што је за посљедицу имало настанак и развој нових начина успостављања и одржавања друштвених односа. Сајбер простор одређујемо као простор у којем се границе успостављају и одржавају на флексибилнији начин у односу на физички простор, односно као просторно-временску цјелину догађаја који настају као посљедица успостављања односа људи и компјутера, људи посредством компјутера и компјутера са компјутерима. Идентификујући разлике, као и заједничке карактеристике физичког и сајбер простора, можемо закључити да сајбер простор представља низ истовремености који посредује у односима човјека са објектима, човјека са околином и људи међусобно. Такође, закључујемо да је сајбер простор комуникацијски поредак и простор могућности који представља диспозитив у најмање двоструком смислу – као репрезент и као медијум друштвених интеракција. Иако сајбер простор јесте електронски простор, дигитални простор и медијски простор, оно што су његове кључне карактеристике које га истовремено чине друштвеним простором су интерактивност и релационалност. То значи да се у и захваљујући сајбер простору, друштвени односи и интеракције стварају и одржавају. Осјећај за сајбер простор је генерисан захваљујући повратној информацији (енгл. feedback). У том простору се остварује интеракција на бар три нивоа: људи и објеката, људи и средине, људи међусобно. С обзиром на чињеницу да сајбер простор садржи такве могућности, он је потенцијални простор другог нивоа (енгл. second order) који се – за разлику од поретка у физичком свијету – успоставља посредством рачунарских технологија. Један од најизраженијих и најчешћих злонамјерних активности јесте коришћење интернета за спровођење криминалних радњи као што су трговина људима, продаја нарко-

тика, вршење разних врста превара, крађа идентитета и сл. Овај облик криминала се у литератури назива високотеехнолошки или сајбер (енгл. cyber) криминал. Карактеристична дјела која могу да се доведу у контекст рада су: дјела против повјерљивости, интегритета и доступности компјутерских података и система (незаконит приступ, пресретање, уплитање у податке или системе, коришћење уређаја, програма, лозинки), дјела везана за компјутере код којих су фалсификовање и крађе најтипичнији облици напада, дјела везана за кршење ауторских и сродних права обухватају репродуковање и дистрибуцију неауторизованих примјерака дјела компјутерским системима.

Класификација сајбер криминала према Дракулић, М., и Дракулић, Р. (2014), указује на сљедеће категорије: политички: сајбер шпијунажа, хакинг (недопуштено, незаконито проваљивање и улажење у компјутерске системе) , сајбер саботажа, сајбер тероризам, сајбер ратовање, економски: сајбер преваре, хакинг, крађа интернет услуга и времена, пиратство софтвера, микрочипова и база података, сајбер индустријска шпијунажа, преварне интернет акције (неиспоручивање производа, лажна презентација производа, удруживање ради постизања веће цијене, трговина робом са црног тржишта, вишеструке личности), производња и дистрибуција недозвољених и штетних садржаја: дјечја порнографија, педофилија, ширење ставова вјерских секти, ширење расистичких, нацистичких и сличних идеја и ставова, злоупотреба жена, манипулација (трговина, дистрибуција и сл.) забрањеним производима, супстанцама и робама: дрогом, људима и дјецом, људским органима и оружјем, повреда сајбер приватности: надгледање е-поште, спем (енгл. spam – нежељене промотивне е-поруке, које се аутоматски шаљу хиљадама људи, а оглашавају или промовишу различите производе и услуге. Циљ неких нежељених порука је преварити вас или оштетити ваш компјутер), фишинг (енгл. phishing – „пецање података“ путем е-поште. Фишинг је процес путем којег преваранти добивају приступ осјетљивим подацима, као што су корисничка имена, лозинке или подаци са кредитних картица, слањем електронских или текстуалних порука, које изгледају као да су их послале легитимне организације), крађа идентитета, прислушкивање, снимање соба за чет (енгл. chat rooms – помоћу чета је могућа комуникација са људима који се налазе у истој чет соби, с тим што је много чешћа комуникација дописивањем тј. куцањем преко тастатуре, него директна комуникација говором, помоћу микрофона и слушалица), праћење е-конференција, приказивање и анализа колачића (енгл. cookies – метод који у софтверу служи за прикупљање информација о лицима која посјећују неку веб локацију, да посјетилац не би морао да се региструје сваки пут приликом посјете).

ПОЈАМ БЕЗБЈЕДНОСТИ ИНФОРМАЦИОНИХ СИСТЕМА

Појам безбједности информационих система, није једноставно једнозначно дефинисати, првенствено због многих вишеструких односа између безбједности и њему сличних појмова, као и све већој сложености промјењивог окружења у којем један информациони систем организације дјелује. Готово да нема ријечи као што је безбједност, која се више користи у савременом животу, а да је појам који се њоме означава истовремено мање одређен и јасан. Овај термин подједнако употребљавају теоретичари безбједносних наука у најширем смислу, али и политичари, представници државних власти, међународних организација и невладиног сектора, индустријалци, медицинари, еколози, правници, економисти итд. У контексту сигурности рачунарских мрежа аутори указују да је безбједност апстрактан модел, док је сигурност актуелна имплементација. При томе, сигуран систем кореспондира моделу који је безбједан у односу на сва права, али модел безбједан у односу у односу на сва права не гарантује сигуран систем. Према Bourgeois (2014), фундаментални концепти безбједности информационих система су везани за информациону безбједност (енгл. information security), која је описана преко три карактеристике: повјерљивост (енгл. confidentiality), интегритет (енгл. integrity) и расположивост (енгл. availability) које се називају „троугао“ или „тројство“ или „тријада“ сигурности. Приликом заштите информације, желимо да ограничимо приступ онима којима је дозвољено да информацију виде, а свима осталима да онемогућимо њен садржај и то је суштина повјерљивости. Интегритет осигурава да информација стварно представља њено намјеравано значење и да није измјењена, случајно или намјерно. Расположивост означава да се информацији може приступити и да се она може измијенити од стране било кога који је ауторизован да то уради у одговарајућем временском оквиру. У циљу да јасно дефинише појам сајбер безбједности, Von Solms и Van Niekerk (2013), указују на разлике које постоје у појмовима информационе безбједности (енгл. information security), безбједности информационих и комуникационих технологија (енгл. information and communication tehnology security), скраћено ICT безбједност и сајбер безбједност и сајбер безбједности (енгл. syber security).

У савременим условима пословања организације остварују своје мисије, визије и циљеве употребом информационих система. Они им омогућавају размјену података, информација и знања са промјењивим окружењем, несметано обављање других активности, као и стварање основе за доношење стратешких одлука. Нови модалитети угрожавања безбједности информационих система појављују се услијед промјењивог небезбједног окружења и пријетњи које вребају из сајбер простора, због чега је

потребно обратити пажњу на исте и адекватно дјеловати, реаговати, јер није више у питању само рањивост информатичко-комуникационе инфраструктуре и информација, већ и људског живота. У самој безбједности информационих система, поред техничких мјера заштите потребно је обратити пажњу и на људски фактор и свијест о безбједности, као најслабију карику и дјеловати како би се пријетње свеле на најмању могућу мјеру. У остварењу повјерљивости, интегритета и расположивости, спроводе се технике или мјере заштите, које су неопходне да би умањиле рањивост система или да га сведу на прихватљиву мјеру са једне стране, а са друге је потребно да буду осмишљене на начин да не утичу негативно на продуктивност. Поред тога потребно је имати у виду да је комуникација унутар рачунарских мрежа сложен проблем, и да би се ефикасно ријешио потребно је примјенити принцип апстракције. Контролисано увођење сложености довело је до тога да имамо вишеслојне референтне моделе мрежне комуникације који се данас користе, при чему су најпознатији ISO/OSI модел и TCP/IP модел. Поменути модели имају архитектуру организовану у слојевима, гдје се сваки слој може посматрати као услуга која се нуди слоју изнад себе. „На сваком слоју постоје комуникациони протоколи путем којих се дефинише формат и редослијед порука, размјењених између најмање двије стране које учествују у комуникацији, као и поступци који се предузимају послије слања и/или примања порука или неког другог догађаја“ (Kurose и Ross, 2009). Начин на који функционишу комуникациони протоколи и рачунарске мреже, па тиме и интернет, даје могућност злонамјерним актерима да наруше повјеривост, интегритет и расположивост, употребом општепознатих механизама самих рачунарских мрежа. Из наведеног можемо закључити да технологија колико са једен стране даје могућности, толико са друге доноси пријетње и ризике које је потребно сагледати и адекватно управљати са њима.

Нападачи користе различите методе и алате, често и у комбинацији, да би компромитовали повјерљивост. Један од алата који је широко у употреби је софтвер за хватање и анализу мрежних пакета (енгл. packet sniffer) путем којег се комуникација пресијеца и снима, а након тога се врши анализа садржаја пакета. Уколико постоји неки осјетљив садржај, лозинка или број картице приказан у облику чистог текста он се може прочитати. Суштина напада на шифру (енгл. password attacks) јесте да се добије приступ систему, путем налога. Напад путем ријечника (енгл. dictionary attack) је врста напада гдје нападач покушава да погоди шифру употребом ријечи из ријечника или често кориштених и познатих шифри. Поред тога, нападач може да покуша да погоди шифру спроводећи сваку могућу комбинацију, што је познато као напад сировом снагом (енгл. brute-force attack). Скенирање портова (енгл. port scanning) је техника која се кори-

сти да би се утврдило који су портови отворени на рачунару, при чему се за популарне протоколе обично зна које портове користе. Уобичајено се користи да се сазна нешто о конфигурацији система, да се утврде потенцијалне слабе тачке и да ли постоје неки сигурносни механизми који контролишу мрежни саобраћај, као нпр. мрежне баријере (енгл. firewalls). Phishing напад је форма напада гдје се најчешће путем електронске поште, прослеђује имејл кориснику, који својим изгледом и садржајем веома подсјећа на имејл њему важног пошиљаоца, нпр. банке, који наводи примаоца на одавање повјерљивих информација као што је број картице или лозинке. Phishing је једна од форми социјалног инжењеринга (енгл. social engineering) као вида психолошке манипулације која се користи да обмане корисника у циљу одавања повјерљивих информација.

Неке од мјера које се примјењују у обезбјеђивању повјерљивости су прије свега, адекватно управљање корисничким налозима и лозинкама. Поред тога, један од битних процеса је аутентификација (енгл. authentication) у коме корисник доказује да је оно за шта се представља. Када корисник покушава да приступи систему, спроводи се утврђивање његовог идентитета. Поред тога, спроводи се и процес ауторизације (енгл. authorization) којом се одређује да ли корисник има право да приступи одређеном ресурсу. Ауторизација се спроводи након процеса аутентификације и одређује чему корисник може или не може да приступи. Провјера аутентичности може имати различите облике. Корисници пружају акредитив који представља нешто што знају – лозинка или лични идентификациони број, нешто што имају – физички предмет („смарт картица", токен) и нешто што јесу – биометријске карактеристике корисника. Да би се повећао степен заштите провјере аутентичности, користи се комбиновање два или више метода за провјеру аутентичности ради отежавања нежељеног упада на систем. Најчешћа комбинација метода је кориштење провјере корисничког имена и лозинке са неким биометријским или физичким методом, односно токеном, паметном картицом или скенером. Ранђеловић (2014) наводи да је Керберос један од најпознатијих мрежних протокола за провјеру идентитета корисника. Име је добио по митском бићу Кербер, зато што центар за дистрибуцију кључева, попут митског бића из грчке митологије има три „главе" прву представља база, другу сервер за провјеру идентитета, а трећу сервер за издавање карата. Керберос је такозвано пријављивање типа „пријави се само једном" (енгл. single sign on), које корисницима омогућава да се само једном пријаве на систем и да након тога, у складу са својим овлаштењима, имају приступ свим ресурсима у систему или мрежи. Након што клијент и послужитељ користе Керберос за доказивање свог идентитета, они такође могу шифровати све своје комуникације како би се осигурала приватност и интегритет пода-

така током њиховог пословања. Према Шнајеру (2007), Један од важних концепата који се примјењује јесте и техника шифровања (енгл. encryption). Отворени текст (енгл. plain text) путем шифровања постаје текст са прикривеним садржајем, тзв. шифрат (енгл. ciphertext). Дешифровање (енгл. decryption) је обрнути процес од шифровања, гдје се од шифрата добија изворни отворен текст. Сви поменути концепти су дио криптографије (енгл. cryptography) – науке и умјетности чувања безбједности података. Криптографски алгоритам (енгл. cryptographic algorithm) је математичка функција која се користи за шифровање и дешифровање. Технологија дигиталног потписа користи технологију асиметричног криптовања. Пошиљаоц и прималац имају пар кључева, од којих је један тајни кључ (енгл. private key), а други свима доступан јавни кључ (енгл. public key). Кључеви представљају математичке алгоритме које је издало сертификационо тијело. Сврха дигиталног потписа је да потврди аутентичност садржаја поруке или интегритет података (доказ да порука није промјењена на путу од пошиљаоца до примаоца), као и да гарантује идентитет пошиљаоца поруке. Дигитални потписи се користе за идентификацију извора информације који може бити нека особа, организација или рачунар. Идеја дигиталног потписа је слична класичном потписивању докумената. Уколико се неки документ жели послати електронским путем, такође се мора потписати. За разлику од класчног потписа, дигитални потпис је готово немогуће фалсификовати. Успјешном провјером дигиталног потписа гарантује се: аутентичност, интегритет и непорицљивост. Примјер кршења интегритета је Салама напад (енгл. salami attack) који представља форму напада које се понавља више пута, а најчешће је везан за добављање финансијеске користи, гдје се малициозни програм користи да украде веома мали дио износа, који се не примјећује једноставно. Када се програм изврши много пута, та сума нарасте. Овај напад је тежак за детекцију и уопште његова детекција у великој мјери зависи од свијести запослених. Такође и напад са посредником (енгл. man-in-the-middle-attack), представља специфичну врсту напада гдје се нападач налази између двије стране које комуницирају и прислушкује комуникацију пресретањем порука и при томе мијења садржај тих порука, при чему учесници комуникације нису свјесни посредника. Ова врста напада може имати неколико форми, а један од њих је преузимање сесије (енгл. session hijacking attack), тровање ARP кеша (енгл. ARP cache poisoning) или DNS Spoofing, који отварају простор за спровођење других напада. Интегритет је везан за очување конзистентности, тачности и поузданости података током цјелокупног циклуса. Подаци не могу да буду промијењени у преносу и подаци не смију да буду измјењени од стране неауторизованих људи. Доста техника које се користе и за очување повјерљивости, користе се и за очување интегри-

тета. Један од напада који се користи за компромитацију расположивости јесте одбијање услуге (енгл. denial of service attack). То је тип напада у коме се услијед великог броја захтјева ка неком серверу или сервису догоди да он постане недоступан јер не може да процесира поменуте захтјеве. Специјалан врста тог напада је дистрибуирано одбијање услуге (енгл. distributed denial of service attack) које долази из више различитих извора и блокирањем једног извора напад се не може зауставити. Један од приступа јесте да нападач програмира мрежу рачунара, познатију као botnet, који преплаве сервер захтјевима и доведу га у стање да он падне и постане недоступан. Према Stallings и Brown (2018), мјере које је потребно спроводити у циљу расположивости, јесу да су подаци доступни унутар свих система и да сервер може да поднесе одговарајуће мрежно оптерећење. Самим тим је потребно и хардвер држати ажурним, надгледати употребу мрежног опсега и обезбједити могућности опоравка и опоравка од катастрофе (енгл. disaster recovery) уколико до тога дође. Описане технике заштите су дио шире стратегије безбједности. Први корак те стратегије јесте дефинисати политику безбједности. Са једне стране она може бити један неформалан документ који описује жељено понашање система, док са друге то може бити документ који садржи правила и праксе, које организација примјењује да би обезбједила безбједносне сервисе. Обично се наводи: вриједност средстава која се штите, рањивости система и потенцијалне пријетње и вјероватноћа напада. Затим слиједи процес имплементације који садржи сљедеће комплементарне активности: превенција, детекција, одговор и опоравак. Након тога слиједе радње у вези осигуравања и процјене. Бјелајац и Весић (2020), наводе да је осигуравање атрибут информационог система који је основ повјерења у то да систем ради у складу са примјењеним политикама. Еваулација је процес утврђивања да ли је систем испунио одговарајуће прописане критеријуме. у организацијама је уобичајено да су формирани тимови који се баве проблемом безбједности, који спроводе цјелокупну стратегију безбједности. Неке организације се одлучују да послове информационе безбједности обављају тимови унутар саме организације док неке ангажују екстерне субјекте специјализоване за такве врсте послова, да ли као помоћ постојећим безбједносним сервисима или које ће за њих те послове обављати у потпуности. Субјекти, односно ораганизације које се баве таквим услугама обављају послове сталног мониторинага, управљње системима за детекцију упада (енгл. intrusion detection systems), управљање заштитним баријерама (енгл. firewalls), надгледање надоградње софтвера на нове верзије, као и оддговарајуће безбједносне процјене, ревизије и одговоре на хитне случајеве, као и разне консултантске услуге. Уобичајено нуде своје услуге употребом платформе рачунарства у облаку (енгл. cloud computing) по моделу

софтвера као услуге (енгл. software-as-a-service). Поред тога што поменути начин повећава безбједност сервиса организације, он се може показати и као финансијски исплатив.

САЈБЕР БЕЗБЈЕДНОСТ У КОРПОРАЦИЈАМА

Сајбер инциденти могу нанијети штету од системског значаја и зато изградња доброг система сајбер безбједности превазилази оквире појединачних пословних организација, односно корпорација. Чињеница је да у данашње вријеме живимо у дигиталном - сајбер свијету и да нам је тај дигитални свијет пружио могућност лакшег пословања и веће продуктивности, али са друге стране је омогућио и отворио нове видове и начине остварења криминалних активности путем којих је могуће угрозити пословне процесе, злоупотријебити пословне информације и сл. У таквом дигиталном – сајбер простору криминалне активности немају временске, просторне, географске нити било какве друге границе. Дигитална трансформација обухвата низ малих и великих технолошких помака које не само да помјерају понуду ка онлајн и дигиталним услугама корпорација, већ укључују и примјену савремене технологије у свим сферама рада. Са једне стране, дигитализација чини интерне процесе ефикаснијим, а са друге стране мијења начин комуникације са корисницима корпорацијских услуга. Поред тога нагли развој ИКТ-а довео је до нових видова комуникације и размјене података који се суштински разликују у односу на до тада разрађен традиционални систем. У циљу регулисања међусобних права и обавеза долази до усклађивања докумената, процедура, правила између учесника комуникационог процеса што захтијева професионалан кадар, квалитетну организацију пословних процеса и примјену савремених технологија. Сајбер безбједност у савременом свијету и савременим системима пословања врло брзо постаје незаобилазна компонента у скоро свим предузећима и корпорацијама, управо због чињенице да се паралелно са развојем ИКТ-а развијају и злонамјерне активности лица и организација које настоје да угрозе одређене корпорације. У циљу супростављања таквим намјерама, пословни субјекти примјењују све расположиве мјере заштите информација које се спроводе у циљу превентивног дјеловања и спрјечавања случајног или намјерног негативног утицаја на рад ИКС-а и злоупотребе информација. Дефинисањем облика угрожавања пословних информација које се налазе у оквиру ИКС-а и формулисањем конкретних мјера које ће се предузимати у циљу спрјечавања неовлаштених лица да дођу до заштићених информација, наведена активност се конкретизује и унапријеђује. Информациони систем игра веома

важну улогу у пословању сваке корпорације. Његово правилно функционисање представља срж управљања информацијама и омогућава ефикасно функционисање организације као и њену конкурентност на тржишту. Неадекватна подршка информационих система, стратегијским циљевима, пословним операцијама и потребама менаџмента организације може озбиљно угрозити њен опстанак и успјех. Компаније квалитетним информацијама и њиховом употребом у бржем и бољем доношењу стратешких одлука могу стећи значајну предност у односу на конкуренцију. Коначно, информациони системи који су засновани на ИКТ технологијама омогућавају корпорацијама да се изборе са нестабилношћу пословног окружења. Неопходност увођења информационих система заснованих на ИКТ технологијама је поред одређених предности унио и недостатке, који се манифестују у виду ризика на пољу безбједности информација. Ови ризици могу настати услијед неког од сљедећих фактора: техничких проблема (отказивање неког дијела система), људске грешке, системских пропуста, превара, односно хакерских напада и спољних фактора.

Свијест о растућем потенцијалу напада са нежељеним посљедицама утицао је на све веће инвестиције и улагања на пољу безбједности информација у корпорацијама. Преваре и хакерски напади на информациони систем корпорације, могу страховито утицати на имовинске губитке корпорације. Поред корпорацијске имовине, жртве могу бити и крајњи корисници, односно пословни сарадници, купци и др.

УПРАВЉАЊЕ КРИЗАМА У СИТУАЦИЈАМА УГРОЖАВАЊА САЈБЕР БЕЗБЈЕДНОСТИ КОРПОРАЦИЈА

Менаџмент корпоративне безбједности у корпорацијама, све више је посвећен безбједносним појавама и догађајима, односно безбједности као услову развоја и просперитета. Међутим нису исти безбједносни изазови, ризици и пријетње у свим корпорацијама. Различити безбједносни изазови, ризици и пријетње којима је изложена корпорација/компанија или нека друга организација или предузеће, у великој мјери утиче на менаџмент корпоративне безбједности и њихове одлуке. Корпорације и привредни субјекти данас посвећују све већи значај менаџменту корпоративне безбједности, односно кризном менаџменту, а посебна пажња је усмјерена на управљање кризама и ванредним ситуацијама, а нарочито се посвећује велика пажња кризном менаџменту везаном за сајбер безбједност корпорација. Као што наводе Милашиновић, Кешетовић и Надић (2009), нагли и све бржи развој информационо комуникационе тех-

нологије, сателитских комуникација и интернета утицао је на драматичну измјену наше перцепције временских и просторних ограничења. Овај технолошки развој утиче и на узроке и на карактеристике кризе. Технологија је постала тако сложена да корисници често не разумију како ради, што отежава откривање и исправљање грешака у функционисању. Све већа зависност од рачунарских система чини социјалне и економске системе све рањивијим. А они су угрожени пријетњама хакера и сајбертерориста. Сајбер простор је постао основни простор за рад свих приватних компанија, али и државних институција, а што се нарочито могло видјети у ситуацији проглашења пандемије вируса COVID-19, гдје је коришћење интернета достигло неслућене границе и тада се у суштини схватило да је функционисање пословних и других система у данашње вријеме неоствариво и немогуће без интернета. Међутим, упоредо са развојем начина и могућности пословања путем интернета у сајбер простору, развијају се изазови, ризици и пријетње који пријете корпорацијама и компанијама које обављају послове у таквим условима. Управо због развоја изазова, ризика и пријетњи и начина њиховог остваривања често се дешава да и поред примјењених мјера безбједности везаних за сајбер простор, ипак може доћи до нарушавања сајбер безбједности, а посљедице које се јављају можемо подијелити у неколико група: Финансијске посљедице, које се јављају услијед крађе корпоративних информација, крађе финансијских информација (банковни подаци, информације о платним картицама), крађе новца, губитак посла или уговора, губитак кредибилитета, повјерење представља суштину односа са клијентима, а нарушавање пословних односа, губитак повјерења доводи до губитка клијената и пословних партнера, губитка продаје и на крају смањењем профита, правне посљедице, закон о заштити података о личности захтјева захтјева од корпорација да управљају безбједношћу свих личних података које посједују, било да се ради озапосленима или клијентима. Компромитација личних података за собом повлачи значајне законске казне. У свим наведеним случајевима, осим штете нанесене самој компанији и бизнису уопште, могу бити погођени и клијенти односно корисници компаније. Због свега наведеног потребно је успоставити ефикасан систем кризног менаџмента у пољу сајбер безбједности у корпорацијама, од постављања превентивних мјера које ће могућност настајања кризе свести на минимум, до управљања кризом, њеног ублажавања, правовременог реаговања и санирања штетних посљедица насталих услијед дјеловања кризе. Сајбер криза може погодити све корпорације и компаније, без обзира на њихову величину, облик посла којим се баве и сл., а највише су изложене сајбер кризама оне корпорације и компаније које немају развијене системе сајбер безбједности, односно које не посвећују довољну пажњу ризицима, изазовима и

пријетњама које пријете у сајбер простору. У оквиру безбједносног менаџмента корпорација, морају да буду ангажовани стручњаци из области сајбер безбједности, да ли екстерни или сопствени, а постоји могућност и обостраног ангажовања. Сви они морају дјеловати брзо у случају настанка кризе, како би установили њен узрок, уклонили га и уз што мању штету ријешили насталу кризу. Брза и одлучна реакција донесена на основу препознавања симптома кризе, одлика су доброг кризног менаџмента и воде према брзом рјешавању кризе са што мањим посљедицама. Свака кризна ситуација се након њеног завршетка треба добро анализирати, како би се дошло до закључака и спознаја који ће омогућити боље дјеловање менаџмента и предузећа у будућности, у истим и сличним ситуацијама. Када је ријеч о стратегијском и кризном менаџменту у одбрани критичне информационе структуре и сајбер безбједности, навешћемо да се заштита критичних информационих инфраструктура базира на четири стуба: превенција и рано упозоравање, детекција, реакција и управљање кризама. Управо у том смислу и сајбер простор представља критичну инфраструктуру, док су истовремено концепти заштите критичне инфраструктуре и сајбер простора уско повезани.

Међутим, у значајном смислу кризни менаџмент је постао стандардизован. Промјењива природа саврмених криза, у које спада и угрожавање сајбер безбједности, има директне импликације на кризни менаџмент. Административни репертоар стратегија превенције и интервенције није одговарајући за савремене кризе, које су све сложеније и све више међузависне. Конвеционални организациони модел координације је неприкладан за поступање са профилирајућим мноштвом организација и појединаца укључених у процес кризног менаџмента. Традиционалне стратегије кризног менаџмента - тајност, привилегија извршне власти, затвореност – губе основу у условима у којима освјешћена јавност жели да зна детаље. Другим ријечима нова криза захтијева и нови начин мишљења. Како кризе постају сложеније и транснационалне, потреба за еластичношћу у односу на превенцију такође расте. Међутим, кризе уопште, а нарочито модерне, стварају ситуације које се не могу предвидјети и захтјевају одговоре који нису програмирани.

ЗАКЉУЧАК

Сајбер безбједност представља заштиту дигиталних информација, уређаја и ресурса, која више не може да се посматра одвојено од безбједности у реалном свијету. Штета која настане као резултат сајбер напада је врло стварна те изазива стварне и озбиљне посљедице и у физичком

свијету. Ипак због специфичности везаних за технологију, врсте, починиоце и жртве оваквих напада, питање сајбер безбједности захтјева посебну бригу свих оних који се баве интернетом. Иако су безбједносне апликације и уређаји од велике важности, није довољно да само инсталирате и прикључите те алатке. Сајбер безбједност захтјева да се постави и скуп промишљених процеса и пракси. Због свега наведеног веома је важно превентивно дјеловање у погледу сајбер безбједности. Потребно је да се сигурносни системи за заштиту информационих система поставе тако да служе потребама одговарајућег корисника. Редовно ажурирање система заштите, проучавање и праћење проблематике из области сајбер безбједности, стално усавршавање особља, како би били у кораку са најновијим технологијама и достигнућима у области сајбер безбједности, је један од најбољих начина за смањивање ризика од угрожавања сајбер безбједности. Међутим, информационе технологије се развијају неслућеном брзином, а самим тим и начини угрожавања сајбер безбједности. Потребно је креирати менаџмент који ће управљати ризиком. Планови за управљање ризицима и мјере за поступање у случајевима угрожавања сајбер безбједности треба редовно да се ажурирају, како би у случају избијања кризе организација могла да се са њом избори, као и да је превазиђе уз минимизирање њених посљедица и што бржи повратак у нормално стање. Такође, обавезно је постојање система за прикупљање и анализирање информација о сајбер безбједности. Иако ниједна криза није иста, проучавање других случајева помаже бољем разумјевању природе кризе и ефикаснијем стварању стратегије одговора на кризу.

ЛИТЕРАТУРА

1. Бјелајац, Ђ., Ж., и Весић, Љ., С., (2020)., *Безбедност информационих система: Прегледни рад.,* Нови Сад
2. Bourgeois, D., (2014)., *Information Systems for Business and Beyond, Saylor Foundation*
3. Bocij, P., Greasley, A., Hickie, S. (2015). Business Information Systems, 5th ed, Pearson, p. 17.
4. Бошковић, М., (2017)., *Индусријска безбедност и заштита.,* Београд: Факултет безбедности, стр. 19, 20.
5. Vaughan E, Vaughan T., (1995)., *Основе осигурања, управљање ризицима.*, Загреб
6. Von Solms, R., Van Niekerk, J., (2013)., *From information security to cyber security*
7. Ђукић, С., (2017)., *Управљање системима.* Београд: Војно дјело
8. Ђукић, С., (2018)., *Функционисање корпорација у кризним ситуацијама.* Београд: Факултет за дипломатију и безбедност

9. Дракулић, М., и Дракулић, Р., (2014)., *Cyber криминал. Везе Cyber криминала са ирегуларном миграцијом и трговином људима* XII
10. Кешетовић, Ж., (2008)., *Кризни менаџмент.,* Београд: Факултет безбедности стр. 19
11. Kurose, J., и Ross, K., (2009)., *Умрежавање рачунара: Од врха ка дну*., Рачунарски факултет.
12. Милашиновић, С., Кешетовић, Ж., и Надић, Д., (2009)., *Моћ и немоћ кризног менаџмента у суочавању са модерним кризама: Прегледни научни чланак.,* Београд
13. Ранђеловић. Д., (2014)., *Управљање информационим системима и њихова заштита.,* Београд., Криминалистичко-полицијска академија
14. Ристић, Д., и Маринковић, Д., (2018)., *Кибер-простор као диспозитив друштвености.,* Нови Сад: Годишњак Филозофског факултета у Новом Саду, Књига XLIII-1.
15. Stallings, W., и Brown, L., (2018)., *Computer Security: Principles and Practice*
16. Тепавац, Н. Д., (2019)., *Облици и субјекти угрожавања пословних информација у сајбер простору*, Министарство одбране Републике Србије
17. Шнајер, Б., (2007)., *Примјењена криптографија, превод другог издања*., Београд., Микро књига
18. *Политичка енциклопедија*. (1975). Београд: Савремена администрација, стр. 494-495
19. WEBnSTUDY.com., Појам и настанак интернета., (16. децембар 2015.), преузето 03.07.2022. са http://www.webnstudy.com/tema.php?id=internet,

CRISIS MANAGEMENT IN CYBER SECURITY THREAT SITUATIONS

Msr[3] Dušan Dakić

Abstract: According Tepavac (2019), reliable and verified information is the basis of meaningful human activity, the establishment of interpersonal, international and business relations. Information especially gains importance with the progress of information and communication technologies and the emergence of global business networks, that is, the networking of institutions and the presence of some form of information and communication technologies in the life of the largest part of the human population. Business information has a special place and role in the world of information, because the efficiency of the functioning of the information and communication system (ICS) of national states and economic entities depends on it. The emergence of a large amount of business information imposes various questions, the most important of which are the following: how to extract the necessary and useful information from a large amount of information, how to use the available information in order to achieve the best business result, how to prevent the misuse of information and ICS and how to protect information and ensure safe and smooth operation of ICS. Protection of business information is an activity that is carried out in order to ensure the smooth and continuous operation of ICS, reducing risks and threats to a minimum. Protection of business information is a joint task of business entities and state institutions. High quality protection of business information, among other things, includes the standardization of information security, and the modern standards used today relate to the generation, reception and storage of data within ICS.

Keywords: cyber security, internet, risk, crisis, crisis management, cyber space, cyber crime.

3 *Master manager of corporate security, employed at theMinistry of Interior, Police Administration Doboj, Police Station Derventa, e-mail: dusan_dakic@hotmail.com*