Upravljanje kibernetičkim rizikom - analiza slučaja

Švarbić, Leon

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Leon Švarbić

Upravljanje kibernetičkim rizikom – analiza slučaja

ZAVRŠNI RAD

Varaždin, 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Leon Švarbić

Matični broj: 0016145611

Studij: Poslovni sustavi

Upravljanje kibernetičkim rizikom – analiza slučaja

ZAVRŠNI RAD

Mentor/Mentorica:

Dr. sc. Ivana Dvorski Lacković

Varaždin, rujan 2023.

Leon Švarbić

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Upravljanje kibernetičkim rizikom jedno je od ključnih strateških područja upravljanja suvremenim poduzećima. Zbog toga ćemo u ovom radu obraditi proces upravljanja kibernetičkim rizicima, metode upravljanja njima te razloge važnosti adekvatnog upravljanja ovom vrstom rizika. Navest ćemo neke od najčešćih kibernetičkih napada koji prave probleme suvremenim poduzećima. Za kraj ćemo analizirati slučaj poduzeća Marriott International koje je bilo tri puta žrtva kibernetičkog napada.

Ključne riječi: kibernetički rizik, analiza slučaja, integrirano upravljanje rizicima (ERM)

Sadržaj

1. Uvod

Kibernetički rizik je zbog raširene upotrebe tehnologije u poduzećima te izloženosti zlonamjernim napadima, jedna od ključnih vrsta rizika kojima su suvremena poduzeća izložena. Kibernetički rizik pripada skupini operativnih rizika te povlači sa sobom mogućnost financijske štete, privremenog prestanka pružanja usluga i negativnog utjecaja na reputaciju uslijed zakazivanja poslovnog informacijskog sustava neke kompanije. Trend digitalizacije poslovanja nosi sa sobom povećani rizik kibernetičke sigurnosti, tj. povećanu vjerojatnost kibernetičkih napada na digitalnu infrastrukturu (Miloš Sprčić i sur., 2019). Također on može dovesti do gubitka imovine i osjetljivih informacija. Razlog koji stoji iza kibernetičkog rizika su kibernetički napadi izvan ili unutar mreže neke organizacije ili poduzeća (Aminian, 2021).

Neadekvatno upravljanje kibernetičkim rizikom može dovesti do povećanog ukupnog rizičnog profila poduzeća. Upravljanje ovom vrstom rizika zahtijeva suvremeni pristup upravljanju rizicima zbog činjenice da su kibernetički rizici povezani s mnogim drugim vrstama strateških i operativnih rizika poduzeća, a kvalitetno upravljanje njime nemoguće je bez holističkog pogleda i strateškog odgovora poduzeća na svim razinama (Miloš Sprčić i Dvorski Lacković, 2022).

U današnjem svijetu događaju se mnoge vrste kibernetičkih napada. U drugom poglavlju govorit ćemo nešto detaljnije o kibernetičkom riziku kao i njegovim upravljanjem. Potom nam slijedi detaljnija analiza kibernetičkih napada poput napada zlonamjernim softverom, društvenim inženjeringom, naprednim dugotrajnim prijetnjama te DDoS. U trećem poglavlju povezat ćemo pojmove upravljanje kibernetičkim rizikom (engl. Cybersecurity risk management - CSRM) sa integriranim pristupom upravljanju rizicima (engl. Enterprise risk management - ERM). Proći ćemo korak po korak kako efikasno provesti CSRM u ERM. Spomenut ćemo vrste kvalitativnih i kvantitativnih metoda koje se koriste specifično za CSRM. Na kraju trećeg poglavlja kratko ćemo analizirati izvještaj o prednostima ulaganja u kibernetičku sigurnost. Za kraju nam slijedi analiza slučaja lanaca hotela Marriott International koji je tri puta u šest godina pretrpio kibernetičke napade. Prilikom analize detaljnije ćemo obraditi svaki napad, kao i propuste koji su ih doveli u takvu situaciju.

2. Upravljanje kibernetičkim rizikom

Cilj sustava upravljanja kibernetičkim rizikom je uspostava otpornog informacijskog sustava kojim je moguće spriječiti sigurnosne napade i ometanja poslovnih procesa (Miloš Sprčić i sur. 2020). Upravljanje kibernetičkim rizikom povezano je s osiguravanjem kontinuiteta poslovanja poduzeća te smanjenjem vjerojatnosti ostvarivanja financijskih gubitaka. Kako bi poduzeća osigurala proaktivno upravljanje kibernetičkim rizicima, preporučljivo je imenovati osobu zaduženu za informacijsku sigurnost – *Chief Information Security Officer* (CICO). (Miloš Sprčić i Dvorski Lacković, 2023.) Kao rezultat toga, tvrtke moraju odabrati gdje će potrošiti svoje ograničene resurse za upravljanje kibernetičkim rizikom. Upravljanje takvih vrsti rizika omogućuje organizacijama donošenje odluka na strukturiran način koji je vođen analizom podataka tog poduzeća. Umjesto pristupa "(engl.) first come first served", organizacija identificira prijetnje koje predstavljaju najveći rizik i na njih usmjerava svoje napore da se riješe. Određivanjem prioriteta prijetnjama na temelju rizika, organizacija osigurava da ne rasipa svoje resurse na manje prijetnje nego da maksimizira učinak ulaganja u sigurnost („CheckPoint“, bez dat.).

Kibernetički rizik se odražava na vjerojatnost i učinak nekog događaja tj. Kibernetičkog napada. Prema Miloš Sprčić i Dvorski Lacković (2023) kibernetički rizik svrstavamo kao podskup operativnih rizika, stoga možemo reći da su to svi rizici u poduzeću koji obuhvaćaju namjerne ili nenamjerne pogreške zaposlenika, kibernetičke ranjivosti, prirodne katastrofe te pogreške u IT sustavima poduzeća ili propusta u proceduri.

U kibernetičke rizike spadaju i kibernetički napadi koji su zlonamjerni pokušaj organizacije ili pojedinca da probije sustave druge organizacije ili pojedinca. Motivi napadača mogu uključivati krađu informacija, financijsku dobit, špijunažu ili sabotažu. (Cassetto, 2023.) Važno je da se u obzir uzme dugotrajni cilj poduzeća te da se konstantno provodi ispitivanje rizika i njihovog potencijalnog utjecaja što omogućuje poduzeću stvaranje strateških ciljeva i smanjenje rizika od kibernetičkih prijetnji. Kada se plan za upravljanje rizikom pravilno implementira, omogućuje se bolje razumijevanje raspona rizika s kojima se suočava. Što poduzeće bolje razumije te rizike, to će bolje moći implementirati proaktivne mjere. („Cybersecurity Exchange“, bez dat.) Bez učinkovitog upravljanja kibernetičkim rizikom, organizacije se mogu izložiti riziku od kibernetičkih napada bez mogućnosti oporavka (Tunggal, 2023).

Kibernetički napadi nisu nasumični. Ako znate gdje tražiti, obično postoje znakovi planiranog napada na poduzeće. Pokazatelji neizbježnog napada uključuju spominjanje organizacije na dark webu, registraciju sličnih naziva domena koje će se koristiti za Phishing

napade i prodaja povjerljivih podataka („Rapid7“, bez dat.). Prema Cremer i sur. (2022.) kibernetički napadi na kritične infrastrukture rangirani su na 5. mjesto u Izvješću o globalnom riziku Svjetskog ekonomskog foruma 2020. godine. Napad zlonamjernim softverom i distribuirano uskraćivanje usluge (DDoS) samo su neki od vrsti kibernetičkih napada.

2.1.1. Napad zlonamjernim softverom (engl. malware)

Malware (engl.) je vrsta softvera koji je dizajniran da nanese štetu računalu ili njegovim korisnicima („McAfee“, bez dat.). Cyber kriminalci stvaraju, koriste i prodaju zlonamjerni softver iz mnogo različitih razloga, no on se najčešće koristi za krađu osobnih, financijskih ili poslovnih podataka („CyberArk“, bez dat.).

Mnogo je različitih načina na koje zlonamjerni softver može zaraziti vaše računalo. Najrasprostranjeniji način je putem zaraženih datoteka koje preuzimate s interneta (npr. Web stranice sa sumnjivim domenama, e-mail linkovi i privitci…). Zlonamjerni kod može biti skriven u svim vrstama datoteka, uključujući videozapise, slike i softver. Kada otvorite te datoteke na računalu, zlonamjerni softver može zaraziti vaš sustav i uzrokovati štetu („McAfee“, bez dat.). Postoji mnogo vrsti zlonamjernih softvera te svaki od njih ima svoju svrhu.

- **Trojan Horse** - Trojanski zlonamjerni softver maskira se kao bezopasan program, što ga čini jednom od vrsta zlonamjernog softvera koju je najteže otkriti. Ova vrsta zlonamjernog softvera sadrži zlonamjerni kod i upute koje, nakon što ih žrtva izvrši, mogu djelovati ispod radara. Često se koristi za propuštanje drugih vrsta zlonamjernog softvera u sustav („CyberArk“, bez dat.).
- **Ransomware** - Ransomware je vrsta zlonamjernog softvera koji prijeti objavljivanjem ili blokiranjem pristupa podacima ili računalnom sustavu, obično šifriranjem, sve dok žrtva napadaču ne plati otkupninu. U mnogim slučajevima postoji rok do kojeg žrtve moraju ispuniti napadačev zahtjev (u većini slučajeva to je otkupnina). Ako žrtva ne plati na vrijeme, podaci nestaju ili se javno objavljuju te prouzrokuju još veću štetu. (proofpoint) Cyptolocker, Petya i Loky neki su od najčešćih i najozloglašenijih vrsti ransomware-a („CyberArk“, bez dat.).
- **Spysware** - Ovaj zlonamjerni softver omogućuje cyber kriminalcima neovlašteni pristup podacima, uključujući osjetljive informacije poput podataka o plaćanju i vjerodajnica (Cassetto, 2023). Spyware prikuplja osobne i osjetljive podatke koje šalje oglašivačima, tvrtkama za prikupljanje podataka ili zlonamjernim akterima radi zarade („Fortinet“, bez dat.). Cilj spyware-a je ostati čim duže neotkriven na zaraženim uređaji kako bi izvukao što više informacija.

2.1.2. Napad društvenim inženjeringom

Prema De Groot (2023), Napadi društvenim inženjeringom obično uključuju neki oblik psihološke manipulacije, zavaravajući korisnike ili zaposlenike da predaju povjerljive ili osjetljive podatke. Društveni inženjering uključuje sve vrste komunikacije kako bi napadač izazivao ljubavne, društvene ili slične emocije u žrtvi, navodeći žrtvu da otkrije osjetljive informacije, klikne na zlonamjerni link ili otvori zlonamjernu datoteku. Na slici 1. prikazan je životni ciklus društvenog inženjeringa.

Slika 1. Životni ciklus društvenog inženjeringa (Izrada prema: „Imperva“, bez dat.)

Napadi društvenim inženjeringom događaju se u jednom ili više koraka. Jedan primjer životnog ciklusa društvenog inženjeringa može izgledati ovako: Počinitelj prvo istražuje željenu žrtvu (tj. organizaciju) kako bi prikupio potrebne informacije, kao što su potencijalne točke proboja i slabi sigurnosni protokoli što je potrebno za nastavak napada. Zatim napadač pronalazi osobu unutar organizacije pokušava steći povjerenje te osobe. Nakon stjecanja povjerenja napadač žrtvi pruža poticaje (društveni, novčani…) za naknadne radnje koje krše sigurnosne protokole, poput otkrivanja osjetljivih informacija ili odobravanja pristupa kritičnim resursima. Kad napadač postigne svoj cilj, on počinje prekrivati sve svoje tragove te naposlijetku prekida sve kontakte s žrtvom i time dolazi do završetka napada.

Napadi društvenim inženjeringom:

- **Scareware sigurnosni softver** – Softver koji se pretvara da skenira viruse, a zatim korisniku redovito prikazuje lažna upozorenja i otkrivanja. Napadači mogu tražiti od korisnika da plati za uklanjanje lažnih prijetnji sa svog računala ili da kupi licencu za softver (Cassetto, 2023). Korisnici koji padnu na ovakve laži prenose svoje financijske podatke napadaču s čime napadači duplo profitiraju. Oni dobiju novac, ali i ostale žrtvine osobne podatke koje mogu dalje preprodati ili zlouporabiti.
- **Deepfakes** – Vrlo sofisticirana, nova vrsta napada koja koristi društveni inženjering. Oni uključuju korištenje umjetne inteligencije za stvaranje fotografija, videa i glasovnih zapisa koji omogućuju napadaču da zvuči kao netko drugi. Ova lažna predstavljanja mogu zvučati vrlo realistično i uvjerljivo (Team, 2021).
- **Phishing** – Prema („*Imperva*“, bez dat.) Phishing prevare najčešća su vrsta napada društvenim inženjeringom. Obično su u obliku e-pošte koja izgleda kao da je iz provjerenog izvora. Ponekad će napadači pokušati natjerati žrtvu da oda podatke o kreditnoj kartici ili druge osobne podatke. U drugim slučajevima, phishing e-poruke šalju se kako bi se dobili podaci za prijavu zaposlenika ili drugi detalji za korištenje u daljnjem napadu na njihovu tvrtku. Napadi poput APT-a i Ransomware-a često počinju s phishing napadom.

2.1.3. Napredne dugotrajne prijetnje (APT)

APT napad je vrsta kibernetičkog napada u kojem napadač ili cijeli njegov tim uspostavlja nedopuštenu, dugotrajnu prisutnost u nekom sustavu kako bi prikupljao vrlo osjetljive podatke. Takvi napadi su pomno planirani i osmišljeni kako bi se ubacili u određenu organizaciju, izbjegli postojeće sigurnosne mjere i prošli ispod radara („CrowdStrike“, 2023). Zbog razine napora potrebnog za izvođenje takvog napada, APT-ovi se obično usmjeravaju na mete visoke vrijednosti, kao što su države i velike korporacije, s krajnjim ciljem krađe informacija tijekom dugog vremenskog razdoblja („Kaspersky“, bez dat.). Glavna opasnost APT napada je da čak i kada su otkriveni i čini se da je prijetnja nestala, hakeri su možda ostavili višestruka „stražnja vrata“ koja im omogućuju da se u sustav vrate kada žele. Osim toga, mnoge tradicionalne cyber obrane, poput antivirusnih programa i vatrozida, ne mogu uvijek zaštititi od ovih vrsta napada.

2.1.4. DDoS (engl. Distributed Denial of Service)

Cilj napada distribuiranim uskraćivanjem usluge je opteretiti ciljani sustav i uzrokovati njegovo prestanak funkcioniranja, uskraćujući pristup svojim korisnicima (Cassetto, 2023). DDoS napadi postižu učinkovitost korištenjem više kompromitiranih računalnih sustava kako bi preko njih usmjerili sve njihove raspoložive resurse na jedan ciljani sustav („CloudFlare“, bez dat.). Za takve napade mogu se koristiti sve vrste kompromitiranih IoT uređaja (npr. Stolna računala, mobiteli, itd…). DDoS se također može koristiti kao maska za druge zlonamjerne aktivnosti kao što je onemogućavanje sigurnosnih uređaja i probijanje sigurnosnih protokola istih.

Postoje tri primarne klase DDoS napada, koji se uglavnom razlikuju prema vrsti prometa koji napadaju sustave žrtava:

- **Napadi temeljeni na volumenu** - Ova klasa napada pokušava stvoriti prekid podataka trošenjem cijele dostupne propusnosti između ciljane stranice i interneta. Velike količine podataka šalju se meti korištenjem nekog od načina stvaranja masovnog prometa, kao što su zahtjevi s Botneta („CloudFlare“, bez dat.).
- **Napadi aplikacijskog sloja** - U ovim napadima napadač pokušava preopteretiti određene funkcije aplikacije kako bi aplikaciju učinio nedostupnom ili da aplikacija ne reagira na zahtjeve korisnika. („Amazon Web Services [AWS]“, 2023).
- **TCP SYN flood napad** - napadi preplavljuju ciljani sustav zahtjevima za povezivanje. Kada ciljani sustav pokuša uspostaviti vezu, napadačev uređaj ne reagira, prisiljavajući ciljani sustav da pričeka da do kraja istekne vrijeme za povezivanje. Ovo brzo ispunjava red čekanja za povezivanje, sprječavajući druge korisnike da se povežu na sustav (Cassetto, 2023).

3. Upravljanje kibernetičkim rizikom (CSRM) kroz integrirani pristup upravljanju rizicima (ERM)

Integrirano upravljanje rizicima (*Enterprise Risk Management*, ERM), koji se ponekad naziva i strateško upravljanje rizicima, važan je element učinkovitog sustava korporativnog upravljanja koji obuhvaća aktivnosti i strategije koje omogućuju poduzeću da identificira, mjeri, smanji ili iskoristi, te da kontrolira i prati izloženost različitim vrstama poslovnih rizika poput strateških, financijskih i operativnih (Miloš Sprčić i Dvorski Lacković, 2023). Prema Brodeur i Pergler (2010.) taj sustav upravljanja većinom funkcionira na principu top-down strategije, što ustvari znači da se sve odluke događaju na najvišoj razini u poduzeću te se nakon toga prenose na niže razine zbog lakše provedbe. Naime top-down strategija se može provesti u 3 mjeseca, dok za bottom-up strategiju je potrebno 12 do 24 mjeseci. Prema Hayesu (2022.) cilj ERM-a je identificirati, procijeniti i pripremiti se za potencijalne gubitke i opasnosti koje mogu dovesti poslovanje do gubitka ili nanijeti veliku štetu poduzeću.

Umjesto da svaka poslovna jedinica upravlja svojim rizicima, ERM zahtijeva da se napravi posebna jedinica koja će upravljati rizicima cijelog poduzeća. Samim time ERM može minimalizirati rizik i otkriti jedinstvene prilike za poduzeće. Da bi se ERM uspješno proveo najvažnije je da su sve poslovne jedinice međusobno u dobroj komunikaciji jer često zna doći do neslaganja lokalnih i vrhovnih menadžera (Hayes, 2022).

Uvođenje ERM-a u poduzeće je proces u koji je potrebno uložiti vremenske, materijalne i ljudske resurse. Također to je proces koji zahtijeva da se kontinuirano nadzire i nadograđuje, sukladno s najnovijim spoznajama i aktualnim zbivanjima. U nastavku možemo vidjeti sliku u kojoj se spominju neke od najvažnijih karakteristika ERM-a (Miloš Sprčić i Dvorski Lacković, 2023).

ERM	Usmjerenost na portfolio rizika te njihovo cjelovito upravljanje. Analiziraju se i razumiju međuovisnosti među različitim rizicima kao i uzroci rizika. Definirani su apetit i tolerancija prema riziku.
	Nadzorni odbor i vrhovni menadžment direktno su uključeni u ERM sustav, koji ima važnu ulogu u korporativnom upravljanju. Upravljanje rizicima uključeno je u strateško odlučivanje.
	Perspektiva je pozitivna- upravljanje rizicima sagledava ne samo potencijalne gubitke i prijetnje već i prilike za stvaranje vrijednosti.
	Proces upravljanja rizicima je strukturiran, politika i postupci upravljanja rizicima su dobro definirani. Implementiran je registar rizika i mapa rizika. Određeni su vlasnici svih prepoznatih rizika te postoji jasna odgovornost za upravljanje.
	Praćenje i izvješćivanje je sustavno, kao i prijenos informacija kroz organizaciju te s vanjskim dionicama. Kultura rizika je dio organizacijske kulture. ERM se kontinuirano unapređuje.

Tablica 1. Karakteristike integriranog upravljanja rizicima (Miloš Sprčić i Dvorski Lacković, 2023).

U našem slučaju ćemo govoriti o upravljanju kibernetičkim rizikom (Cybersecurity Risk Management, CSRM) kroz ERM proces. Ukoliko želimo uspješan ERM moramo imati vrlo dobro postavljene tzv. Registre kibernetičkih rizika. Prema NISTu (2020) oni pružaju konzistentnost u bilježenju i prenošenju informacija o rizicima kroz cijelo poduzeće. Pomoću njih možete pratiti i kontrolirati nedostatke u mnogim segmentima poduzeća na jednom mjestu kao i pratiti potencijalne informacije o riziku pojedinih projekata. Registri se unutar poduzeća prenose između svih poslovnih jedinica te svaki registar sadrži svoje informacije o stvarima poput: opisu rizika, izvoru prijetnje, udarcu na poduzeće, vjerojatnosti događanja, ishodu, razini rizika, trošku te planu rješavanja („CyberSaint Security“, bez dat.). Na slici 2. možemo vidjeti primjer ispunjenog registra rizika.

Rizik	Izvor prijetnje	Udarac	Vjerojatnost	Ishod	Razina rizika	Trošak	Plan rješavanja
Ugroženi podaci prijave u sustav	Zlonamjerni E-mal	-120 sati	Srednja	Gubitak organizacijskih računa	Srednja	100 sati	Organizacijski mailovi se provjeravaju softverski za prijetnje
Curenje podataka	Korištenje interneta na poslovnim uređajima u osobne svrhe	-300 sati	Mala	Neovlašteni pristup nezaposlenim osobama	Velika	50 sati	Ograničiti pristup web sadržaju nepotrebnom za funkcioniranje organizacije
Zaštita medijskih podataka na mobitelu	prijenosni digitalni medij nije sigurnosno kopiran	-250 sati	Velika	gubitak podataka i imovine tvrtke	Velika	120 sati	Zapisivati i izvještavati o svim mobilnim medijima, tko ima pristup i njihov sadržaj
Ugrožena cloud mreža	Davatelj cloud usluge koristi nešifriranu mrežu	-100 sati	Mala	Primljeni i poslani podaci davatelju usluge su ugroženi	Mala	50 sati	Promjena davatelja usluge

Slika 2. Primjer registra rizika (Izrada prema: „CyberSaint Security“, 2020.)

S obzirom da se provođenje implementacije ERM-a mora prilagoditi poduzeću i njezinom postojećem poslovanju, ne postoji jedinstveni stav kako provesti njegovu implementaciju. Zato postoje smjernice odnosno standardi koji služe poduzećima da olakšaju njegovu provedbu (Miloš Sprčić i Dvorski Lacković, 2023). Kao što postoje standardi za provedbu ERM-a, tako postoje i standardi za njegovo poboljšanje. U našem slučaju ćemo obraditi detaljniju analizu provedbe NISTIR 8286 standarda, na postojeći ERM u poduzeću, koji služi za poboljšanje upravljanja kibernetičkom sigurnosti. Prema NISTu (2020.) on se sastoji od 7 komponenata:

- Analiza unutarnjeg okruženja
- Prepoznavanje rizika
- Analiziranje rizika
- Prioritiziranje rizika
- Planiranje i provođenje strategije za rješavanje rizika
- Rizik kao prilika poduzeća
- Registar kibernetičkih rizika na razini poduzeća

3.1. Unutarnje okruženje

(„Establish the Context“, bez dat.) spominje da prije utvrđivanja rizika, najprije trebamo odlučiti o opsegu aktivnosti koje planiramo provesti, uključujući svoje ciljeve, i razviti razumijevanje svoje radne okoline. Analiziranje internog okružena definira opseg procesa upravljanja rizikom i postavlja kriterije prema kojima će se rizici procjenjivati. Opseg treba odrediti u sklopu organizacijskih ciljeva tvrtke. Rizici su neizvjesnosti koje utječu na postizanje poslovnih ciljeva, pa se rizici ne mogu u potpunosti identificirati ako su ti ciljevi i strategije nejasni. Odabir ključnih ciljeva unutar poslovanja trebao bi biti vođen procjenom vanjskog i unutarnjeg okruženja koje trenutno može utjecati na tvrtku. Pregled vanjskih i unutarnjih okruženja na početku planiranja procjene rizika pomaže u identificiranju procesa koji mogu biti podložni povećanim rizicima i, kao takvi, izvukli bi najveću vrijednost iz procjene rizika.

Unutarnje okruženje odnosi se na upravljanje i strukturu te kulturu i filozofiju upravljanja rizicima, uključujući sklonost tvrtke riziku (Miloš Sprčić i Dvorski Lacković, 2023). Stoga bi kultura organizacije trebala poticati transfer informacija i rasprave o rizicima od srednjeg menadžmenta do vrhovnog menadžmenta i nadzornog odbora. Vrhovni menadžeri trebali bi razgovarati licem u lice s menadžerima na nižim razinama o upravljanju rizicima, npr. dati povratne informacije o izvješćima o rizicima ili zahtijevati dodatne informacije, bez obzira na to postoje li odstupanja od poslovnih planova (Miloš Sprčić i Dvorski Lacković, 2023; prema CIMA & CGMA, 2015).

Prema Miloš Sprčić i Dvorski Lacković (2023) zapošljavanje glavnog menadžera rizika (*Chief Risk Officer*, CRO) se smatra kao jedna od složenijih komponenti zrelosti ERM sustava. Glavni menadžer rizika (CRO) preuzima vlasništvo nad sustavom integriranog upravljanja rizicima te nosi najveću odgovornost za nadzor centraliziranog procesa upravljanja rizicima. Uloga CRO posebno je važna u kontekstu upravljanja kibernetičkim rizikom, a u većim poduzećima često surađuje s funkcijom *Chief Information Security Officer* (CISO) (Miloš Sprčić i Dvorski Lacković, 2023), koja je zadužena za informacijsku sigurnost.

3.2. Prepoznavanje rizika

Nakon procjene unutarnje okoline slijedi nam prepoznavanje rizika te bilježenje istog u registar rizika. To uključuje pozitivne, ali i negativne rizike na koje poduzeće može naići.

Postoji više vrsti pristupa prepoznavanja rizika, ali najčešći je metodologija koja slijedi ova tri pravila („European Cybersecurity Competence Community [ECCO]“, bez dat.) :

- Identificiranje imovine
- Identificiranje prijetnje toj imovini
- Identificiranje ranjivosti

3.2.1. Identificiranje imovine

Kako biste odredili svoju izloženost kibernetičkom riziku, prvo morate analizirati svu imovinu koju posjedujete. Nažalost u većini slučajeva ne možete zaštititi sve, stoga morate odlučiti što Vam ima veći, a što manji prioritet za zaštitu („ECCO“, bez dat.). National Institute of Standards and Technology [NIST] (2018.) opisuje imovinu kao „podaci, osoblje, uređaji, sustavi i objekti koji omogućavaju poduzeću da neprekidno obavlja svoj rad“. Za davanje prioriteta imovini, ne gleda se samo cijena te imovine nego u obzir treba uzeti i njezinu dugotrajnu uporabu. Kao što je na primjeru NIST (2020.) objašnjeno, organizacija bi mogla izračunati izravne troškove nekog istraživanja i razvoja novog proizvoda, ali dugoročni gubici krađe vlasništva proizvoda mogli bi utjecati na buduće prihode, cijene dionica, reputaciju poduzeća i konkurentsku prednost.

3.2.2. Prepoznavanje prijetnji

Analiza prijetnji uključuje prepoznavanje potencijalnih izvora koji mogu nanijeti štetu imovini (informacijama, podacima, te fizičkoj imovini). Prijetnja može nastati od strane osobe s štetnim namjerama, ali također može nastati nenamjerno ili neizbježno kao npr. Prirodna katastrofa, tehnički kvar ili ljudska pogreška (NIST, 2020).

Čak i kada su prijetnje jasno povezane s kibernetičkom sigurnosti, mora se precizirati vrsta prijetnje. Npr. Hakiranje predstavlja ozbiljnu prijetnju poduzeću. DDoS hakiranje će blokirati pristup vašim podacima (čineći ih nedostupnima). Ransomware napad učiniti će isto (i natjerati Vas da platite u tom procesu ako hoćete doći do svojih podataka). Napad zlonamjernog softvera može instalirati program za čitanje svega što tipkate na računalnim tipkovnicama te na taj način ukrasti podatke. Zato je vrlo važno da se prepozna točna vrsta prijetnje da bi se na pravi način reagiralo („ECCO“, bez dat.).

3.2.3. Prepoznavanje ranjivosti imovine

Sljedeći korak u prepoznavanju rizika je prepoznati ranjivosti imovine koju posjedujete. Veliki problem kod velikog broja poduzeća je što zaposlenici nisu dovoljno educirani o kibernetičkoj sigurnosti. Samim time poduzeće postaje ranjivo jer npr. Zaposlenici imaju slabe zaporke ili nisu upoznati s e-mail prijetnjama.

Određene slabosti, kao što su pogreške u softveru, pogrešne konfiguracije i prisutnost zlonamjernog softvera mogu se identificirati pomoću automatiziranih programa. (NIST, 2020)

3.3. Analiziranje rizika

Svaki rizik koji se nalazi u registru kibernetičkih rizika se analizira kako bi se procijenila vjerojatnost da će se taj rizični događaj dogoditi i da bi se utvrdile posljedice tog događaja. (NIST, 2020) Analizu rizika treba redovito provoditi kako bi se identificirale nove potencijalne prijetnje. Najčešće stavke analize su: analiza rizika mrežne sigurnosti i analiza rizika informacijske sigurnosti. To su ključne stavke koje se moraju analizirati u svakom poduzeću kako bi se identificirala najvažnija imovina koja se može naći u središtu kibernetičkog napada („Centraleyes“, bez dat.).

3.3.1. Metode analiziranja rizika

- Kvalitativne
- Kvantitativne

Kvalitativne metode mjere vjerojatnost i utjecaj određenog rizika na poduzeće. Razumijevanje mogućnosti da se rizični događaj dogodi i značaja koji će on imati za poduzeće, omogućuje poduzeću da odredi prioritet s kojim se rizicima treba prvo pozabaviti („Centraleyes“, bez dat.). Neke od kvalitativnih metoda koje se primjenjuju za kibernetički rizik su: fokus grupa, Delfi metoda i analiza povijesnih događaja.

Miloš Sprčić i Dvorski Lacković (2023.) navode da je cilj *fokus grupe* da pojedinci koji su direktno uključeni u upravljanje kibernetičkim rizicima rasprave određenu temu na temelju podataka koje su dobili od organizacijskih jedinica. Važno je da fokus grupu čine eksperti i da je omogućeno da svaki ekspert izrazi svoj pogled i mišljenje vezano uz specifično područje na kojem bi se mogao javiti rizik. Idealna veličina za fokus grupu je šest do dvanaest sudionika što osiguravaju da je grupa dovoljno velika za stvaranje proaktivnih i različitih ideja, ali ne prevelika da bi ljudi mogli propustiti priliku za svoj doprinos („WorkSafe“, bez dat.).

Metoda *analiza povijesnih događaja* temelji se na diskusiji i kvalitativnoj analizi eksternih i internih događaja koji su imali utjecaj na poduzeća te razumijevanju posljedica koje su nastale kao rezultat tih događaja. Ova nam analiza omogućuje da vidite isti događaj iz različitih perspektiva, omogućujući vam da steknete dragocjene uvide u to kako odgovoriti na određene rizike ili kako poboljšati odgovor vaše tvrtke na isti rizik (Miloš Sprčić i Dvorski Lacković, 2023).

Kvantitativna metoda uključuje brojčane vrijednosti. To znači da se kod ove metode može statistički prikazati vjerojatnost i brojčano vrednovanje dobitka ili gubitka. Prema članku Centralayesa (bez dat.) savršena je za određivanje troškova ili vremena koje će biti potrebno za odrađivanje projekta. Ukoliko se analizirani rizik dogodi, posljedice se mogu izraziti u financijskom i tehničkom obliku (NIST, 2020).

Kvantitativne metode *analiza scenarija i analiza osjetljivosti* temelje se na osmišljanju specifičnih stresnih scenarija kod kojih se kvantificira vjerojatnost i učinak određenih rizičnih događaja na poslovne ciljeve poduzeća. Važnost pri provođenju ovih analiza se stavlja na detaljno definiranje svih pretpostavki određenog scenarija (Miloš Sprčić i Dvorski Lacković, 2023).

Prilikom odabira metode poduzeće mora odlučiti da li im se više isplati ići na skuplju kvantitativnu ili jeftiniju kvalitativnu metodu. Kvalitativna metoda otkriva većinu rizika te dovodi do najvećeg smanjivanja tih rizika u većini slučajeva. Dok je kvantitativna metoda skuplja, no zato ona daje detaljnije rezultate i može se koristiti za specifične scenarije (Quinn i sur., 2021).

3.4. Prioritiziranje rizika

Nakon identificiranja, analize rizika i njihovog evidentiranja u registar kibernetičkih rizika, trebalo bi odrediti i naznačiti prioritete tih rizika. Prioritiziranje rizika važno je da bismo mogli na vrijeme primijeniti odgovarajuće preventivne mjere koje bi spriječile kibernetičke prijetnje s minimalnim utjecajem na poslovanje („RiskOptics“, 2022). Da bismo odredili razinu prioriteta rizika potrebne su nam informacije kao što su vremenski trendovi, potencijalni događaj, vjerojatnost događaja i kada bi se taj rizik mogao ostvariti (kratkoročno, srednjoročno, dugoročno). Također razina rizika se može odrediti na temelju troškova prevencije i vrijednosti informacija.

Nocco i Stulz (2006; prema Miloš Sprčić i Dvorski Lacković (2023.)) kažu da je bitno angažirati grupe stručnjaka iz različitih odjela, koji poznaju poduzeće i njegovo poslovno okruženje, kako bi procijenili izloženost poduzeća različitim rizicima. Nakon što stručnjaci

postignu konsenzus oko liste rizika, rizici se ocjenjuju na mjernim ljestvicama značajnosti i vjerojatnosti koje su razvijene za specifične potrebe te organizacije. Ljestvica značajnosti je prikazana u Tablici 2. koja ima rang od 1 do 5 s obzirom na utjecaj koji pojedini rizik predstavlja poduzeću u smislu štetnosti koje rizik može prouzročiti. Rizik ocijenjen s ocjenom 5 je najvećeg utjecaja, a rizik ocjene 1 je rizik s najmanjim utjecajem na postavljene ciljne vrijednosti.

Značajnost	Ocjena
Kritična	5
Visoka	4
Srednja	3
Niska	2
Zanemariva	1

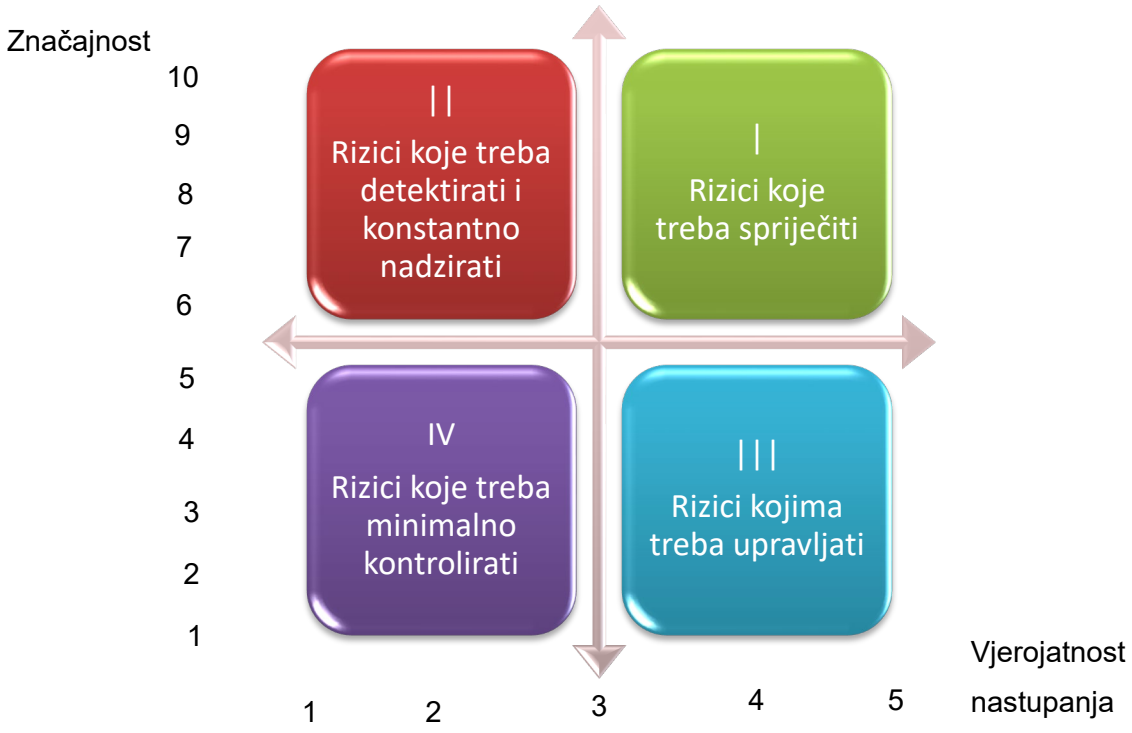
Tablica 2. Primjer alternativne ljestvice procjene značajnosti rizika za nekvantitativne ciljeve poduzeća (Miloš Sprčić i Dvorski Lacković, 2023).

Tablica 3 nam predstavlja procjenu vjerojatnosti nastupanja događaja te se također sastavlja u rangu vrijednosti od 1 do 5. Ako se smatra da je realizacija rizika gotovo nemoguća, rizik dobiva ocjenu 1, dok rizici s ocjenom 5 upućuju na sigurnu realizaciju (Miloš Sprčić i Dvorski Lacković, 2023).

Vjerojatnost	Ocjena	Opis ocjene
< 5%	1	Vrlo rijetko
≥ 5% < 25%	2	Malo vjerojatno
≥ 25% < 65%	3	Moguće
≥ 65% < 95%	4	Vjerojatno
> 95%	5	Gotovo sigurno

Tablica 3. Primjer mjerne ljestvice vjerojatnosti nastupanja rizika (Miloš Sprčić i Dvorski Lacković, 2023).

Kada spojimo ove dvije tablice dobivamo mapu rizika. Prema Miloš Sprčić i Dvorski Lacković (2023) mapiranje rizika pomaže menadžerima da odluče kojim rizicima treba upravljati na korporativnoj razini, koje rizike treba prenijeti na druge sudionike na tržištu i koju kombinaciju mjera treba primijeniti kako bi se postigla optimalna izvedba u smislu upravljanja rizicima. Mapa rizika se prikazuje u koordinatnom sustavu kao što možemo vidjeti na Grafu 1.



Graf 1. Mapa rizika (Miloš Sprčić i Dvorski Lacković, 2023).

Prema položaju rizika u koordinatnom sustavu, poduzeće donosi odluku kojim rizicima treba posvetiti najviše pozornosti odnosno na koje treba odmah reagirati, a koji rizici ne predstavljaju značajnu opasnost prema poduzeću te se mogu kasnije rješavati ili u potpunosti zanemariti (Miloš Sprčić i Dvorski Lacković, 2023).

Primjer: Cyber napad na jedan Data centar će poduzeće koštati 10.000$ te mu se može dodijeliti prioritet 1. razine. A u drugom slučaju ako postoji mogućnost napada na cjelokupnu cloud infrastrukturu poduzeća i rezultat tog napada je gubitak preko 1 milijun dolara, tom riziku dodijelit će se prioritet 5. odnosno najviše razine („RiskOptics“, 2022).

3.5. Planiranje i provođenje strategije za rješavanje rizika

Cilj učinkovitog upravljanja rizikom, uključujući rizike kibernetičke sigurnosti, je identificirati načine za smanjivanje ili toleranciju potencijalnih rizika na što je moguće isplativiji način (NIST, 2020). Kao što smo prije spomenuli postoje pozitivni i negativni rizici. Način reagiranja na njih je različit. Za negativne rizike moramo poduzeti određene korake da čim više smanjimo negativan ishod koji oni mogu potencijalno izazvati. Dok pozitivne rizike uzimamo u obzir kao prilike koje poduzeće može iskoristiti te poboljšati i unaprijediti svoje poslovanje („AWS“, 2023).

Rizik	Smanjivanje	Smanjivanje vjerojatnosti pojave rizika
	Prenošenje	Prebacivanje odgovornosti za rizik na vanjskog suradnika
	Izbjegavanje	Uklanjanje aktivnosti koja bi mogla izazvati rizik
	Prihvaćanje	Staviti do znanja za rizik postoji, ali ne poduzeti nikakvu akciju da se spriječi

Tablica 4. Vlastita izrada (Prema izvoru: „AWS“, 2023).

Primjena ovih strategija ne mora značiti da će menadžeri odabrati samo jednu od njih. Često se događa da menadžeri primjenjuju hibridnu strategiju, tj. Da se koristi više strategija odjednom kako bi se postigao željeni učinak (NIST, 2020).

1. **Smanjivanje**

   Primjenjivanje akcije koja smanjuje prijetnje, ranjivosti i utjecaje danog rizika na prihvatljivu razinu

   Rješenja mogu dovesti do sprečavanja gubitak resursa poduzeća (npr. Smanjenje vjerojatnosti da prijetnja uspije naštetiti poduzeću tako da se uvedu dodatne preventivne mjere poput pojačane enkripcije podataka) ili barem ograničiti taj gubitak (Iqbal, 2019).

2. **Prenošenje**

   Najčešći primjer ove strategije je kupovina usluge nekog vanjskog suradnika (npr. Kupovina osiguranja kibernetičke sigurnosti). Iako takva osiguranja pružaju povratak financijskih sredstava u slučaju napada ili prirodne katastrofe, često posljedice poput gubitka povjerenja kupaca dugotrajno ostavljaju negativan dojam o poduzeću (Iqbal, 2019).

3. **Izbjegavanje**

   U nekim slučajevima ako menadžeri procijene da je izloženost riziku veća od neke njihove određene tolerancije, oni će utvrditi da je najbolja strategija djelovanja upravo ta da se uopće ne provodi aktivnost koja bi mogla dovesti do rizika.

   Kao primjer možemo navesti neko proizvodno poduzeće koje ne želi spojiti svoj pogon na Internet zbog prevelikog rizika da će netko to zlouporabiti, što može dovesti poduzeće u velike financijske dugove ukoliko se onesposobi pogon na duže vrijeme (Iqbal, 2019).

4. **Prihvaćanje**

   Ukoliko se rizik nalazi unutar prihvatljive razine tolerancije, ne poduzimaju se nikakve akcije prevencije. Iako se ništa ne poduzima za prevenciju, takav rizik se i dalje mora prijaviti i pratiti da bi se osiguralo da on ostaje u prihvatljivoj razini tolerancije (Iqbal, 2019).

Budući da se rizici kibernetičke sigurnosti i njihovi utjecaji na druge rizike često mijenjaju, poduzeće rizike treba stalno pratiti kako bi se osiguralo da ostanu unutar prihvatljivih razina (NIST, 2011). Na primjer, kontinuirano praćenje može odrediti kada se negativni rizici približavaju granici tolerancije koja je postavljena za taj specifični rizik. Nadalje ono automatski može javiti uzbunu i zahtjev za ponovni pregled tog rizika da bi se pravovremeno reagiralo i implementirale dodatne mjere za rješavanje istog (NIST, 2020).

3.6. Rizik kao prilika poduzeća

U kibernetičkoj industriji pozitivni rizici se odnose na potencijalnu dobit imovine, znanja i sveukupnog poboljšanja („AWS“, 2023). Mnoga poduzeća još uvijek ne uzimaju u obzir da rizik može predstavljati i poslovnu priliku, što ih stavlja u lošu poziciju zbog mogućih propuštenih poslovnih prilika. Primjer rizika kao poslovne prilike možemo navesti kada poduzeće uvede inovaciju ili samoinicijativno uvede viši stupanj kibernetičke zaštite, prije nego se dogodi kibernetički napad. Jedna od tih inovacija je segmentacija mreže i kontrola pristupa s najmanjim privilegijama. Nesbo (2022.) nam objašnjava kako segmentacija mreže uključuje podjelu mreže na manje, izolirane segmente kako bi se ograničile kibernetičke prijetnje, dok implementacija kontrole pristupa s najmanjim povlasticama osigurava da korisnici i sustavi imaju pristup samo onim resursima koji su potrebni za njihove uloge. Ove proaktivne mjere ograničavaju sposobnost napadača da se slobodno kreće unutar mreže i pristupi osjetljivim informacijama, smanjujući potencijalni učinak kibernetičkog napada. Kada se poduzeće odluči vremenski i financijski riskirati uvesti ovakve inovacije, one značajno mogu poboljšati cjelokupni kibernetički položaj organizacije i smanjiti vjerojatnost uspješnih kibernetičkih napada.

Vodafone (2017.) je proveo istraživanje koje pokazuje da izvršno vodstvo razumije negativne kibernetičke rizike, ali često ne razumije pozitivan rizik ili poslovnu vrijednost. Međutim ovo istraživanje pokazuje da vodstvo CSRM-a razumije koliko je važno imati jaku kibernetičku sigurnost i koju važnost to daje poduzeću. Istraživanje je provedeno 2017. godine na 1434 ispitanika, uključujući mala, srednja i velika poduzeća koja djeluju u jednoj ili više zemalja. 61% intervjua obavljeno je s poduzećima s manje od 250 zaposlenika, a 39% s poduzećima s 250 ili više zaposlenika.

Prema izvješću („Vodafone“, 2017):

- 73% ispitanika smatra da poboljšana sigurnost stvara nove poslovne prilike.
- 89% ispitanika je reklo da bi poboljšanje njihove sigurnosti povećalo lojalnost i povjerenje kupaca.
- 89% vjeruje da je posjedovanje učinkovite kibernetičke sigurnosti relevantna konkurentska prednost koja im pomaže da se razlikuju od svojih konkurenata.

Kao što smo kroz cijeli rad naglašavali važnost ulaganja u upravljanje kibernetičkim rizikom i na koji način poboljšati kibernetičku sigurnost, tako se i u izvješću spominje da 73% rastućih poduzeća ulažu u kibernetičku sigurnost i čine je sastavnim dijelom svog ICT proračuna. To vjerojatno objašnjava zašto ove tvrtke imaju tako širok raspon financijskih

prednosti nad drugima. Te prednosti uključuju povećanu lojalnost kupaca, privlačenje novih kupaca, mogućnost lansiranja novih proizvoda i usluga.

Pošto su pozitivni rizici relativno novi pojam u kibernetičkom svijetu, oni se često stavljaju u poseban registar tzv. Registri prilika. Ako poduzeće odluči uvesti pozitivne rizike u svoje poduzeće, postoje 4 strategije djelovanja koje može koristiti (NIST, 2020).

1. **Iskorištavanje**
   Maksimiziranje vjerojatnosti pojave rizika kako biste ostvarili njegov pozitivan učinak (Iqbal, 2019).
2. **Udjeljivanje**

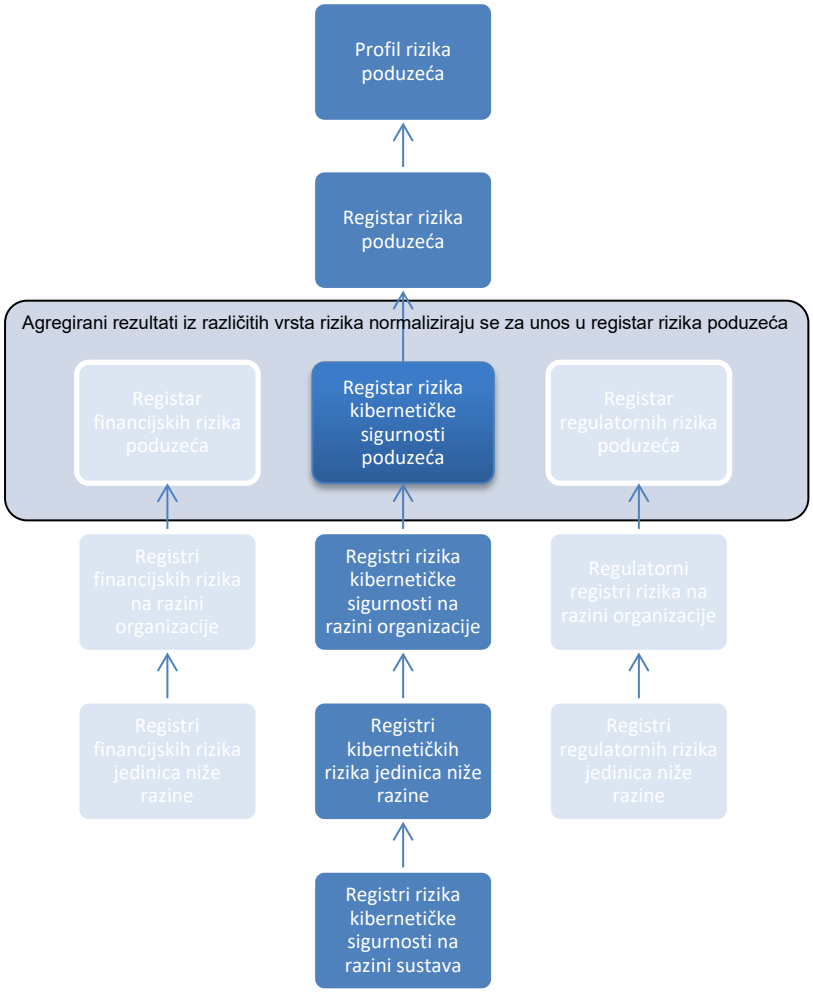
   Dodijelite vlasništvo drugom poduzeću koje može bolje iskoristiti priliku, da bi u budućnosti oba poduzeća imali koristi od tog proizvoda (Iqbal, 2019).

3. **Poboljšanje**
   Povećati vjerojatnost i pozitivan učinak prilike (npr. ulagati ili sudjelovati u obećavajućoj kibernetičkoj tehnologiji) (Iqbal, 2019).
4. **Zanemarivanje**
   Zanemariti mogućnost rizika i ne poduzimati ništa. Ova strategija je uobičajena kada je vjerojatnost rizika vrlo niska ili kada su koristi od potencijalnog pozitivnog ishoda minimalne (Iqbal, 2019).

3.7. Registar kibernetičkih rizika na razini poduzeća

Ključni ishod identifikacije rizika i komunikacijskih elemenata potrebnih za rješavanje tih rizika je sposobnost stvaranja registra kibernetičkih rizika na razini poduzeća. Svaka razina poduzeća ima jedinstven skup kibernetičkih rizika koji se moraju uključiti pri razmatranju ERM-a. Integracija sadržaja registara kibernetičkog rizika (Cybersecurity Risk Register, CSRR) niže razine u registre više razine omogućuje učinkovit prijenos informacija o riziku iz CSRM-a u ERM.

Kada se neki registar napravi, on se odmah može vidjeti na svim razinama poduzeća, no vidljiv je samo zaposlenicima koji imaju dovoljno visoka dopuštenja. Daljnje akcije odlučuju menadžeri registara rizika u poduzeću (Enterprise Risk Register, ERR) koji procjenjuju koliko su važni CSRR-i za uspješno poslovanje poduzeća. Također oni mogu dati ovlaštenja menadžerima nižih razina da imaju uvid u rizike visoke važnosti, što omogućuje poduzeću olakšani način upravljanja kibernetičkim rizicima. (NIST, 2020)



Graf 2. Integracija registara rizika kibernetičke sigurnosti u profil poduzeća (Izrada prema: NIST, 2020.)

4. Analiza slučaja hotelskog lanca Marriott International

4.1. Prva povreda podataka Marriott International

Povreda podataka najgora je noćna mora svakog hotela - osobito kada osobni podaci i podaci o gostima procure. Napad na hotelski lanac je počeo 2014. godine, ali nije bio otkriven sve do 2018. godine (Kerner, 2018). Naime, Marriott je 2016. godine kupio Starwood hotele koji su već bili pod napadom dvije godine. Ova povreda Marriott-ovih podataka razotkrila je osobne podatke stotina milijuna gostiju iz raznih zemalja koji su tijekom proteklih nekoliko godina izvršili rezervacije u objektima poduzeća Starwood (Young, 2021).

Napadači su 2014. godine upali u sustav za rezervaciju gostiju putem Trojan virusa za udaljeni pristup (engl. Remote Access Trojan RAT). Glavni razlog što su lako upali u sustav je bilo Starwood-ovo korištenje neažuriranih Windows Server sustava što je ostavilo otvorena „stražnja vrata“. Pomoću RAT-a napadači su uspjeli doći do korisničkog imena i lozinke jednog od administratora cijelog sustava, što je sve teklo neotkriveno.

Nisu samo Starwood-ovi sigurnosni sustavi krivi za ove katastrofalne posljedice. Marriott je nakon akvizicije otkrio zaseban napad koji se dogodio 2015. godine te povodom tog propusta odlučio je otpustiti cijeli IT odjel Starwood-a. Njihovim otpuštanjem došlo je do nedostatka osoblja za brzo uvođenje Marriott-ovog sustava rezervacija u Starwood hotele te je bilo odlučeno da ostane njihov stari sustav. Ne samo da je to dopustio, nego Marriott se nije ni potrudio da pogleda dublje u njegov sustav te prilikom toga dopustio da se originalni napad, koji traje već dvije godine, nastavi neprekidno odvijati. Napadači su čak uspjeli pronaći ključeve za dešifriranje podataka, dešifrirali podatke, izvukli ih iz sustava te ih potom ponovno šifrirali kako bi ostali neotkriveni. Te akcije su trajale sve do 2018. godine kada je Marriott-ov sustav izdao upozorenje i otkrilo se da imaju ogromni proboj u cijelom sustavu. Napadači su uspjeli izvući podatke od otprilike 500 milijuna gostiju, od čega su kod 327 milijuna gostiju uspjeli izvući podatke kreditnih kartica, putovnica, mobilnih brojeva i sl. Financijska posljedica ovog napada se procjenjuje na 12.5 milijardi dolara.

4.2. Druga povreda podataka

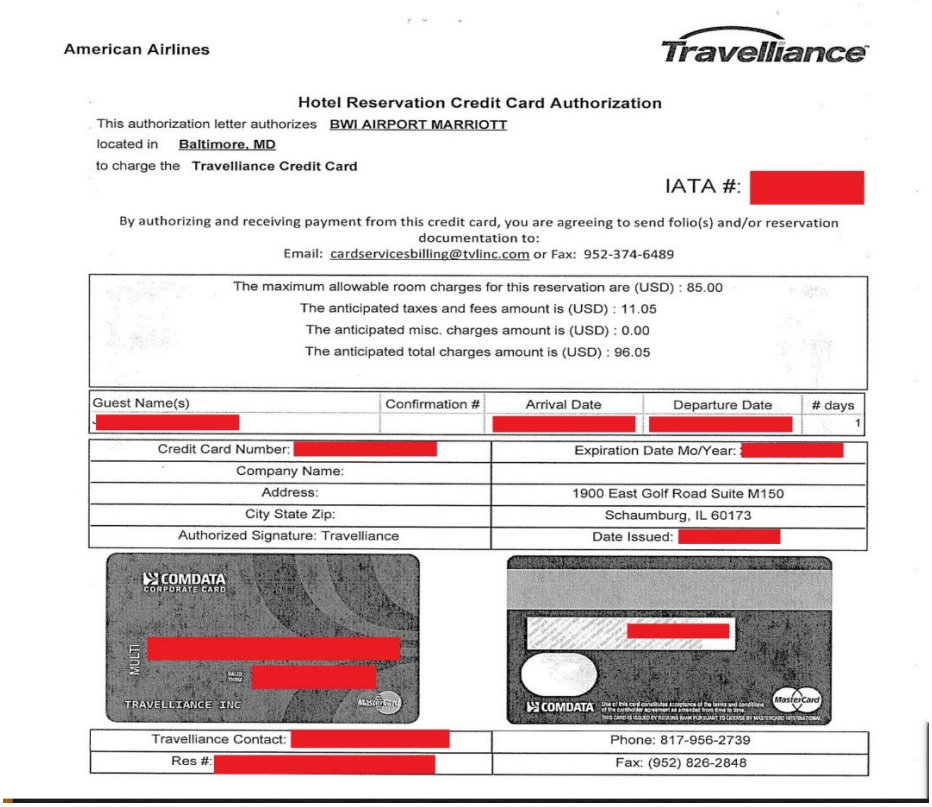
Nakon posljednje velike povrede podataka, očekivalo se da će Marriott ojačati svoju kibernetičku infrastrukturu, obučiti svoje sigurnosne timove i nadograditi svoje sustave. Međutim, najnovija povreda podataka dovodi u pitanje njegove napore u borbi protiv prijetnji. Marriott International prijavila je veliku povredu podataka 31. ožujka 2020., označavajući drugu veliku povredu podataka u posljednje dvije godine. U napadu koji je trajao 2 mjeseca, bilo je zahvaćeno 5.2 milijuna gostiju diljem svijeta („CloudTech“, 2020). Napadači su uspjeli društvenim inženjeringom ukrasti korisnička imena i lozinke dvaju zaposlenika. Ti zaposlenici su imali pristup aplikaciji za pružanje usluga unutar hotela te su preko aplikacije uspjeli doći do daljnjih podataka.

Prema Data Privacy Manageru (2020.) ovaj napad je bio manje razoran nego onaj iz 2014. godine jer nisu razotkriveni kritični podaci poput kreditnih kartica, nego samo kontakt informacije kao npr. Imena, prezimena i mobilni brojevi.

Iz ovog napada možemo zaključiti da Marriott International nije puno ulagao u kibernetičku sigurnost, jer u suprotnom sigurnosni sustavi su trebali otkriti i izvijestiti velik broj zahtjeva za pristup podacima s jednog mjesta. Uvođenjem CSRM-a zasigurno bi se prijetnja otkrila na vrijeme te bi se napad znatno ublažio ili čak i spriječio.

4.3. Treća povreda podataka

Posljednja u nizu povreda podataka se desila 2022. godine. Napadači su kao i 2020. godine iskoristili društveni inženjering na jednom od suradnika u hotelu i tako dobili pristup njegovom računalu (Powell, 2022). Dissent (prema GNN (2020.)) kaže da je u ovom napadu izvučeno 20GB podataka te da oni uključuju podatke kreditnih kartica i povjerljive informacije. Marriott je odmah izvijestio i kontaktirao svih 400 ljudi koji su bili pogođeni napadom.



American Airlines

Travelliance

Hotel Reservation Credit Card Authorization

This authorization letter authorizes BWI AIRPORT MARRIOTT
located in Baltimore, MD
to charge the Travelliance Credit Card

IATA #: [redacted]

By authorizing and receiving payment from this credit card, you are agreeing to send folio(s) and/or reservation documentation to:
Email: cardservicesbilling@tvlinc.com or Fax: 952-374-6489

The maximum allowable room charges for this reservation are (USD) : 85.00
The anticipated taxes and fees amount is (USD) : 11.05
The anticipated misc. charges amount is (USD) : 0.00
The anticipated total charges amount is (USD) : 96.05

Guest Name(s)	Confirmation #	Arrival Date	Departure Date	# days
[redacted]		[redacted]	[redacted]	1

Credit Card Number: [redacted]	Expiration Date Mo/Year: [redacted]
Company Name:	
Address:	1900 East Golf Road Suite M150
City State Zip:	Schaumburg, IL 60173
Authorized Signature: Travelliance	Date Issued: [redacted]

Travelliance Contact: [redacted]	Phone: 817-956-2739
Res #: [redacted]	Fax: (952) 826-2848

Slika 3. Primjer ukradenih podataka iz 3. napada („DataBreaches“, 2022.)

4.4. Problemi zbog nedostatka CSRM-a

Jedno područje u kojem je Marriott dobro prošao bilo je uvođenje nadzornih rješenja za sustave koji sadrže osjetljive podatke. Jedan od programa koji je hotel koristio za zaštitu podataka, IBM Guardium, otkrio je anomaliju u bazi podataka rezervacija gostiju Starwooda 7. rujna. Upozorenje Guardium-a pokrenuo je upit s administratorskog računa za vraćanje broja redaka iz tablice u bazi podataka. Ovaj se upit istaknuo jer je ukazivao na to da ljudski faktor ometa bazu podataka (O'Flaherty, 2019). Međutim, Marriott-ovo praćenje baze podataka bilo je ograničeno. Iako je Guardium na kraju otkrio proboj, napadač je prije toga uspio kopirati cijele tablice. Malo je vjerojatno da se ljudski faktor miješa u upite koji su automatizirani u bazi podataka, tako da se ovaj napad prije mogao otkriti i spriječiti robusnijim rješenjem za nadzor i zaštitu podataka.

I dan danas kao i kod mnogih drugih tvrtki, primjetan je nedostatak stručnosti u upravljanju kibernetičkim rizikom na razini uprave i izvršne uprave Marriotta. Trenutačni odbor ima 14 članova, ali nitko od njih nema iskustvo u kibernetičkoj sigurnosti. Marriott i dalje nema posebno povjerenstvo za kibernetičke rizike („Marriott International News Center“, bez dat.).

4.5. Poduzete mjere tijekom svih napada

Prije nego što se desio prvi napad, Marriott International je imao kupljeno kibernetičko osiguranje koje uključuje pravne troškove, PR troškove i forenzičku analizu (Schwartz, 2021). Ta investicija se pokazala kao dobra odluka jer je pokrila 71 od ukupnih 72 milijuna pravnih i forenzičkih troškova. Marriott je nastavio do današnjeg dana uzimati kibernetičko osiguranje, no žali se da svakim intervalom osiguranje postaje skuplje.

Nakon 2. napada u Marriott-u su vidjeli potrebu za drastičnim poboljšanjem kibernetičke sigurnosti. Zaposlili i napravili tim IT stručnjaka za sigurnost koji su imali zadatak napraviti dubinsku analizu trenutnog sustava i implementirati promjene kako bi osigurali da lanac hotela up-to-date sigurnosne protokole za sprečavanje prijetnji.

Sigurnosni tim je također uveo i novi način pohranjivanja podataka putovnica i kreditnih kartica u poboljšanom šifriranom formatu. Po javnim informacijama iz 2021. godine razmatralo da se ti podaci pohranjuju na svakoj lokaciji da bi se smanjio utjecaj provale bilo kojeg drugog sustava. Makar je sigurnosni tim opet zakazao nakon uvođenja ovih noviteta, ovaj način pohranjivanja se pokazao učinkovitim jer je u posljednjem napadu pogođeno samo 400 gostiju. Svi povrijeđeni podaci su se nalazili na jednoj lokaciji te zato napadač nije uspio napraviti veću štetu.

(Hatcher, bez dat.) spominje da nakon dva uzastopna napada društvenim inženjeringom vodstvo Marriott-a je shvatilo važnost edukacije svojih zaposlenika da se tome odupru. Samim time prije početka rada su uveli obavezne seminare koji educiraju zaposlenike na što trebaju paziti. Napomenuto je i da svi zaposlenici moraju stvoriti kulturu svijesti o sigurnosti, dajući kibernetičkim prijetnjama istu pažnju kao i fizičkim prijetnjama.

5. Zaključak

Današnje digitalno okruženje čini upravljanje kibernetičkim rizikom neophodno za organizacije svih vrsta i sektora. Rasprostranjenost tehnologije, u kombinaciji s kibernetičkim prijetnjama koje se stalno razvijaju, jasno pokazuje koliko je zaštita osjetljivih informacija i kritične infrastrukture zapravo važna. Ova praksa uvođenja upravljanja kibernetičkim rizikom više ne bi trebala smatrati neobaveznom, već bitnom u današnjem poslovnom svijetu. Rizik kibernetičke sigurnosti, potencijalna šteta koju predstavljaju kibernetičke prijetnje, obuhvaća širok skup aktivnosti od povrede podataka i zlonamjernih napada do špijunaže i sabotaže. Kibernetički kriminal predstavlja sve veću opasnost za poduzeća, vlade i pojedince, s financijskim gubicima, štetom po ugledu ili čak nacionalnoj sigurnosti koji su ugroženi jer se opseg i sofisticiranost napada eksponencijalno povećavaju - sve ih je teže predvidjeti ili u potpunosti izbjeći. Organizacije moraju primijeniti proaktivne sigurnosne mjere protiv ovakvih napada tako da ograniče kontrole pristupa, uvedu programi obuke zaposlenika, implementiraju sustave za otkrivanje upada i pravovremeno softversko krpanje te redovno procjenjuju i analiziraju ranjivosti. Kako organizacije sve više ovise o digitalnoj tehnologiji za svakodnevno poslovanje, organizacije moraju koristiti učinkovite strategije upravljanja rizikom kako bi identificirale, analizirale, procijenile i učinkovito ublažile kibernetičke prijetnje s ciljem zaštite imovine, održavanja povjerenja klijenata održavanja operativnog kontinuiteta.

Implementiranje upravljanja kibernetičkim rizikom u integrirani pristup upravljanju rizicima također je ključna komponenta za njegovu ukupnu učinkovitost. Usklađivanjem ciljeva kibernetičke sigurnosti s cjelokupnom strategijom rizika organizacije omogućuje organizaciji da lakše odredi prioritete ulaganja uz učinkovitu alokaciju resursa, potiče svijest o riziku među zaposlenicima i stvara kulturu koja naglašava da se treba paziti kibernetičkih prijetnji. Kroz integrirani pristup upravljanja rizikom, rizik se tretira holistički, a ne pojedinačno što dolazi do izražaja ako organizacija ima više razina poslovanja.

Važno je spomenuti pozitivne rizike koji se odnose na potencijalne koristi i prilike koje mogu proizaći iz strateških sigurnosnih mjera. Prihvaćanje pozitivnih rizika također može dovesti do poboljšane učinkovitosti, budući da organizacije mogu iskoristiti inovativna kibernetička rješenja kako bi stekle konkurentsku prednost u digitalnom okruženju.

6. Popis literature

[1] Amazon Web Services [AWS] (2023). *AWS Best Practices for DDoS Resiliency* Preuzeto 18.8.2023. s AWS Best Practices for DDoS Resiliency - AWS Whitepaper (amazon.com)

[2] Amazon Web Services [AWS] (2023). *AWS Perscriptive Guidance: Positive risk within cybersecurity* Preuzeto 18.8.2023. s AWS Prescriptive Guidance - Positive risk within cybersecurity (amazon.com)

[3] Aminian, N. (2021). *What is Cybersecurity Risk? Definition & Factors to Consider* Preuzeto 7.7.2023. s What is Cybersecurity Risk? Definition & Factors to Consider (securityscorecard.com)

[4] Cassetto, O. (2023). *Cybersecurity threats: Everything you Need to Know* Preuzeto 7.7.2023. s Cybersecurity Threats: Types and Challenges - Exabeam

[5] Centraleyes (bez dat.) *Risk Prioritization* Preuzeto 17.8.2023. s What is Risk Prioritization | Centraleyes

[6] CheckPoint (bez dat.) *What is Cybersecurity Risk Management* Preuzeto 8.7.2023. s What is Cybersecurity Risk Management? - Check Point Software

[7] CloudFlare (bez dat.) *What is a DDoS attack?* Preuzeto 17.8.2023. s What is a distributed denial-of-service (DDoS) attack? | Cloudflare

[8] CloudTech (2020). *Marriott reported another dana breach: Why cyber risk assesment is important* Preuzeto 16.8.2023. s Marriott reported another data breach: Why cyber risk assessment is important (cloudcomputing-news.net)

[9] Cremer, F., Sheehan, B., Fortmann, M. (2022). *Cyber risk and cybersecurity: a systematic review of data availability* Preuzeto 10.7.2023. s Cyber risk and cybersecurity: a systematic review of data availability | The Geneva Papers on Risk and Insurance - Issues and Practice (springer.com)

[10] CrowdStrike (2023). *Advanced Persistent Threat (APT)* Preuzeto 5.9.2023. s What is an Advanced Persistent Threat (APT)? - CrowdStrike

[11] CyberArk (bez dat.) *What is Malware?* Preuzeto 10.7.2023. s What is a Malware Attack? - Definition (cyberark.com)

[12] CyberSaint Security (bez dat.) *Risk Register Examples for Cybersecurity Leaders* Preuzeto 6.9.2023. s Risk Register Examples for Cybersecurity Leaders (cybersaint.io)

[13] Cybersecurity Exchange (bez dat.) *How to Effectively Manage Cybersecurity Risk* Preuzeto 8.7.2023. s What Is Nine Steps of A Cybersecurity Risk Management Framework | EC-Council (eccouncil.org)

[14] DataPrivacyManager (2020). *Marriott security dana breach – what really happened?* Preuzeto 16.8.2023. s Marriott security data breach- what really happened? – Data Privacy Manager

[15] De Groot, J. (2023). *What Are Social Engineering Attacks? (Types & Definition)* Preuzeto 5.9.2023. s What Are Social Engineering Attacks? (Types & Definition) (digitalguardian.com)

[16] Dissent (2022). *EXCLUSIVE: Marriott hacked again? Yes. Here's what we know.* Preuzeto 18.8.2023. s EXCLUSIVE: Marriott hacked again? Yes. Here's what we know. (databreaches.net)

[17] Dvorski Lacković, I. i Miloš Sprčić, D. (2022). Utjecaj upravljanja kibernetičkim rizikom na poslovne pokazatelje poduzeća. *Zbornik Ekonomskog fakulteta u Zagrebu, 20* (2), 33-46. Preuzeto 6.9.2023. s zbornik_ekonomski_2-2022_KB (1) (srce.hr)

[18] Eling, M., McShane, M., Nguyen, T. (2021). *Cyber risk management: History and future research directions* Preuzeto 7.7.2023. s Cyber risk management: History and future research directions (wiley.com)

[19] *Establish the Context* (bez dat.) Preuzeto 6.9.2023. s Risk Management Framework - Establish the Context (charteredaccountantsanz.com)

[20] European Cybersecurity Competence Community [ECCO] (bez dat.) *Cyber Risk Identification* Preuzeto 17.8.2023. s Cyber Risk Identification | Cyberwatching

[21] Executech (bez dat.) *Top 15 types of Cybersecurity Risks & How To Prevent Them* Preuzeto 7.7.2023. s Top 15 Types of Cybersecurity Risks & How To Prevent Them - Executech

[22] Fortinet (bez dat.) *What is Cybersecurity Management?* Preuzeto 7.7.2023. s What Is Cybersecurity Management? Framework, Risks and Trends | Fortinet

[23] Fortinet (bez dat.) *What is Spyware?* Preuzeto 10.7.2023. s What Is Spyware? Definition, Types And Protection | Fortinet

[24] Frigo, M.L. Darren, S.G. (2022). *Strategic Management of Cybersecurity Risks* Preuzeto 7.7.2023. s Strategic Management of Cybersecurity Risks | IMA (sfmagazine.com)

[25] Hatcher, L-J. (bez dat.) *Marriott dana breaches and cybersecurity insurance: a case study* Preuzeto 18.8.2023. s Marriott Data Breaches and Cybersecurity Insurance: A Case Study - VENZA® - Better Visibility. Better Defense. (venzagroup.com)

[26] Hayes, A. (2022). *Enerprise Risk Management (ERM): What Is It and How It Works* Preuzeto 7.7.2023. s Enterprise Risk Management (ERM): What Is It and How It Works (investopedia.com)

[27] Imperva (bez dat.) *Social Engineering* Preuzeto 5.9.2023. s What is Social Engineering | Attack Techniques & Prevention Methods | Imperva

[28] Iqbal, M. (2019). *Negative Risk (threat) and Positive Risk (opportunity) – PMP/CAPM* Preuzeto 16.8.2023. s Negative Risk (threat) and Positive Risk (opportunity) - PMP/CAPM - Mudassir Iqbal, PMP

[29] Kaspersky (bez dat.) *What Is Advanced Persistent Threat (APT)?* Preuzeto 18.8.2023. s What Is an Advanced Persistent Threat (APT)? (kaspersky.com)

[30] Kerner, S. M. (2018). *IT Security Lessons from the Marriott Dana Breach* Preuzeto 16.8.2023. s IT Security Lessons from the Marriott Data Breach (esecurityplanet.com)

[31] Marriott International News Center (bez dat.) *Bord of directors* Preuzeto 18.8.2023. s Leadership | Marriott News Center

[32] McAfee (bez dat.) *What is Malware?* Preuzeto 10.7.2023. s What is malware and how cybercriminals use it | McAfee

[33] Miloš Sprčić, D., Puškar, J., Zec, I. (2019). *Primjena modela integriranog upravljanja rizicima – Zbirka poslovnih slučajeva* Preuzeto 6.9.2023. s Book 1.indb (unizg.hr)

[34] Miloš Sprčić, D., i Dvorski Lacković, L. (2023). *Upravljanje rizicima: Teorijski koncepti i primjena u poslovnoj praksi* Zagreb: Naklada Slap

[35] National Institute of Standards and Technology [NIST] (2018). *Framework for Improving Critical Infrastructure Cybersecurity* Preuzeto 4.9.2023. s Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

[36] Nesbo, E. (2022). *What Is Network Segmentation and How Does It Improve Security?* Preuzeto 7.9.2023. s What Is Network Segmentation and How Does It Improve Security? (makeuseof.com)

[37] O'Flaherty, K. (2019.) *Marriott CEO Reveals New Details About Mega Breach* Preuzeto 16.8.2023. s Marriott CEO Reveals New Details About Mega Breach (forbes.com)

[38] Powell, O. (2022). *OITW: Marriott International suffers latest in series of dana breaches* Preuzeto 16.8.2023. s IOTW: Marriott International suffers latest in series of data breaches (cshub.com)

[39] Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G., Gardner, R. K., *Identifying and Estimating Cybersecurity Rsik for Enterprise Risk Management* Preuzeto 8.7.2023. s Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (nist.gov)

[40] Radziwill, N. M. & Benton, M. C., 2017: Design for X (DfX) in the Internet of Things (IoT). Journal of Quality Management Systems, Applied Engineering, & Technology Management (JoQAT). Vol. 1.

[41] Rapid7 (bez dat.) *What is Cybersecurity Risk Management?* Preuzeto 8.7.2023. s Cybersecurity Risk Management | Rapid7

[42] RiskOptics (2022). *Cyber Risk Prioritization: The what, Why, and How* Preuzeto 18.8.2023. s Cyber Risk Prioritization: The What, Why, and How — RiskOptics (reciprocity.com)

[43] Schauer, S., Stamer, M., Bosse, C., Pavlidis, M., Mouratidis, H., König, S., Papastergiou, S. (2017). *An adaptive supply chain cyber risk management methodology* Preuzeto 7.7.2023. s An adaptive supply chain cyber risk management methodology (econstor.eu)

[44] Schwartz, S. (2021). *Marriott is still covering – and recovering – expenses from its 2018 dana breach* Preuzeto 16.8.2023. s Marriott is still covering — and recovering — expenses from its 2018 data breach | Cybersecurity Dive

[45] Stine, K. Quinn, S. Witte, G. Gardner, R.K. [NIST] (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)* Preuzeto 7.7.2023. s Integrating Cybersecurity and Enterprise Risk Management (ERM) (nist.gov)

[46] Team C. (2021). *What Is a Social Engineering Attack and How Can You Prevent It?* Preuzeto 4.9.2023. s What Is a Social Engineering Attack and How Can You Prevent It? (websitesecuritystore.com)

[47] Trautman, L. J., Ormerod, P. C. (2017). *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things.* Preuzeto 7.7.2023. s https://ssrn.com/abstract=2982629

[48] Tunggal, A.T. (2023). *What is Cybersecurity Risk Managment? Preventing Cyber Attacks* Preuzeto 7.7.2023. s What is Cybersecurity Risk Management? Preventing Cyber Attacks | UpGuard

[49] University of North Dakota [UND] (bez dat.) *Why Cyber Security Is Imortant for Business* Preuzeto 6.7.2023. s Why Cyber Security Is Important for Business - University of North Dakota Online (und.edu)

[50] Vodafone (2017). *Cyber Security Research: The Innovation Accelerator* Preuzeto 6.9.2023. s Cyber Security Research: The Innovation Accelerator (vodafone.com)

[51] WorkSafe (bez dat.) *Focus group guide* Preuzeto 6.9.2023. s Focus Group Guide (worksafe.qld.gov.au)

[52] Young, K. (2021). *Cyber Case Study: Marriott Dana Breach* Preuzeto 18.8.2023. s Cyber Case Study: Marriott Data Breach - CoverLink Insurance - Ohio Insurance Agency

7. Popis slika

8. Popis tablica i grafova