PRIMJENA DIGITALNIH TEHNOLOGIJA I IT REVIZIJE U OTKRIVANJU POSLOVNIH PRIJEVARA

Krnić, Daria

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Analiza i poslovno planiranje

PRIMJENA DIGITALNIH TEHNOLOGIJA I IT REVIZIJE U OTKRIVANJU POSLOVNIH PRIJEVARA

Diplomski rad

Daria Krnić

Zagreb, rujan 2022.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Analiza i poslovno planiranje

PRIMJENA DIGITALNIH TEHNOLOGIJA I IT REVIZIJE U OTKRIVANJU POSLOVNIH PRIJEVARA

APPLICATION OF DIGITAL TECHNOLOGIES AND IT AUDIT IN DETECTING BUSINESS FRAUDS

Diplomski rad

Student: Daria Krnić

JMBAG studenta: 0067568980

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, rujan 2022.

Sažetak

Ciljevi ovog rada su:

1. Objasniti pojam poslovnih prijevara, te istražiti njihove vrste i utjecaj na poslovanje
2. Prikazati metode i vrste digitalnih tehnologija koje uočavaju i sprječavaju poslovne prijevare
3. Istaknuti mehanizme i načine provedbe IT revizije kao važnog alata u otkrivanju i sprječavanju prijevara
4. Analizirati studije slučaja iz poslovne prakse i kritički analizirati primjenu digitalnih tehnologija i IT revizije u otkrivanju i sprječavanju prijevara.

Korištena metodologija se zasniva na prikupljanju sekundarnih podataka, poput knjiga, stručnih članaka i časopisa, te intervjua sa stručnjacima iz promatranog područja.

U radu je u prva tri poglavlja dan teoretski pregled prve tri točke ciljeva rada, s ciljem da upravo teoretska podloga može dati uvid i više znanja za analizu i usporedbu odabranih studija slučaja, te potom kritički zaključak svake od tih studija.

Najvažniji fokus rada je analiza relevantnih studija slučajeva iz poslovne prakse. Korišteni su različiti poslovni slučajevi s ciljem bolje generalizacije za sva poduzeća. Zaključeno je da su poduzeća u većini slučajeva bila meta internog ili eksternog napada zbog nedovoljne implementacija i/ili nedovoljne educiranosti o digitalnom poslovanju.

Ključne riječi: poslovna prijevara, digitalne tehnologije, digitalna ekonomija, IT revizija, otkrivanje poslovnih prijevara

Summary:

Aims of this work are:

1. Explain the concept of business fraud, and investigate their types and impact on business
2. Show the methods and types of digital technologies that detect and prevent business fraud
3. Highlight the mechanisms and ways of implementing IT audit as an important tool in fraud detection and prevention
4. Analyze case studies from business practice and critically analyze the application of digital technologies and IT auditing in fraud detection and prevention.

The methodology used is based on the collection of secondary data, such as books, professional articles and magazines, and interviews with experts in the observed field.

In the first three chapters of the work, a theoretical overview of the first three points of the work's aims is given, with the goal that the theoretical basis can provide insight and more knowledge for the following analysis and comparison of the selected case studies, and then a critical conclusion for each of these studies.

The focus of this work is the fourth point of aims, that is, the analysis of relevant case studies from business practice. Different business cases were used with the goal of better generalization for all companies. Therefore, it was concluded that companies were in most cases the target of an internal or external attack due to insufficient implementation and/or insufficient education about digitalysation.

Key words: business fraud, digital technologies, digital economy, IT audit, business fraud detection

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(vlastoručni potpis studenta)

_____

(mjesto i datum)

Sadržaj

1. Uvod

1.1. Predmet i ciljevi rada

U doba novih tehnologija i svakodnevnog brzorastućeg tržišta, otvara se cijeli novi svijet za prijevare i prevarante. Predmet ovog rada odnosi na pregled razvoja primjene digitalnih tehnologija i IT revizije kao alata otkrivanja i sprječavanja poslovnih prijevara, te identificiranje ključnih obilježja njihove primjene u tom području.
Ciljevi rada su:

1. Objasniti pojam poslovnih prijevara, te istražiti njihove vrste i utjecaj na poslovanje
2. Prikazati metode i vrste digitalnih tehnologija koje uočavaju i sprječavaju poslovne prijevare
3. Istaknuti mehanizme i načine provedbe IT revizije kao važnog alata u otkrivanju i sprječavanju prijevara
4. Analizirati studije slučaja iz poslovne prakse i kritički analizirati primjenu digitalnih tehnologija i IT revizije u otkrivanju i sprječavanju prijevara.

1.2. Metode istraživanja i izvori podataka

U radu će se prikupljati i obrađivati sekundarni podaci iz navedenog područja, poput knjiga, članaka, stručnih radova i intervjua. U radu će se prikazati nekoliko studija slučajeva iz prakse, usporediti njihovi rezultati i kritički analizirati doprinos digitalnih tehnologija i IT revizije u otkrivanju i sprječavanju poslovnih prijevara.

1.3. Sadržaj i struktura rada

Prvi rada dio se odnosi na pregled pojma i objašnjenje vrsta poslovnih prijevara. Iako poslovne prijevare postoje oduvijek, intenzivnom primjenom digitalnih tehnologija u poslovanju postale su učestalije, ali su se pojavile i neke potpuno nove vrste i kategorije. U drugom poglavlju će se objasniti pojam digitalnih tehnologija i primjerima prikazati koristi i prednosti njihove primjene u poslovanju. Obradit će se i mogući problemi, nedostaci i izazovi

primjene digitalnih tehnologija u poslovanju, osobito s aspekta zloporaba i veće izloženosti novim vrstama napada.

S druge strane, digitalne tehnologije se mogu koristiti i kao vrlo učinkovit alat za otkrivanje i sprječavanje poslovnih prijevara. To je osobito prisutno u informatiziranom poslovnom okruženju gdje se podaci o svim poslovnim transakcijama pohranjuju u bazama podataka informacijskog sustava, čime se stvaraju temelji za njihovu brzu analizu i stalnu kontrolu. Podaci o poslovanju koji su pohranjeni u bazama podataka mogu se neprekidno analizirati primjenom različitih digitalnih alata, mogu se odrediti „okidači" sumnjivih transakcija ili zloporaba, što pruža sasvim nove prilike u proaktivnom otkrivanju i sprječavanju poslovnih prijevara. Digitalna tehnologija najčešće brže i točnije detektira prijevaru u usporedbi s čovjekom, uz to je izuzet ljudski faktor subjektivnosti.

U četvrtom poglavlju će se opisati proces unutarnje i vanjske IT revizije i objasniti kako se sustavne i stalne IT revizije mogu koristiti kao alat otkrivanja i sprječavanja prijevara. IT revizijama provjeravamo postoje li odgovarajuće kontrole u (informatiziranom ili digitaliziranom) poslovnom procesu i u kojoj mjeri su te kontrole učinkovite. Najčešće se radi o automatiziranim kontrolama koje su 'ugrađene' u logiku poslovnih procesa, ali i raznim primjerima IT kontrola, tehnoloških kontrola i ostalih vrsta kontrola kojima se osigurava neometano funkcioniranje informacijskog sustava, odnosno poslovnog sustava. Naime, u današnjim poslovnim okruženjima gotovo sve poslovne transakcije se provode automatizmom rada informacijskog sustava, pa je osobito važno stalno provjeravati jesu li sve 'ugrađene' IT kontrole učinkovite, što je upravo najvažniji cilj i zadatak IT revizija.

Na taj način se unutarnje i vanjske IT revizije koriste kao važan alat u praćenju poslovnih događaja koji se pohranjuju u informacijskom sustavu. U ovom poglavlju pobliže će se objasniti Benfordov zakon, kao podloga za kvantitativne preglede koji se tijekom IT revizije koriste u svrhu otkrivanja poslovnih prijevara.

U posljednjem poglavlju rada prikazane su studije slučajeva primjene digitalnih tehnologija i IT revizije, kao alata za uočavanje i sprječavanje poslovnih prijevara. Analizirat će se nekoliko primjera iz poslovne prakse, usporedit će se rezultati i nalazi i diskutirati u kojoj mjeri razvoj tih alata može doprinijeti konceptu kontinuiranog otkrivanja i sprječavanja prijevara i zloporaba. Uz sve pozitivne strane primjene tehnologije u poslovanju, propusti se ipak događaju, pa će studije slučajeva iz prakse omogućiti zaključnu kritičku analizu uzroka i posljedica poslovnih prijevara i uloge digitalnih tehnologija i IT revizije.

2. Poslovne prijevare

2.1. Objašnjenje pojma i vrste poslovnih prijevara

U današnje vrijeme, kada su digitalne mogućnosti neograničene, neograničene su i mogućnosti poslovnih prijevara. Česte su medijske objave o značajnim prijevarama, poput masovnih krađa identiteta ili službenih upozorenja na zlonamjerne poruke. No, svakodnevno su svi korisnici Interneta potencijalna meta prijevare. Ponekad korisnici mogu utjecati na to hoće li biti prevareni, te se prethodno stečenim znanjima i iskustvima zaštititi. U drugu ruku, postoje invazivne prijevare, poput računalnih virusa od kojih se ponekad nemoguće ili vrlo teško zaštititi.[1]

Prijevare nije uvijek jednostavno kategorizirati, jer nerijetko imaju elemente različitih vrsta, no cilj prevaranta je uvijek isti – iznuditi korist od žrtve. Korist ne mora uvijek biti materijalna, već se i prijevarom smatra i instaliranje nepoželjnog *softwarea* npr. onog koji nedopušteno bilježi aktivnost korisnika prikupljajući podatke koji služe za ciljani marketing.[2]

Poslovna prijevara, često se naziva i korporativna prijevara, odnosi se na nezakonite aktivnosti koje poduzima pojedinac ili tvrtka na nepošten ili neetičan način.[3] Često je ova vrsta prijevare osmišljena kako bi se dala korist počinitelju ili tvrtki.[4]

U sljedećem poglavlju su opisane vrste digitalnih poslovnih prijevara poput mrežne krađe identiteta (engl. *phishing*), hakerskih napada i zlonamjernog programskog koda (engl. *malware)* kao i njihove potkategorije.[5]

2.1.1. Mrežna krađa identiteta

Mrežna krađa identiteta (engl. *phishing*, u nastavku će se koristiti pojam *phishing*) je vrsta računalne prijevare s ciljem krađe identiteta. *Phishing* se odnosi na aktivnosti kojima prevaranti i računalni kriminalci slanjem lažnih elektroničkih poruka, koje izgledaju kao da su

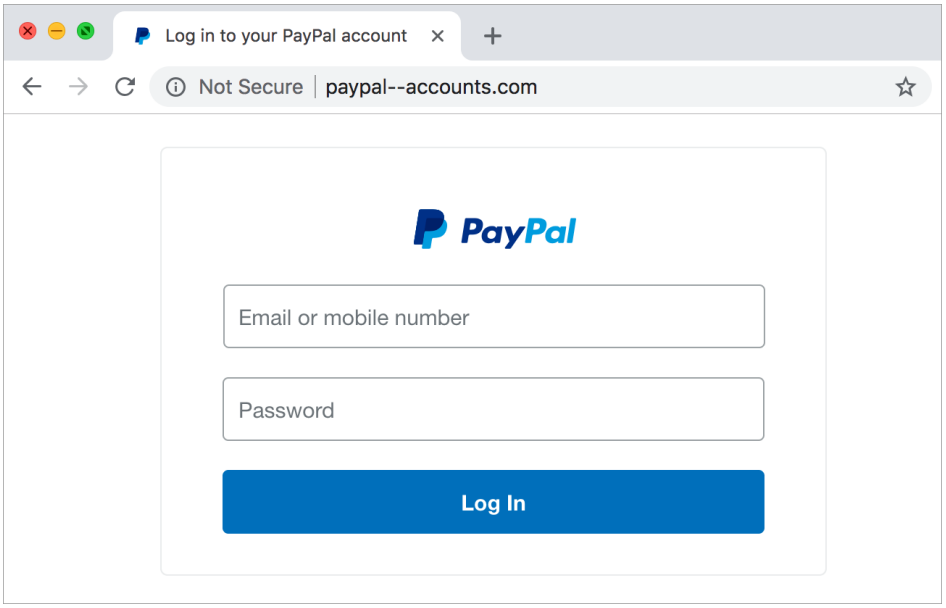
[1] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu.
[2] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu.
[3] Reeves, M. (2022): *Corporate fraud*, https://www.investopedia.com/terms/c/corporate-fraud.asp, pristupljeno 11.7.2022
[4] Reeves, M. (2022): *Corporate fraud*, https://www.investopedia.com/terms/c/corporate-fraud.asp, pristupljeno 11.7.2022
[5] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str. 135

ih poslale izvorne institucije, dobiju pristup povjerljivim korisničkim podacima (primjerice, pristupnih podataka, brojeva i autorizacijskih šifri kreditnih kartica i bankovnih računa) [6].Putem e-maila ili SMS poruke *phisher* mami svoju žrtvu u otkrivanje povjerljivih podataka, poput imena i prezimena, lozinki i broja kartice. Uz *phishing* se često spominje pojam društvenog inženjeringa (engl. *social engineering)* koji iskorištava neznanje, osobito starijih osoba, sa svrhom elektroničke prijevare.[7]

Primjer klasične *phishing* prijevare obično se odvija ovako - haker iz povjerljivih izvora banke krade podatke poput e-mail adrese, imena i prezimena, zatim na prikupljene e-mail adrese šalje e-mail koji na prvi pogled izgleda kao autentična poruka iz banke. U toj elektroničkoj poruci *phisher* obavještava žrtvu da je osvojila nagradu velikog iznosa, te da potvrdi svoj broj kartice. U tim slučajevima se traži CVV/CVC, odnosno broj koji se nalazi na poleđini kartice. Kada žrtva upiše sve svoje podatke, *phisher* ima sve informacije koje su mu potrebne da bi izvršio prijevaru i često krađu novca. Žrtva tek shvaća da je prevarena kada primijeti novac koji nedostaje na računu.[8]

[6] Spremić, M. (2017): Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, str. 49
[7] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:.* International Conference on Computing, Communication and Automation (ICCCA2016).
[8] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:.* International Conference on Computing, Communication and Automation (ICCCA2016).

Slika 1.: Primjer *phishing* stranice[9]



Na gornjoj slici je vidljivo da se *phishing* stranica PayPala na prvi pogled ne razlikuje u usporedbi s originalnom stranicom. S obzirom da je riječ o nijansama, važno je obratiti pažnju na detalje i primijetiti da je URL drukčiji nego što je od prave PayPalove stranice, te se u takvim sitnicama mogu raspoznati *phishing* stranice, što nepažljivom i neinformiranom korisniku može promaknuti.[10]

Postoje četiri vrste *phishinga:* lažiranje e-maila, lažni računi na društvenim mrežama, hakiranje i trojanski konj.[11]

Prijevara lažiranjem e-maila se radi na način da se sroči e-mail u kojem će primatelj pomisliti da se odnosi isključivo na njega, obično od strane neke institucije, poput banke ili telefonskog operatera. Kada primatelj vidi svoje ime i naizgled poznatu e-mail adresu, automatski lakše odaje svoje privatne podatke. Od primanja ovakvih e-mailova se teško zaštititi, ali je moguće povećati oprez pri njihovu otvaranju i davanju osobnih podataka. Sada velik broj e-mail platformi ima već razrađene algoritme za prepoznavanje *phishinga* i na takve poruke automatski upozorava korisnika, odnosno kategorizira ih kao neželjenu poštu.[12]

---

[9] Fox, P. (2020). Phishing attacks, Preuzeto s: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/phishing-attacks Pristupljeno 30.06.2022.

[10] Fox, P. (2020). Phishing attacks, Preuzeto s :https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/phishing-attacks

[11] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:*. International Conference on Computing, Communication and Automation (ICCCA2016).

[12] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:*. International

Kontaktiranje putem lažnih profila se odvija najčešće putem Facebooka, Twittera i LinkedIna. *Phisher* najčešće stavi profilnu sliku atraktivne osobe ili poznatog sportaša. Zatim prevarant šalje poruke ciljanim skupinama preko kojih traži novac, GooglePlay i Amazon bonove i slično. Usprkos činjenici da društvene mreže imaju snažne algoritme u cilju sprječavanja lažnih profila, prevaranti su dosjetljivi i uvijek pronađu način da profil izgleda što autentičnije. Najbolji način sprječavanja takvog *phishinga* je prihvaćanje isključivo osoba koje su poznate iz privatnog života, te je potrebno pojačati oprez kada se radi o dijeljenju hobija (npr. najdražeg nogometnog kluba) i načina života, jer baš takve informacije stvaraju podlogu za napad.[13]

Trojan horse, odnosno trojanski konj je namjerna prijetnja sigurnosnom sustavu. Takav je računalni virus izrađen na način da se naizgled bezopasni kodovi „uvuku" u sistem, te svaki klik mišem rezultira nekom akcijom. Autor virusa ima potpunu kontrolu nad radom računala. Također, trojanski konj funkcionira na način da sa „zaraženog" računala šalje na sve e-mail adrese primatelja link ili datoteku koja sadrži virus, te se na taj način širi – baš kao i pravi virusi. Kako bi se spriječilo dopiranje trojanskog konja na računalo, nužno je koristiti antivirusne programe, kao i povećati oprez pri preuzimanju datoteka s interneta.[14]

Hakerski napadi su malo drukčiji od *phishinga* i trojanskog konja. U lažnim e-mailovima i kontaktiranjem putem lažnih profila se iskorištava naivnost žrtve, dok u hakerskim napadima haker koristi silu. U hakerske napade spadaju korištenje algoritama za otkrivanje lozinki, ulaženje u interne sustave poduzeća s ciljem krađe povjerljivih informacija, neprimjetno instaliranje programa koji pohranjuju privatne podatke i slično. Ponekad ne postoji mogućnost za zaštitu od hakerskih napada, ali uvijek je važno lozinke držati privatnima i ne koristiti najjednostavnije lozinke. Također, potrebno je pojačati oprez pri preuzimanju programa i ekstenzija na računalo, pogotovo ako je riječ o poslovnim računalima na kojem se nalaze povjerljivi i privatni podaci.[15]

Conference on Computing, Communication and Automation (ICCCA2016). str. 538

[13] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:*. International Conference on Computing, Communication and Automation (ICCCA2016). str. 538

[14] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:*. International Conference on Computing, Communication and Automation (ICCCA2016). str. 538

[15] Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:*. International Conference on Computing, Communication and Automation (ICCCA2016). str. 538

2.1.2. Zlonamjerni računalni sustavi

„Zlonamjerni računalni sustavi (engl. *malware*, u nastavku će se koristiti pojam malware) su računalni virusi i ostali zlonamjerni računalni kodovi napisani i distribuirani s namjerom da naprave štetu nad računalnim i ostalim resursima.“[16]

Tri najpoznatije vrste *malware-a* su *adware*, *ransomware* i *spyware*.[17]

Adware, kako samo ime sugerira, su zlonamjerni oglašivači programi, koji nerijetko dolazi kao neželjeni dodatak uz besplatne programe ili kao pop-up prozori s internetskih stranica. Reklame koje dolaze putem *adwarea* uglavnom nude nagrade ili pogodnosti, npr. kupone za maloprodajne lance ili zelenu kartu. Njihov cilj je namamiti korisnika da uđe u stranicu i otkrije osobne podatke.[18]

Računalni crv je podskupina *malware-a*. „Crvi su zlonamjerni programi sastavljeni od samo kopirajućega koda koji omogućava razmnožavanje i širenje crva i tereta i koji skenira mrežu tražeći računalo s odgovarajućim propustom na kojega se može kopirati i replicirati. Ovi virusi su sposobni vrlo brzo usporiti ili srušiti računalnu mrežu ili onemogućiti i usporiti mrežne usluge.“[19]

Ransomware je vrsta računalne ucjene u kojoj se nakon neovlaštenog napada na računalo korisnika kriptiraju svi njegovi podaci.[20] Napadači za povratak podataka traže otkupninu (engl. *ransom*) koja je najčešće u kripto valuti, s obzirom da je preko kripto valute teže ući trag napadaču. Posebno pogodna skupina su poslovni korisnici, odnosno službena računala koja sadrže povjerljive podatke, kao i podatke neophodne za nastavak rada.[21]

Spyware je računalni virus kojem je primarni cilj krađa osobnih podataka. Virus se ponaša kao „špijun“ te pohranjuje korisnikovu aktivnost na računalu, npr. e-mailove, pojmove koje

[16] Spremić, M. (2017). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu., str. 49
[17] Spremić, M. (2017). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu., str. 49
[18] Chien, E. (2005). Techniques of Adware and Spyware. VB2005 Conference.
[19] Spremić, M. (2017). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu.
[20] Spremić, M. (2017). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu., str. 49
[21] Spremić, M. (2020). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu., str 47.

pretražuje, povijest online kupovine... Iz tih podataka, *spyware* može imati razne koristi poput ciljanog oglašavanja i preusmjeravanja na reklamne web stranice.[22]

2.2. Pregled teoretskih okvira koji se koriste u otkrivanju prijevara

2.2.1. Teorija igara

Prvi teoretski okvir koji objašnjava prijevare zasniva se na teoriji igara. Model objašnjava odnos između revizora, vlasnika i menadžera, te sistematično objašnjava kolike su šanse za prijevaru uz određene uvjete. Teorija igara je primjenjiva u raznim poslovnim i životnim situacijama, no ovdje je fokus na revizoru i menadžeru. Ova teorija daje solidan okvir i uvid u razmišljanja revizora i menadžera, te njihovo donošenje odluka koje rezultira uočavanjem i počinjenjem prijevare, što je fokus ovog rada.[23]

Ova teorija igara pretpostavlja da menadžer ima jednu odluku za donijeti, dok revizor ima dvije. Menadžer odlučuje prvi, te je odluka hoće li počiniti prijevaru, te su moguća dva odgovora – da ili ne. Nakon toga je red na revizora, on bez da zna menadžerovu odluku odlučuje hoće li testirati kontrole i koliko detaljno će testirati račune poduzeća. Kao i menadžer, revizor ima dva moguća odgovora, u prvom slučaju su to - da ili ne, a u drugom – manje ili više detaljno. Šanse za otkrivanje prijevare se povećavaju s detaljnosti testiranja.[24]

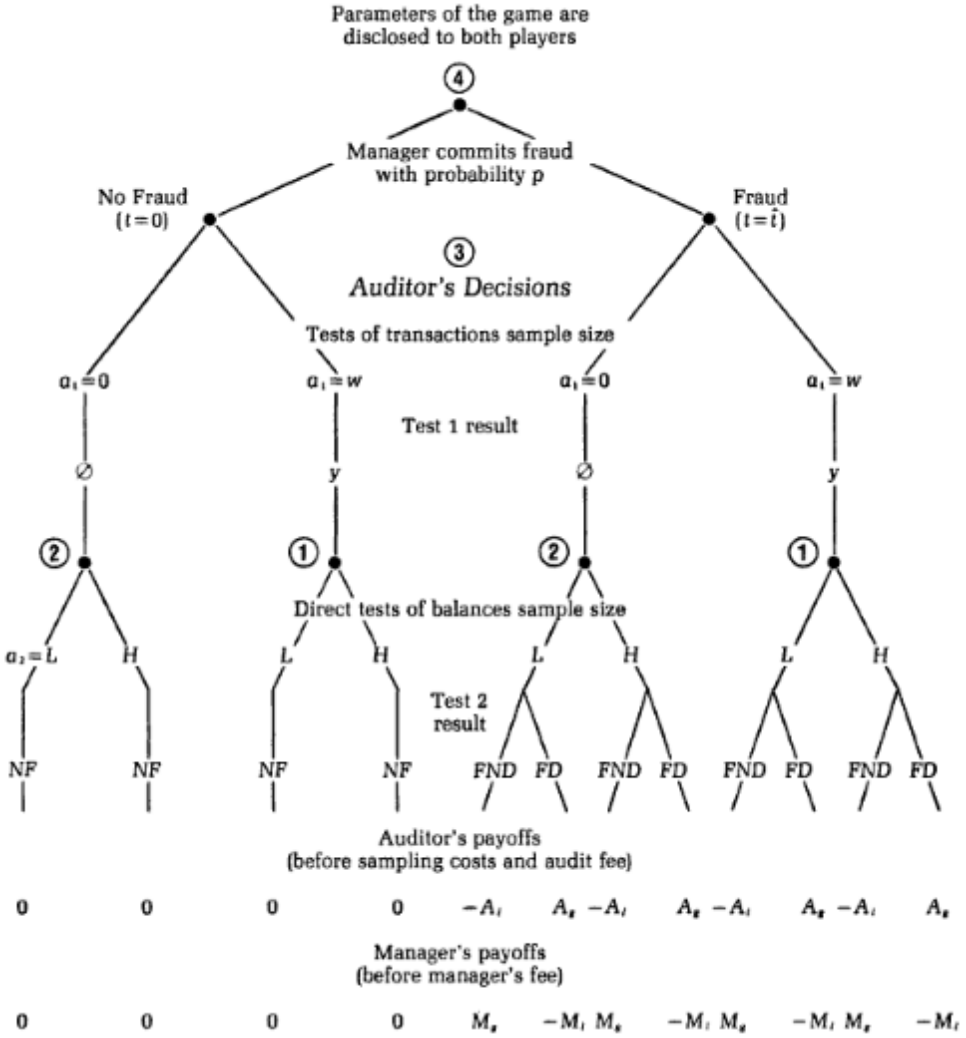
U ovoj teoriji postoje četiri nezavisne varijable. Prva varijabla je kazna koju će revizor morati platiti u slučaju da ne otkrije prijevaru, a da se ona dogodila. Druga varijabla se odnosi na revizorske, odnosno računovodstvene standarde koje je revizor dužan primjenjivati. Treća varijabla je kvaliteta interne kontrole, dok je četvrta varijabla revizorska naknada, koja odražava konkurenciju na revizorskom tržištu. Teorija prikazuje utjecaj četiri nezavisne varijable na testiranje transakcija i računa poduzeća, otkrivanje prijevare i učestalost prijevare.[25]

---

[22] Chien, E. (2005). Techniques of Adware and Spyware. VB2005 Conference.
[23] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str 754
[24] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str 754
[25] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting*

Otkriveno je da što je veća kazna za revizora koji ne otkrije prijevaru, manje su šanse za istu. Također, detaljnijim testiranjem računa poduzeća, manja je potreba za testiranjem transakcija. Uz to, povećanje zahtijevanih testiranja povećava i cijenu revizije i otkrivanje prijevare, dok smanjuje opcionalna testiranja i delegiranje prijevare.[26]

Slika 2.: Dijagram teorije igara u slučaju menadžera i revizora[27]



Izvor: Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782.

Association, 753-782., str 754

[26] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782.

[27] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782.

Razvoj događaja prethodno opisane teorije je prikazan na slici 2.. Na početku, menadžer i revizor imaju jednako znanje o distribuciji slučajnih pogrešaka za tekuću financijsku godinu. Zbog pojednostavljenja modela, pretpostavljamo da su slučajne pogreške normalno distribuirane. Koliko se revizor može osloniti na interne kontrole ovisi o broju slučajnih pogrešaka. Testirajući transakcije, revizor može smanjiti kontrolni rizik i bolje isplanirati testiranje računa poduzeća. U deblu dijagrama je prikazana menadžerova odluka hoće li počiniti prijevaru ili ne. Slijedeći na redu je revizor, on odlučuje hoće li testirati transakcije, bez da zna menadžerov odgovor. U slučaju da revizor ne odluči testirati transakcije, njegov drugi korak je utemeljen na povijest prijevara u poduzeću. Idući korak je odluka hoće li revizor testirati račune poduzeća detaljno ili manje detaljno (H i L na dijagramu). U ovom modelu je otkrivanje prijevare moguće samo drugim testiranjem, odnosno drugom odlukom revizora. U slučaju da revizor odluči testirati detaljnije (H), i dalje vjerojatnost otkrivanja prijevare neće biti 100%. [28]

I menadžer i revizor dobivaju naknadu za obavljeni posao. Što je testiranje detaljnije, revizor od svoje naknade oduzima troškove testiranja. U slučaju da je otkrivena prijevara, revizor dobiva nagradu označenu kao A_g. Nagrada može biti u novcu, ali označava i dobru reputaciju koju revizor stječe otkrivanjem prijevare. U slučaju da ne otkrije prijevaru, postoji mogućnost da će se prijevara otkriti u budućnosti, stoga A_i označava dugoročnu vrijednost u kojoj su sadržani penali koje bi revizor trebao platiti, ali i „cijenu“ loše reputacije.[29]

Menadžer ima drukčije raspoređene dobitke i gubitke. U slučaju da je prijevara uspješno izvedena, odnosno revizor ju nije otkrio, menadžerov dobitak iznosi M_g. U drugu ruku, ako je menadžer otkriven, njegov gubitak, odnosno penali u tom slučaju iznose vrijednost M_i[30].

Ova metoda sažima i kombinira razmišljanja menadžera i revizora u počinjenju i uočavanju prijevare. Teorija igara nudi i kombinira sve moguće opcije, te iskazuje svu nagradu i štetu koju one donose. Stoga se okvirno i može procijeniti i predvidjeti ponašanje dvije uključene strane.[31]

---

[28] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str 754

[29] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str. 757

[30] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str. 757

[31] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782., str. 757

2.2.2. Dempster-Shafer teorija

Dempster-Shafer teorija (u nastavku D-S teorija) je prikladna za otkrivanje prijevara jer uzima u obzir podatke iz nekoliko heterogenih izvora, te uzima u obzir sve dostupne informacije. D-S teorija se često koristi u otkrivanju prijevara preko *Mobile Money Transfer* aplikacija (MMT). MMT su aplikacije koje omogućuju transakcije virtualnim novcem za online plaćanja, prebacivanje novca i općenite svakodnevne transakcije. Kao i sve platforme za transfer novca, i MMT ima rizik od pranja novca i financiranja ilegalnih aktivnosti, poput terorizma.[32]

Fuzija podataka je metoda u kojoj se koristiti nekoliko izvora heterogenih podataka s ciljem unaprjeđenja preciznosti. Ova teorija se smatra okvirom, s obzirom da pokriva teoretski dio, ali nudi i matematičku podlogu za izračune. Uz to, teorija je pogodna za računanje vjerojatnosti prijevara s virtualnim novcem jer gleda širu sliku, uzimajući sve varijable u obzir. Model provjerava navike potrošača, poput prosječnog dnevnog/mjesečnog trošenja i sitnice poput različite adrese dostave i naplate. Fuzija podataka u ovom slučaju se koristi kroz tri komponente: *Rule based filter*, *Dempster-Shafer Combinier* i *Analyser*.[33]

Filtar temeljen na pravilima (*engl*. *rule based filter)* je modul koji kontrolira korisnikove transakcije i dodjeljuje im vjerojatnost da je riječ o prijevari. Ta vjerojatnost se izražava kao vrijednost devijacije od normalnog ponašanja korisnika. Prvo pravilo (R1) je broj koliko je puta je napravljena autentikacija. Što je taj broj veći, veće su i šanse za prijevaru, odnosno da neovlaštena osoba pokušava ući u račun korisnika. Pravilo broj dva (R2) je odgoda pokušaja autentikacije, odnosno vrijeme koje je prošlo između dvije autentikacije. Program određuje svoju granicu, npr. 15 sekundi, te ako je vrijeme između dvije autentikacije duže od 15 sekundi, povećava se vjerojatnost da je riječ o prijevari. Treće pravilo (R3) opaža korisnikove uobičajene transakcije, te obraća pažnju na iznos. Pretpostavlja se da je korisnikova potrošnja normalno distribuirana, te ima svoju standardnu devijaciju. Ovo pravilo računa odstupanje od uobičajenih iznosa, te je ta vrijednost preko Gaussove krivulje izvedena kao vjerojatnost da je

[32] Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., & Romano, L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing*, 754-762., str. 758

[33] Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., & Romano, L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing*, 754-762., str. 758

transakcija prevarantska. U MMT transakcije uglavnom nemaju obilježja prevarantskih, ali D-S teorija pokušava izdvojiti one koje indiciraju prijevaru.[34]

Uloga *Dempster-Shafer Combinera* (DSC) je kombinirati dokaze koji proizlaze iz primjene pravila R1, R2 i R3 i izračunati ukupnu očekivanu vrijednost svake transakcije. Za otkrivanje prijevara u MMT sustavu, D-S teorija dopušta uvođenje alternativnih i eventualno preklapajućih stanja i pravila za izračunavanje razina pouzdanosti povezanih s njima. Da bismo primijenili Dempsterovo pravilo kombinacije, moramo definirati okvir razlučivanja u koji je potrebo uključiti skup međusobno isključivih i iscrpnih mogućnosti. [35]

Analyser je završna faza korištenja ove teorije u svrhu otkrivanja prijevare. Tri vjerojatnosti kombiniraju se korištenjem Dempster-Shaferovog pravila kombinacije i daju vrijednost sumnje u prijevaru (F) ili slučaj da prijevare nema (NF) za svaki pokušaj provjere autentičnosti kao i za svaku transakciju koju su izvršili korisnici. Pretpostavlja se da je F minimalna vjerojatnost da dođe do prijevare dođe. Ako je F > 0, postoji mogućnost da će doći do prijevare. [36]

2.2.3. Trokut prijevare, dijamant prijevare i pentagon prijevare

Trokut prijevare *(engl. fraud triangle)* je teorija koja objašnjava da prijevara ima tri čimbenika. Čimbenici su pritisak, prilika i racionalizacija. Ta tri čimbenika imaju i svoje faktore, na pritisak mogu utjecati financijska stabilnost pojedinca, eksterni pritisak, osobne financijske potrebe i financijski ciljevi. Na priliku utječu kultura u kojoj pojedinac radi, odnosno može počiniti prijevaru, kao i efektivnost praćenja transakcija i organizacijska struktura. Dok na racionalizaciju utječe do koje mjere počinitelj može opravdati svoje postupke.[37]

Dijamant prijevare (engl. fraud diamond) je unaprjeđenje trokuta prijevare. Uz već postojeća tri čimbenika, uvodi se novi - sposobnost. Ova ekstenzija teorije zagovara da će u poduzeću

[34] Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., & Romano, L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing*, 754-762., str. 758

[35] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. *Jurnal Dinamika Akuntansi*, 154-165. str. 156

[36] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. *Jurnal Dinamika Akuntansi*, 154-165., str. 156

[37] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. Jurnal Dinamika Akuntansi, 154-165., str. 156

doći do prijevare ako u njemu postoji određena osoba koja je sposobna izvršiti prijevaru. Faktori koji određuju sposobnost pojedinca da napravi prijevaru su funkcija u organizaciji, kapacitet pojedinca da razumije poslovne procese poput računovodstvenih ili manjkavosti internih kontrola unutar poduzeća, uvjerenje da neće biti uhvaćen na djelu, te mogućnost nošenja sa stresom nakon počinjene prijevare.[38]

Pentagon prijevare *(engl. fraud pentagon)* je unaprijeđena verzija dijamanta prijevare. Uz spomenuta četiri čimbenika, u ovu teoriju se uvodi novi čimbenik - arogancija. S obzirom da je model trokuta prijevare predstavljen 1950-ih godina, Marks (2012) zagovara da se od tad promijenio poslovni model, te da arogancija ipak igra ulogu u počinjenju poslovne prijevare. Prema Marksu (2012) 89% prijevara u poduzeću je izvedeno od strane top-menadžmenta, odnosno izvršnih direktora i direktora financija, dok je u 70% tih slučajeva motiv prijevare bila arogancija, odnosno pohlepa. Predloženo je i pet karakteristika direktora koji će napraviti prijevaru[39]:

1. Osobnost koja ima visok ego i razmišlja da je CEO, odnosno on poznata i slavna osoba.

2. Razmišlja da primjena interne kontrole ne može spriječiti prijevare koje čini.

3. Ponašanje koje često zastrašuje podređene i/ili suradnike.

4. Imaju autokratski stil upravljanja.

5. Imaju strah od gubitka pozicije i/ili statusa koji je postignut.[40]

Opisane teorije same po sebi nisu dostatne za otkrivanje i pravovremeno sprječavanje poslovnih prijevara. No ovi teoretski okviri daju sveobuhvatnu podlogu za algoritme i trendove koji se moderniziraju s brzorastućom digitalizacijom, no teorijska podloga za njihov razvoj ostaje ista. Algoritmi i trendovi u otkrivanju i sprječavanju prijevara će biti obrađeni u narednim poglavljima. [41]

---

[38] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. Jurnal Dinamika Akuntansi, 154-165

[39] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. Jurnal Dinamika Akuntansi, 154-165.

[40] Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. Jurnal Dinamika Akuntansi, 154-165.

[41] Spremić, M. (2017). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet u Zagrebu.

2.3. Primjeri poslovnih prijevara

Poslovne prijevare su svakodnevica, te su često noviteti na tržištu idealna prilika za prijevaru. Brzorastuća tržišta poput bitcoina i NTF često nemaju dobro razrađeni sustav zaštite, dok u drugu ruku postoje starije prijevare poput Ponzijeve scheme i prijevare kreditnim karticama koje su digitalizacijom dobile novo ruho.[42]

2.3.1. Ponzijeva schema

Ponzijeva schema je prevarantski trik koji započinje tako da prevarant osnuje ustanovu za prikupljanje depozita, uglavnom od investitora. Prevarant poziva investitore da deponiraju novac u njegov projekt, uz prinos veći od tržišnog. Kamate se isplaćuju iz novca novih deponenata i samim time investitori ne sumnjaju, tako prevarant ostvaruje kredibilitet i time veći broj investitora. Čitava se schema raspada kad više nema dovoljno novih investitora kojima bi se isplaćivale kamate na stare investicije, te tada obično prevarant bude otkriven.[43]

Ponzijeva shema je doživjela digitalizaciju, odnosno sada se preko Ponzijeve scheme rade prijevare s bitcoinovima. Bitcoin je decentralizirana kripto valuta koja omogućava siguran i neometan prijenos novčanih sredstava, bez opažanja nadležnih tijela. Pojedinci mogu primati i slati bitcoinove, bez otkrivanja svog pravog identiteta. Trenutno investitori nude projekte s visokim prinosom u kojima se udjel plaća bitcoina. Vlasnik projekta isplaćuje visoke prinose iz novca koji dobije od novih investitora. Takav pothvat je održiv se dok postoje novi zainteresirani investitori, te u slučajevima kada je tržište kripto valuta stabilno, no u trenutku kada više nema novih investitora, prevarant je otkriven, te cijela „investicija“ pada u vodu.[44]

Stručnjaci su pokušali razviti sustave za rudarenje podataka koja ručno ili polu-automatizirano pretražuju internet u potrazi za adresama koje su uključene u bitcoin prijevare. Tek nakon ove faze moguće je automatizirati analizu. Međutim, ovi pristupi su

[42] Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *Crypto Valley Conference on Blockchain Technology*, Caligari.
[43] Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *Crypto Valley Conference on Blockchain Technology*, Caligari.
[44] Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *Crypto Valley Conference on Blockchain Technology*, Caligari.

neučinkoviti kada adrese prijevare nisu javno dostupne, npr. jer prevarant privatno komunicira s registriranim korisnicima ili objavljuju samo putem *deepweba* ili *darkweba*. U tim slučajevima bilo bi poželjno da imaju alate koji automatski pretražuju bitcoin *blockchain*, te bilježi sumnjiva ponašanja i identificira adrese povezane s prijevarnim radnjama.[45]

2.3.2. Prijevare s kreditnim karticama

Prijevara je jedan od najvećih izazova u industriji kreditnih kartica. Glavni ciljevi su identificirati različite vrste prijevare s kreditnim karticama i pregledati alternativne tehnike koje su korištene u otkrivanju prijevara. Također važno područje promatranja je predstaviti, usporediti i analizirati nedavno objavljene nalaze i rezultate iz sličnih slučajeva. Ovisno o vrsti prijevare s kojima se susreću banke ili tvrtke za kreditne kartice, mogu se usvojiti i provesti razne mjere. Važnost primjene tehnika borbe protiv prijevare je minimiziranje prijevare s kreditnim karticama. Ipak, još uvijek postoje etički problemi kada se pravi klijenti kreditne kartice pogrešno klasificiraju kao lažni.[46]

Postoje četiri vrste prijevare s kreditnim karticama: bankrot, krađa, prijava s lažnim podacima i bihevioralna prijevara.[47]

Bankrot je vrsta kartičarske prijevare gdje je pojedinac svjestan da nema dovoljan iznos za podmiriti obvezu po dospijeću, odnosno insolventan je. Ovo je jedna od vrsta prijevara koju je najteže za predvidjeti. Pojedinac odlučuje koristiti kreditnu karticu, iako je svjestan da nije solventan. Kada dođe račun za naplatu potrošnje kreditne kartice, pojedinac proglašava osobni bankrot, te banka sama snosi troškove.[48]

---

[45] Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *Crypto Valley Conference on Blockchain Technology*, Caligari.
[46] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[47] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[48] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64

Krađom se kategoriziraju prijevare kada osoba koristi karticu koja ne glasi na njegovo ime. Uglavnom je riječ o fizičkoj krađi gdje prevarant otuđuje karticu, te s njom troši sve dok pojedinac, odnosno banka ne blokira karticu.[49]

Ponekad osobe koji imaju problema sa solventnošću i koji su svjesni da nisu dobar kandidat za posjedovanje kreditne kartice kreiraju prijave za kartice s lažnim podacima. Banke razvijaju algoritme koji traže duplikate, odnosno dvije osobe sa sličnom prijavom. Na primjer, algoritam traži osobe s istim prezimenom i poštanski brojem, te u slučaju da se pronađu duplikati, vjerojatno je riječ o osobi koja nedopušteno koristi dvije kreditne kartice iste banke. [50]

Bihevioralna prijevara je kategorija prijevare gdje su otuđene informacije s legitimnih kartica, te su korištene pri kupnji u online dućanima ili telefonskom prodajom. [51] „Prednost“ ove vrste prijevare je što prevarant ne mora fizički imati karticu da bi počinio prijevaru.[52]

2.3.3. Nezamjenjivi token NFT

Nezamjenjivi token (engl. *Non-fungible token, u nastavku će se koristiti kratica* NFT), je vrsta digitalne imovine u kojoj su pohranjene informacije. S obzirom da je svaki NFT jedinstven, lako je ući u trag vlasniku, te se iznimno lako trguje njima.[53]
U 2021. godini na promet na NFT tržištu je bio preko 23 milijarde USD, dok Morgan Stanley predviđa da će do 2030. promet iznositi čak 240 milijardi dolara. Brzorastuće tržište i trgovanje neopipljivom imovinom otvara brojene prilike za prijevare preko NFT platforma. Postoje dvije vrste prijevara s NFT – krađa i investiranje. Krađa je slična fizičkoj krađi, držatelji NFT imaju svoj virtualni novčanik u kojem pohranjuju raznu imovinu, poput NFT i kripto valuta, te hakiranjem i *malwareom* se može na neovlašten način doći do tuđe imovine.

[49]Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[50] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[51] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[52] Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield., str. 64
[53] Kshetr, N. (2022). Scams, Frauds and Crimes in the Nonfungible Token Market. Greensboro: University of North Carolina.

Druga vrsta je lažno predstavljanje i promoviranje projekata za koje je vlasnik svjestan da se neće izvršiti. Kada vlasnik prikupi dovoljno novca nestaje, te investitori ostaju prevareni.[54]

2.3.4. Pranje novca

Pranje novca je proces čiji je cilj prikrivanje tragova koji vode do stvarnog izvora nezakonito stečenog novca. To je sustav koji se svakim danom razvija – koriste se razne tehnike, a perači novca postaju sofisticiraniji. Kriminalci se skrivaju iza složenih transakcija koje uključuju međunarodne transfere, disperziju na manje iznose ili transfere na račune različitih osoba, mijenjanje oblika novca. Također, perači novca postaju vrlo umreženi, te ih savjetuju bankarski stručnjaci, brokeri, računovođe, odvjetnici…[55]

Pranje novca se uglavnom može prikazati u tri faze: faza ulaganja gdje je novac ostvaren temeljem kriminalnog djelovanja, faza prikrivanja i faza integracije.[56]

Klasični primjer pranja novca može biti – poduzeće registrirano u Hrvatskoj i primarno obavlja djelatnosti u Republici Hrvatskoj dobiva fakturu za usluge iz poduzeća koje je registrirano u *offshore* državi, na primjer Kajmansko otočje. Kada poduzeće plati fakturu, za njega do predstavlja trošak. Na prvi pogled u toj situaciji nije ništa čudno, no ova dva poduzeća su vlasnički povezane. Prednost *offshore* računa je ta što ne postoje restrikcije za podizanje gotovine kao Hrvatskoj, gdje se takve isplate oporezuju.[57]

2.3.5. Napadi unutar poduzeća

Usprkos činjenici da su digitalne prijevare u poduzećima uglavnom povezane s eksternim napadima na poduzeća, napadi unutar poduzeća nisu zanemarivi i ponekad mogu prouzrokovati veće štete. Zaposlenici poduzeća su povijesno sudjelovali u nekima od najvećih prijevara ikada zabilježenih. Zaposlenici su često prvi na udaru kada dolazi do digitalni prijevara, ali su i najveći uzrok popuštanja sigurnosti unutar poduzeća.[58] Prijevare su najčešće motivirane nezadovoljstvom na radnom mjestu, potrebom za novcem i pohlepom. Kao što je već spomenuto, moderniziranjem poslovanja, prijevare su uglavnom računalne. Najčešće

[54] Kshetr, N. (2022). Scams, Frauds and Crimes in the Nonfungible Token Market. Greensboro: University of North Carolina.
[55] Cindori, S. (2007). The Money Laundering Prevention System. *Financial theory and practice*, 59-76., str. 62
[56] Bejaković, P. (1997). Pranje novca. *Financijska praksa*, 461-466.
[57] Cindori, S. (2007). The Money Laundering Prevention System. *Financial theory and practice*, 59-76.
[58] Samonas, S. (2005). *Insider fraud and routine activity theory.* Las Vegas: 12th Annual Security Conference.

prijevare koje zaposlenici u poduzeću rade su krađa osobnih podataka klijenta, mijenjanje ili brisanje informacija u zamjenu za novac, prebacivanje novca s računa firme na svoj račun.[59]

Napadi unutar poduzeća mogu biti značajno veća prijetnja, s obzirom da zaposlenici često točno znaju gdje i što treba tražiti. Također su i puno upućeniji u interne procese i kontrole od hakera. Na primjer, u velikom poduzeću, poput banke ili neke druge depozitarne institucije se svaki dan događa bezbroj transakcija. Naravno, ako prema unutarnjim kontrolama nije ništa sumnjivo, ne provjeravaju se vrijednosti iznad interno dogovorene granice (npr. 10000 kn). Stoga zaposlenici imaju internu informaciju, te shvaćaju da na svoj privatni račun mogu nekoliko puta mjesečno isplaćivati iznos od nekoliko tisuća kuna. [60]

[59] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Westford: Software Engineering Institute.

[60] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Westford: Software Engineering Institute.

3. Primjena digitalnih tehnologija u poslovanju

Kao što je već objašnjeno, digitalne tehnologije u poslovanju u 21. stoljeću nisu više opcija, već imperativ. U prethodnom poglavlju su opisane vrste i dani primjeri poslovnih prijevara. Cilj ovog poglavlja je prikazati prednosti primjena digitalnih tehnologija, te na koji način one služe u otkrivanju i sprječavanju poslovnih prijevara, odnosno kako su implementirane u stvarnom svijetu.[61]

Naravno, primjena digitalnih tehnologija ima svoje prednosti, ali sa sobom nosi i određene rizike koji su detaljno objašnjeni u idućem poglavlju.[62]

3.1. Objašnjenje pojma digitalnih tehnologija

3.1.1. Objašnjenje i vrste digitalnih tehnologija

Da bismo objasnili pojam digitalne tehnologije, važno je objasniti širi pojam – digitalna ekonomija. Pojam digitalna ekonomija je sveobuhvatni pojam digitalizacije već postojećih proizvoda i usluga, kao i poslovanja i tržišta. Temelj digitalne ekonomije je korištenje digitalnih tehnologija u svim aspektima poslovanja i poslovnog procesa.[63]

Konceptualno se digitalna ekonomija sastoji od: integracije i simultane primjene neovisnih tehnologija i njihovih mogućnosti, integraciji progresivnih koncepcija poslovanja, korištenju digitalnih platformi poslovanja, uspješnih digitalnih poslovnih modela i vođenja utemeljenog na poduzetničkoj organizacijskoj kulturi, inovativnosti i stvaranju novih, dodatnih vrijednosti.[64]

Iz koncepcije digitalne ekonomije izveden je koncept digitalne tehnologije. „Digitalne tehnologije su vrlo važan infrastrukturni čimbenik digitalne ekonomije i odnose se na upotrebu digitalnih resursa (tehnologije, alata, aplikacija i algoritama) kojima se učinkovito pronalaze, analiziraju, stvaraju, prosljeđuju i koriste digitalna dobra u računalnom okruženju.“

[61] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str. 20
[62] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str. 20
[63] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu.
[64] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu.

Temeljene digitalne tehnologije možemo razvrstati u šest pod-tehnologija: mobilne tehnologije, društvene mreže, računalstvo u oblacima (engl. *cloud)*, veliki podaci, senzori i Internet stvari (*engl. Internet of things*). U sekundarne digitalne tehnologije pripadaju: 3D printeri, roboti, dronovi, nosive tehnologije, virtualne i proširene stvarnosti i umjetna inteligencija. [65]

Obilježja digitalne tehnologije koja omogućuje stvaranje novih, odnosno inovativnih poslovnih modela su: istodobna primjena svih dostupnih digitalnih tehnologija, ugradnja tehnologija u proizvode i usluge, kao i sposobnost izdvajanja digitalnog sadržaja iz uređaja, zatim analiza i sposobnost brze digitalizacije sadržaja, zaključno s intenzivnom razmjenom digitalnog sadržaja. Posljednje obilježje je sposobnost digitalizacije poslovanja i poslovnih modela, te stvaranje funkcionalnih digitalnih platformi.[66]

Istodobna primjena svih digitalnih tehnologija kombinira primarne i sekundarne podatke međusobno ovisnih i neovisnih digitalnih tehnologija. Takvom kombinacijom je moguće stvoriti nove, dosad neviđene proizvode, usluge i poslovne modele. Primjer takve kombinacije je platforma za online kupovinu ASOS koja kombinira *cloud* u kojem se nalaze svi proizvodi, preko *big data* tehnologije pamti i uči iz ponašanja proizvođača, izrađuje preferencije potrošača i uz sve to koristi online kartično plaćanje.[67]

Ugradnja u proizvode i usluge, sposobnost izdvajanja digitalnog sadržaja iz uređaja, njihova analiza i interakcija je obilježje koje ima sposobnost izdvajati informacije i podatke iz uređaja, te analizirati podatke s ciljem povezivanja i integrirana uređaja, odnosno usluge s okolinom, čineći ga pametnijim i prilagođenijim. Primjer takve digitalizacije poslovanja su samo-poslužni rent-a-bike punktovi koji se nalaze u svim većim gradovima diljem Europe. Takav princip poslovanja simultano kombinira mobilne tehnologije, lokacijske usluge, društvene mreže, te na posljetku online bankarstvo.[68]

Intenzivna razmjena digitalnog sadržaja i interaktivnost obilježava umreženost fizičkih uređaja i resursa. Fizički resursi poput zgrada, postrojenja, automobila, dizala itd., ali i procesi, ljudi i timovi postaju digitalizirani primjenom tehnologija koje očitavaju informacije o njihovome stanju i prosljeđuju te informacije drugim uređajima i svojoj okolini s ciljem unaprjeđenja performansa tih resursa. Primjer intenzivne razmjene digitalnog sadržaja i

[65] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str. 20
[66] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str.20
[67] Spremić, M. (2017): *Digitalna transformacija poslovanja,* Ekonomski fakultet u Zagrebu., str. 20
[68] Spremić, M. (2017). *Digitalna transformacija poslovanja*, Ekonomski fakultet u Zagrebu., str. 20

interaktivnosti su vozila Tesla, koja su digitalizirana do mjere da sama voze, te brojnim senzorima opažaju okolinu, te šalju povratne informacije automobilu, bez ljudskog faktora.[69]

Sposobnost, odnosno mogućnost digitalizacije poslovanja označava digitalizaciju već poznatih poslovnih modela s ciljem unaprjeđivanja već postojećeg modela i samim time stvaranje novih i održivih izvora prihoda. Primjer digitalizacije poslovanje je aplikacije ApplePay koja se nalazi unutar AppleWalleta. Sada više nije potrebno fizički koristiti karticu, već sustavi u mobitelu i POS aparatu prepoznaju digitalnu kreditnu karticu kojom se može beskontaktno plaćati.[70]

3.2. Koristi i izazovi primjene digitalnih tehnologija u poslovanju

3.2.1. Koristi primjene digitalnih tehnologija u poslovanju

Koristi primjene digitalnih tehnologija možemo podijeliti na one mjerljive i nemjerljive. Mjerljive koristi su one koje se mogu kvantificirati, odnosno brojčano izraziti što se u poslovanju povećalo ili smanjilo i za koliko, npr. uštede od automatizacije procesa ili povećanje prihoda od prodaje uslijed povećanja vidljivosti. Preduvjet kvalitetnog mjerenja poslovnih performansi je kontinuirano praćenje svih poslovnih procesa. Nemjerljive koristi digitalizacije poduzeća su kvalitativne, u takve koristi spada npr. poboljšanje imidža i iskustvo korištenja.[71]

Produktivnost je jedna od najznačajnijih koristi za poduzeće koje se digitaliziralo. Odnosi se na poboljšanje performansi ključnih poslovnih procesa.[72]

Poduzeće digitalizacijom stvara vrijednost za krajnje korisnike. Iako poduzeće ponekad neće osjetiti izravno koristi od digitalizacije poslovanja kroz direktno povećanje prihoda, kupci će to uvijek primijetiti i cijeniti. Stoga se dodana vrijednost stvara u formi zadržavanja kupaca, koji će dalje preporučivati poduzeće. Na primjer, dostavljačka služba koja je odlučila uvesti besplatnu uslugu online praćenja pošiljki će imati konkurentsku prednost nad onom koja nema. Stoga se tek kroz razdoblje od nekoliko godina može vidjeti pozitivan pomak.[73]

---

[69] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[70] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[71] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[72] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 55
[73] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 55

Također, jedan od pozitivnih utjecaja digitalizacije poduzeća je povećanja broja kupaca. Maloprodajni lanci koji su postojali u većim gradovima sada su dostupni i u manjima, te se samim time povećava broj kupaca, odnosno korisnika online platforme.[74]

3.2.2. Izazovi primjene digitalnih tehnologija u poslovanju

Usprkos brojnim dobrim stranama digitalizacije poslovanja, digitalizacija sa sobom nosi izazove, koji ne moraju nužno biti negativne strane digitalizacije, ali unose novu dimenziju u poslovanje za koju poduzeće mora biti spremno. Složenom digitalizacijom se stavlja veliki izazov na informatiku.[75]

U digitalnoj transformaciji postoji izazov vodstva koji zahtjeva nove sposobnosti viših rukovoditelja i izvršnih direktora, te prihvaćanje novih vrijednosti kao što su transparentnost informacija, prilagodljivost i otpornost. Postoji tržišni izazov koji će zahtijevat dublje razumijevanje strateških implikacija otkrivanja tržišta i nenamjernog otkrivanja strateškog smjera kroz digitalne poteze. Postoji širi izazov ekosustava koji zahtijeva nove oblike digitalne suradnje, procesa i infrastrukture. Digitalna poslovna strategija je vrlo bitna tematika za vodstvo jer nudi sveprisutnost informacija, te samim time transparentnost postaje imperativ. Ako voditelj na bilo kojoj razini ne razumije kako koristiti digitalne tehnologije i njezine neophodne popratne sastavnice, digitalizacija će predstavljati izazov za poduzeće. Također, ako nisu svjesni utjecaja koji digitalizacija ima na dioničare, kupce, zaposlenike i cjelokupni prodajni lanac, izazov će se pretvoriti u negativnu stranu digitalizacije.[76]

Drugi izazov digitalizacije je to što ona traži stalnu i sveobuhvatnu primjenu napredne tehnologije. U ovom slučaju digitalna tehnologija konstantno mora biti *up to date* s najnovijim trendovima i pronalaziti nove načine kako bi konačnim korisnicima proizvoda ili usluge isporučili najbolji mogući proizvod. Ponekad, takvo održavanje sustava može biti vremenski i financijski iscrpno.[77]

Idući izazov je obilježen očekivanjima koje poslovanje ima prema informatici. U inicijalnim fazama najvažniji kriterij primjene informatike i IT-a u poslovanju je bilo smanjenje troškova

[74] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 55
[75] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, V. (2013). Visions and Voices on Emerging Challenges in Digital Business Strategy. Fox School of Business Research Paper, 1-31.
[76] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, V. (2013). Visions and Voices on Emerging Challenges in Digital Business Strategy. Fox School of Business Research Paper, 1-31.
[77] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

i operativna efikasnost. Dok su kvaliteta, pouzdanost, sigurnost i brzina stvaranja novih rješenja bili su u drugome planu. Danas su svi čimbenici jednako važni, s naglaskom na stvaranju dodatne vrijednosti.[78] U 21. stoljeću informatika više ne služi samo za usklađivanje poslovanja, već je imperativ i na novim, inovativnim poslovnim modelima i stvaranju dodane vrijednosti za poduzeće.[79]

Četvrti izazov je taj što uvođenje digitalizacije podrazumijeva da se IT mora bezuvjetno koristiti kao strateška poslovna funkcija, kojoj sada menadžment treba pridavati značajno više pažnje. Digitalizacija poduzeću može donijeti veću poslovnu vrijednosti, prema literaturi[80] to može biti čak i povećanje prihoda za 40 posto, ali i 20 posto povećanja troškova. Zbog toga je bitno skrenuti posebnu pažnju na IT, te ga početi promatrati kao jednu od najvažnijih poslovnih funkcija.[81]

3.2.3. Rizici primjene digitalnih tehnologija u poslovanju

Uz prednosti i izazove digitalizacije poslovanja, takva transformacija nosi i određene rizike. Poslovnim rizicima su izloženi svi poslovni subjekti, ali na posebnom su udaru oni koji koriste digitalne tehnologije za ostvarenje svojih poslovnih ciljeva. Rizici ne moraju biti samo tehnološke prirode, već je i pogrešna procjena rizika donosi svojevrstan rizik.[82]

Informatički, odnosno digitalni rizici se mogu prikazati kao funkcija imovine, prijetnje i ranjivosti. Imovina se odnosi na imovinu poduzeća, te uključuje imovinu poput materijalne, nematerijalne i financijske. Prijetnjama za poduzeće se smatraju neželjeni događaji, na koje poduzeće može, ali ponekad i ne može reagirati ili predvidjeti. Ranjivost poduzeća uglavnom označava manjkavost sustava u vidu nedovoljne implementacije (učinkovitih) kontrola.[83]

Dvije važne karakteristike poslovnih rizika su to da su uvijek prisutni i da imaju dualnu narav. Informatički rizici su sveprisutni neovisno o tome je li ih poduzeće otkrilo ili ne. Dualna narav poslovnih rizika se odnosi na to da kvalitetno vođene informatičke cjeline stvaraju dodanu vrijednost, poslovne prilike i održivu konkurentnost poduzeća, dok nekvalitetno

[78]Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu, str. 57
[79] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 57
[80] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 57
[81] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 57
[82] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 57
[83] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 57

vođene informatičke cjeline imaju suprotan učinak na poslovanje – ne stvaraju dodanu vrijednost, stvaraju gubitke, te s tim problemima kumuliraju brojne probleme za poduzeće.[84]

Rizici primjene digitalnih tehnologija u poslovanju su sistematizirani u četiri kategorije:

1. **Strateški (korporativni) rizici** – ova vrsta rizika obilježava rizik neusklađenosti poslovanja između poduzeća i informatike. U strateškim rizicima najviše su ugroženi strateški interesi poduzeća, te na najvišoj razini upravljanja mogu prouzročiti veliku štetu i financijske gubitke. Strateški rizici najčešće predstavljaju propust menadžmenta zbog kojih poduzeće ima smanjenu konkurentnost i nemogućnost praćenja trendova digitalnih tehnologija. Primjeri takvog rizika su implementiranje pogrešne strategije informatike, nespremnost na digitalnu transformaciju, rizik da poduzeće ne shvaća prednosti i održivost korištenja digitalnih tehnologija u svom poslovanju.[85]
2. **Rizik provedbe informatičkih programa i projekata** – odnosi se na rizike koji pretpostavljaju da će ulaganja u informatiku biti neispravno vođena, te se dovodi u pitanje efikasnost i učinkovitost ulaganja u digitalizaciju.[86]
3. **Rizici provedbe poslovnih procesa** – obuhvaća sve rizike u svakodnevnom korištenju digitalnih tehnologija u poslovnim procesima. U procjeni ovog rizika, neophodno je uzeti u obzir sve čimbenike koji bi mogli uzurpirati funkcioniranje poslovnih procesa. Primjeri rizika provedbe poslovnih procesa su sigurnosni rizici, rizici provedbe informatičkih usluga, rizik provedbe transakcija, rizik neovlaštenog pristupa sustavu.[87]
4. **Infrastrukturni informatički rizici** – to su rizici koji se odnose na rad informatičke infrastrukture, te opreme kao i ostali rizici koji mogu omesti funkcioniranje informatičke infrastrukture. Takvi rizici su svi oni koji se odnose na dostupnost i funkcionalnost računalne mreže, infrastrukturne podrške i komunikacijske infrastrukture.[88]

Upravljanje (informatičkim) rizicima predstavlja proces poduzeća u kojem se koristi analitički proces u kojem poduzeće otkriva, prepoznaje, umanjuje i nadzire potencijalne rizike. Cilj upravljanja rizicima je identificirati slabosti unutar i van poduzeća, te procijeniti njihovu veličinu. Pravovremena identifikacija i svjesnost okruženja poduzeća

[84] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 139
[85] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 139
[86] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 140
[87] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 140
[88] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 140

mu daju dovoljno vremena za izradu strateškog i kriznog plana, te ako uistinu dođe do realizacije rizika, poduzeće će se puno lakše snaći.[89]

Plan upravljanja rizicima se sastoji od pet koraka:

1. Identifikacija poslovnih rizika
2. Određivanje razine informatičkog rizika procjenjivanjem težine, odnosno utjecaja na poslovanje i imovinu samog poduzeća
3. Određivanje najefikasnijih protumjera spoznanim rizicima postavljanjem informatičkih kontrola
4. Alokacija odgovornosti, provedba i dokumentiranje informatičkih kontrola
5. Konstantan nadzor, konstantno revidiranje planova upravljanja informatičkim rizicima i usklađenje sa strategijom poslovanja poduzeća[90].

3.3. Vrste i trendovi primjene digitalnih tehnologija u uočavanju i sprječavanju poslovnih prijevara

S obzirom da je digitalizacija brzorastuća industrija, ona kao takva zahtjeva ažurna rješenja u svim poljima, tako i u pravovremenom uočavanju i sprječavanju digitalnih poslovnih prijevara.[91]

Trenutni razvoj strojnog učenja i umjetne inteligencije za otkrivanje rizika i prijevare je da tvrtke ulažu više u te tehnologije i da su učinkovitije, ali i skuplje. Prednost inovativnijih tehnologija je što pomaže financijskim institucijama da ranije otkriju rizike i prijevare.[92]

3.3.1. Umjetni imunološki sustav

Poduzeća svakim danim progresivno daju značaj tehnologijama za sprječavanje prijevara i ulažu u njih, osobito iz razloga što je uz današnju dostupnost medija i digitalizacije puno lakše steći loš imidž i reputaciju. Stoga se poduzeća oslanjaju na strojno učenje *(engl. machine learning)* i umjetnu inteligenciju u otkrivanju prijevara. Strojno učenje je metoda za

[89] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 140
[90] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 146
[91] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu
[92] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

uočavanje i sprječavanje poslovnih prijevara. U ovoj metodi algoritmi traže obrasce u velikim bazama podataka, ali puno brže i efikasnije nego što bi čovjek to napravio. S informacijama prikupljenima iz procesa, lako je predviđati ponašanja, što je optimalan alat u uočavanju i sprječavanju poslovnih prijevara.[93]

Rudarenje podataka *(engl. data mining)* je jedna od najraširenijih metoda za uočavanje i sprječavanje poslovnih prijevara. To je proces sortiranja velike količine podataka, s ciljem identifikacije obrazaca i kreiranja veza među obrascima s ciljem rješavanja problema. Uz takvu pomoć je puno lakše predvidjeti sve buduće scenarije.[94]

Jedna od vrsta rudarenja podataka je model umjetnog imunološkog sustava, koji imitiraju ljudski imunološki sustav koji stvara stanice za detektiranje stranih tijela. Kada se stanice razviju antitijela, one će lakše raspoznati strana tijela.[95] Ova vrsta otkrivanja prijevare je česta u otkrivanju prijevara s kreditnim karticama. Kreditne kartice se koriste svakodnevno i najčešće bez loše namjere, te se prema literaturi[96] tek jedna od tisuću kartičnih transakcija smatra prijevarom. Stoga umjetni imunološki sustav ima mogućnost prepoznavanja stranog tijela, odnosno prijevare. Glavni algoritmi umjetnog imunološkog sustava su[97]:

1. Negativna selekcija – svrha negativne selekcije je stvoriti toleranciju na T-stanice, odnosno stanice koje će prepoznati negativne antigene, bez interakcije s „normalnim“ stanicama. Nakon što su generirane T-stanice, one moraju proći kroz negativnu selekciju. T-stanice koje će reagirati, odnosno upozoravati na „normalne“ stanice su odmah uništene. [98]
2. Selekcija kloniranja – u ovom algoritmu se osigurava da se samo stanice koje su prošle negativnu selekciju kloniraju. Stanice mogu biti i prejake – kada će prepoznati i dobre stanice, te preslabe – kada ne raspoznaju ništa. Kada su pronađene poželjne

[93] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[94] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410
[95] Donning, H., Eriksson, M., Martikainen, M., & Lehner, O. M. (2019). Prevention and detection for risk and fraud in the digital age – the current situation. *ACRN Journal of Finance and Risk Perspectives*, 86-97.
[96] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410
[97] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410
[98] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410

stanice, njihov genetski kod je kopiran iz roditeljske stanice. Također, stanice mogu mutirati, odnosno unaprjeđivati svoja svojstva.[99]

Ovaj sistem funkcionira na način da se stvori baza prošlih slučajeva. Ti slučajevi obično imaju opis problema i način na koji je problem bio riješen. Kada dođe do novog problema, u bazi se traže prošli slični slučajevi. Rješenja sličnih slučajeva se testiraju, u slučaju da se ne podudara s već poznatim slučajevima, rješenje se revidira, dok se ne nađe ono optimalno. Također, pozitivna strana ovog modela je to što ima sposobnost predviđanja iz prikupljenih podataka iz prošlosti.[100]

Što se tiče kartičarskih prijevara, model je isti, ali je terminologija drugačija. Inicijalno, izrađuje se baza podataka slučajeva, oni su kategorizirani kao normalna transakcija ili pokušaj prijevare. Za pokušaje prijevare, svaki slučaj je vezanim informacijama uz slučaj, poput informacija o vlasniku kartice, navike potrošnje, uobičajeno vrijeme transakcija... Iz dobivenih informacija, algoritam generira okidače na koje će reagirati u slučaju da se sumnja na prijevaru. Nakon toga, okidači podliježu negativnog selekciji opisanoj iznad. Stanice, odnosno okidači koji su prošli negativnu selekciju se kreću klonirati. Kada se stanice kloniraju, poželjna je mutacija, jer se onda svi mogući okidači kombiniraju, tvoreći najefikasnije i optimalno rješenje. Kada se dogodi transakcija koja je sumnjiva i podliježe testiranju za prijevaru, sličnosti između okidača i baze podataka se računaju, te sistem određuje hoće li signalizirati prijevaru. Kada je prijevara potvrđena, ona se unosi u bazu, te novi slučaj mutira s prijašnjima, stvarajući dodatne kombinacije okidača.[101]

3.3.2. Strojno učenje

Strojno učenje *(engl. Machine learning)* je metoda za uočavanje i sprječavanje poslovnih prijevara. Ovom metodom algoritmi traže obrasce u velikim bazama podataka, ali puno brže i efikasnije nego što bi čovjek to napravio. S informacijama prikupljenima iz procesa, lako je predvidjeti poslovne prijevare. Strojno učenje ima dvije vrste – s nadzorom i bez nadzora. [102]

---

[99] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str 1410

[100] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410

[101] Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics., str. 1410

[102] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th

Strojno učenje s nadzorom se češće koristi, te funkcionira na principu da su dane smjernice i do kojih zaključaka treba doći, te su mogući rezultati već poznati. Učenje bez nadzora umjesto toga identificira složene procese i obrasce bez ikakvih smjernica i ljudske intervencije, što može pomoći u rješavanju problema koje ljudi inače sami ne bi mogli riješiti.[103]

Potporni vektorski stroj *(engl. Support Vector Machine)* se smatra apstraktim strojnim učenjem koji pokušava učiti „vježbajući" na određenom setu podataka, te iz toga pokušava izraditi očekivanje, koje će aplicirati i generalizirati na ostalim podacima. Vektorski stroj je binarni sustav, odnosno ima dva moguća rješenja – prijevara ili nije prijevara. Potporni vektorski stroj se može kategorizirati kao model učenja s nadzorom zajedno s povezanim algoritmima koji se koriste za prepoznavanje uzoraka, analizu podataka, regresijsku analizu i klasifikaciju. Imajući grupu primjera za trening, od kojih svaki pripada zasebnoj kategoriji iz dvije kategorije, algoritam trenira na primjerima kako bi izgradio model koji određuje kojim kategorijama pripadaju novi primjeri.[104]

Drugi algoritam strojnog učenja je stablo odlučivanja, te se u procesu odlučivanja može koristiti kao statistički model. Kao i SVM, on grupira podatke u kategorije i formira dijagram za rezultate, npr. stablo. Stablo se kreće iz korijena prema listovima, te svaki list predstavlja jednu kategoriju. Objekt s primarnom ulogom je u korijenu, dok su kategorije u listovima stabla. Proces klasifikacije je sljedeći[105]:

1. Svi primjeri na kojima je model trenira se pozicioniraju u korijenu stabla
2. Primjeri se distribuiraju s obzirom na njihove atribute
3. Atributi su odabrani koristeći statističke metode
4. Proces se ponavlja dok svi primjeri nisu uspješno klasificirani[106].

Umjetne neuronske mreže je jedan od algoritama u strojnom učenju izveden iz sustava koji postoji u ljudskom mozgu. Ljudski mozak, koji se sastoji od milijun neurona, koristi električne i kemijske signale za komunikaciju, a zatim ih obrađuje. Posebne strukture, poznate

---

International Symposium on Digital Forensics and Security (ISDFS).
[103] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[104] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[105] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[106] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).

kao sinapse, povezuju te neurone, koji omogućuju prolaz signala. Neuronska mreža, kao jedan od algoritama u strojnom učenju, simulira ponašanje 'neurona' iz biološkog sustava, imajući sposobnost prepoznavanja uzoraka, uz korištenje u strojnom učenju tako što ima grupu međusobno povezanih „neurona“ koji radi na ulazu za isporuku izlazne vrijednosti, koji se sastoji od tri sloja. Prvi sloj je *input* sloj – on mora primiti ulazne vrijednosti varijabli s objašnjenjem, jer je najčešće broj čvorova jednak broju eksplanatornih varijabli. Idući je skriveni sloj - jedan ili više slojeva se može formirati u skrivenom sloju i tu se stvarna obrada vrši putem ponderiranog sustava veza. Posljednji je *output* sloj - svi skriveni slojevi povezuju se s *output* slojem, koji generira izlaznu vrijednost na temelju predviđanja varijabli odgovora. U klasifikaciji, izlazni sloj je obično predstavljen jednim čvorom.[107]

3.3.3. Meta učenje

Meta učenje *(engl. meta-learning)* je oblik strojnog učenja koji koristi informacije dobivene rudarenjem podataka ili strojnim učenjem s ciljem povećanja kvalitete rezultata dobivenih u budućim primjenama, koja se također naziva learning-for-learning. Razlikuje se od strojnog učenja jer meta-učenje pruža način učenja o samom procesu, a time i znanje o tome koje značajke i algoritmi se mogu najučinkovitije primijeniti.[108]

Financijske usluge, s naglaskom na banke su shvatile da izmjenom informacija o prijevarama doprinose unificiranom sustavu za prepoznavanje prijevara koji će baratati s puno više informacija.[109]

Najpoznatija metoda meta-učenja je Combiner strategija gdje se atributi i ispravne klasifikacije transakcija kreditne kartice koriste se za obuku višestrukih osnovnih klasifikatora. Predviđanja osnovnih klasifikatora koriste se kao novi atributi za klasifikator meta-razine. Kombinacijom izvornih atributa, predviđanja osnovnog klasifikatora i ispravne klasifikacije za svaku instancu (pravilo sastava), stvara se novi "kombinirani" skup podataka

[107] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[108] Donning, H., Eriksson, M., Martikainen, M., & Lehner, O. M. (2019). Prevention and detection for risk and fraud in the digital age – the current situation. *ACRN Journal of Finance and Risk Perspectives*, 86-97.
[109] Stolfo, S. J., Fan, D. W., Lee, W., & Prodromidi, A. L. (1997). *Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results.* New YorK City: Columbia University.

koji se koristi za obuku za generiranje klasifikatora meta-razine. Predviđanja iz klasifikatora meta razine zatim se koriste kao konačna predviđanja u strategiji kombiniranja.[110]

Prva faza metode meta-učenja sastoji se od osposobljavanja baznih klasifikatora. U meta-učenju, osnovni klasifikatori se konstruiraju primjenom algoritma na 50:50 prijevara ili nije prijevara distribuirani skup podataka za obuku kako bi se postavila očekivanja osnovnog klasifikatora. Skup podataka za obuku podijeljen je u 9 pod skupova koji imaju omjer 50:50 za distribuciju prijevare. Osnovni algoritmi se zatim primjenjuju na podatke 9 pod skupova za generiranje 27 različitih osnovnih klasifikatora (3 algoritma primijenjena na 9 različitih pod skupova). Druga i treća faza procesa meta-učenja koriste skup podataka za provjeru valjanosti za generiranje oba predviđanja osnovnog klasifikatora kao i meta-klasifikator. U drugoj fazi, skup podataka za provjeru valjanosti koristi se kao ulaz za 27 osnovnih klasifikatora za proizvodnju 27 jedinstvenih skupova predviđanja. Ta se predviđanja zatim kombiniraju s izvornim skupom podataka za provjeru valjanosti u trećoj fazi.[111]

Kao što je vidljivo iz ovog poglavlja, za otkrivanje poslovne prijevare nije dovoljno samo uočiti, već koristiti sve dostupne digitalne alate, te ih kombinirati imajući na umu rizike. Optimizacijom svih dostupnih znanja, trendova i algoritama se stvara savršeni alat za otkrivanje i sprječavanje prijevare.[112]

Naravno da poduzeće nije u mogućnost koristiti sve dostupne alate i znanja, no nije ni potrebno koristiti sve, već iskoristiti maksimalno dostupne alate.[113]

[110] Stolfo, S. J., Fan, D. W., Lee, W., & Prodromidi, A. L. (1997). *Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results.* New YorK City: Columbia University.
[111] King-Fung Pun, J. (2011). *Improving Credit Card Fraud Detection using a Meta-Learning Strategy.* Toronto: University of Toronto.
[112] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[113] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

4. Vanjska i unutarnja IT revizija kao mehanizmi otkrivanja i sprječavanja prijevara

U ovom radu je stavljen fokus na algoritme i trendove za uočavanje i sprječavanje prijevara. Kombinacije i modifikacije se često koriste u internim kontrolama, no veliki značaj imaju u unutarnjoj i vanjskoj reviziji informacijskih sustava.[114]

Kvaliteta informacijskih sustava se mjeri kao odstupanje od njegove idealne performanse. Što je odstupanje manje, sustav je kvalitetniji i obrnuto. „Revizija informacijskih sustava (engl. *information system audit*, često će se u nastavku koristiti i pojam IT revizija) je sustavan postupak kojim se ocjenjuje djeluje li informatika u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama.“[115]

Fokus revizije informacijskih sustava je temeljito i ispravno ispitati kontrole unutar svih dijelova informacijskog sustava, dok je cilj procjena zrelosti i razine uspješnosti.[116]

Reviziju informacijskih sustava dijelimo na vanjsku i unutarnju.[117]

4.1. Ciljevi vanjske i unutarnje revizije i metode provedbe

4.1.1. Vanjska IT revizija

Cilj vanjske revizije financijskih izvještaja je pružiti objektivno neovisno ispitivanje i provjeriti daju li financijski izvještaji vjerodostojan prikaz financijskih izvještaja i poštuju li računovodstvene standarde. To ne samo da povećava vrijednost i transparentnost financijskih podataka koje poduzeće prikazuje, što zauzvrat povećava povjerenje korisnika i smanjuje

[114] Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu., str. 39
[115] Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu., str. 39
[116] Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu.
[117] Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu.

rizik ulagača, već neovisna, odnosno vanjska revizija također osigurava veću transparentnost za dioničare, naglašavajući važna područja.[118]

Revizija informacijskih sustava (IT revizija) razlikuje se od revizije financijskih izvještaja. Dok je svrha revizije financijskih izvještaja procijeniti prikazuju li se financijski izvještaji vjerodostojno i ispravno, svrha IT revizije je procjenjivanje internih kontrola unutar poduzeća. To uključuje, ali nije ograničeno na, učinkovitost i sigurnosne protokole, razvojne procese, te IT upravljanje i/ili nadzor istih. Implementacija kontrola u poduzeće je iznimno bitna, ali često nije dovoljna za pružanje odgovarajuće razine sigurnosti. Osobe zadužene za sigurnost informacijskih sustava moraju istražiti jesu li kontrole implementirane ispravno, njihovu učinkovitost i/ili je li došlo do kršenja sigurnosti i u slučaju da jest, koje radnje poduzeće treba poduzeti kako se ne bi to ponovilo. Na ta pitanja trebaju odgovoriti neovisna tijela, što su u ovom slučaju eksterni revizori. Oni su zaduženi za reviziju informacijskih sustava u poduzeću.[119]

Često se IT revizija dijeli na dvije vrste: opći pregled kontrole i revizija kontrolnog pregleda aplikacije. [120]

Suprotno tome, neki IT revizori smatraju da postoje tri temeljne vrste kontrola bez obzira na vrstu revizije koju treba izvršiti, a osobito u području informacijskih tehnologija. Mnogi teoretski okviri i standardi pokušavaju raščlaniti kontrole sustava u još vrsta, poput sigurnosne kontrole, kontrole pristupa i AI kontrole. U nastojanju da se definira što više vrsta uključenih kontrola, na kraju se sve svodi da su te kontrole izvedene iz tri temeljne kontrole, a to su: preventivne kontrole, detektivske kontrole i reaktivne/korektivne kontrole.[121]

4.1.2. Unutarnja IT revizija

Napredak informacijskih i komunikacijskih tehnologija učinio je dostupnim velike količine informacija. Ova dostupnost također stvara značajne rizike za računale sustave, kao i za

---

[118] Hadfield, J. (n.d.). What's the difference between an internal and external audit? Preuzeto 30. Lipanj 2022 iz Menzies: https://www.menzies.co.uk/helping-you/audit-compliance/what-is-an-audit/internal-audit-vs-external-audit/ Pristupljeno 11.07.2022.
[119] Rainter, K. R., & Cegielski, C. G. (2011). *Introduction to information systems.* Danvers: John Wiley & Sons, Inc.
[120] Rainter, K. R., & Cegielski, C. G. (2011). *Introduction to information systems.* Danvers: John Wiley & Sons, Inc.
[121] Rainter, K. R., & Cegielski, C. G. (2011). *Introduction to information systems.* Danvers: John Wiley & Sons, Inc.

informacije i kritične operacije i infrastrukture koje oni podržavaju. Unatoč značajnom napretku u području informacijske sigurnosti, mnogi su informacijski sustavi još uvijek ranjivi na unutarnje ili vanjske napade. Postojanje interne revizije informacijskog sustava povećava vjerojatnost donošenja adekvatnih sigurnosnih mjera i sprječavanja ovih napada, kao i smanjenja negativnih posljedica napada.[122]

Kako bi se poduzeće ispravno i pravovremeno zaštitilo, treba ispravno definirati rizike.[123]

4.2. Primjena IT revizije u otkrivanju i sprječavanju prijevara

4.2.1. Primjena vanjske IT revizije u otkrivanju i sprječavanju prijevara

U sklopu ovog rada je obavljen razgovor sa stručnjakom iz područja vanjske IT revizije. Pri angažiranju vanjske IT revizije, poduzeće koje je subjekt revizije osim zakonske obveze, teži ka poboljšanju svojih informacijskih sustava, koji se značajno odražavaju na sveukupno poslovanje poduzeća.[124]

Također, procesi u vanjskoj IT reviziji se mogu djelomično automatizirati, no donošenje zaključaka, se svodi isključivo na ljudski faktor, odnosno na samog revizora. Revizor temeljem prikupljenih informacija, poslovnog okruženja, rizika, dobrih praksi i profesionalne prosudbe donosi cjelokupni zaključak o efikasnosti IT sustava poduzeća.[125]

4.2.2. Primjena unutarnje IT revizije u otkrivanju i sprječavanju prijevara

Literatura predlaže da da se tri područja računalne aktivnosti trebaju redovito pratiti: kontrola pristupa korisnika, praćenje aktivnosti sustava, i revizijski trag. Ove aktivnosti su zatvorene za osnovne mehanizme za provedbu sigurnosti[126]:

---

[122] Alwashah, A., M., & Al-karabsheh, F. I. (2021). The role of internal and external audit in reducing the risk of accounting information systems (from the estimation of the internal and external auditor). *Journal of Management Information and Decision Sciences*, 1-16.
[123] Rainter, K. R., & Cegielski, C. G. (2011). *Introduction to information systems.* Danvers: John Wiley & Sons, Inc.
[124] Intervju sa stručnjakom iz područja IT revizije (Ivanščak, M.: Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (proveden 5. srpnja 2022., ispitivač D. Krnić)
[125] Intervju sa stručnjakom iz područja IT revizije (Ivanščak, M.: Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (proveden 5. srpnja 2022., ispitivač D. Krnić)
[126] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48.

- provjera autentičnosti principala (Tko je to rekao? ili Tko dobiva te informacije? - ljudi, grupe, strojevi ili programi)
- autoriziranje pristupa (Kome se vjeruje za izvršavanje određenih operacija na ovom objektu?)
- revizija odluka čuvara (Što se dogodilo? i Zašto?)[127]

Cilj sigurnosti u kontroli pristupa korisnika područje je koje želi optimizirati produktivno vrijeme na računalu, smanjiti rizik od pogreške i prijevare, eliminirati neovlašteni pristup i osigurati povjerljivost informacija. Također je očita nužnost trajno pratiti aktivnost sustava jer zlonamjerne radnje sabotaže ili prijevare će se vjerojatnije dogoditi ako su male šanse za otkrivanje. Četiri pitanja koja moraju biti postavljena o vjerojatnim područjima rizika su[128]:

1. Može li ovo dogoditi ovdje?
2. Kako?
3. Jesu li sigurnosne mjere prikladne za uočavanje i sprječavanje prijetnje?
4. Kako možemo poboljšati mjere?[129]

Korištenje učinkovite sigurnosti i kontrola sustava može značajno smanjiti pojavu incidenata i/ili negativne posljedice, s povećanjem mogućnost prevencije i otkrivanja. Još jedna važna sigurnosna radnja je održavanje detaljnih zapisa tko je što učinio i kada i evidencija u slučaju da su zabilježeni pokušaji kršenja sigurnosti. Sve te su informacije vrlo važne za unutarnjeg IT revizora.[130]

4.2.3. Plan vanjske IT revizije

Vanjska revizija informacijskog sustava poduzeća se može sumirati u osam koraka, a to su[131]:

1. Definiranje opsega IT revizije
2. Planiranje potrebnih resursa, te vremenskog plana
3. Održavanje sastanka s ciljem boljeg razumijevanja procesa unutar poduzeća
4. Prikupljanje dokumentacije

[127] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[128] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[129] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[130] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[131] Intervju sa stručnjakom iz područja IT revizije (Ivanščak, M.: Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (proveden 5. srpnja 2022., ispitivač D. Krnić)

5. Testiranje
6. Izrada preporuka i po potrebi nacrta finalnog izvještaja
7. Usklađivanje s klijentom
8. Izrada finalnog izvještaja

Ponekad vanjski IT revizor može biti angažiran samo za reviziju dijelova, odnosno segmenata poslovanja poduzeća. Stoga se koraci mogu modificirati po potrebi, no fokus je na testiranju i izvještavanju, te se ti koraci smatraju najvažnijima.

4.2.4. Plan unutarnje IT revizije

Sigurnosna revizija se sastoji od pet glavnih ciljeva, a to su[132]:

- Provjeriti postojanje sigurnosne politike, standarda, smjernica i procedura
- Identificirati nedostatke i ispitati učinkovitost postojeće politike, standarde, smjernice i procedure
- Identificirati i razumjeti postojeće rizike i ranjive toče poduzeća
- Pregledati postojeće sigurnosne kontrole operativnih, administrativnih i upravljačkih pitanja, i osigurati poštivanje minimalnih sigurnosnih standarda
- Dati preporuke za poboljšanja sustava[133].

Kako bi se osigurala usklađenost sigurnosne politike i odredio minimalni skup kontrola potrebnih za smanjenje rizika na prihvatljivu razinu, revizije sustava treba provoditi povremeno s obzirom da se ranjivosti i prijetnje mijenjaju s vremenom i okolinom. Revizije mogu biti razne, poput revizije novog programa, redovite revizije, nasumične revizije ili revizije izvan radnog vremena. Tehnike koje se koriste u procesu revizije mogu uključivati automatizirane alate za reviziju (gotovi sustavi za reviziju sigurnosti i/ili vlastiti razvijeni alati sigurnosnih revizora) ili mogu postojati tehnike ručnog pregleda (npr. napadi društvenog inženjeringa i kontrolni popisi za reviziju).[134]

Proces revizije može uključivati nekoliko koraka. Predloženo je da se proces unutarnje IT revizije odvija u sedam koraka[135]:

[132] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[133] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[134] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46
[135] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 46

1. skeniranje ranjivosti - skeniranje infrastrukture
2. revizija izvješća - revizija izvješća kao što su zapisnici, izvješća sustava za otkrivanje upada, itd.
3. revizija sigurnosne arhitekture - revizija postojeće sigurnosne arhitekture
4. revizija osnovne linije - revizija sigurnosne postavke kako bi provjeriti je li u skladu sa sigurnosnom osnovom organizacije
5. interna kontrola i revizija tijeka rada - revizija postojećeg tijeka rada
6. revizija politike - revizija sigurnosne politike kako bi se osiguralo da je u skladu s poslovnim ciljem
7. procjena prijetnji/rizika - procjena različitih rizika i prijetnji s kojima se suočavaju informacijski sustavi tvrtke. [136]

Tijekom i sa završetkom procesa revizije može se izraditi niz izvješća poput - izvješće s ranjivostima identificiranim u informacijskom sustavu organizacije, izvješće s prijetnjama i rizicima s kojima se organizacija suočava kao rezultat postojećih ranjivosti uključujući pogrešnu politiku, arhitektura i slično, te revizorsko izvješće koje daje pregled sigurnosti i rezultate svih revizija.[137]

Proces revizije sigurnosti postaje sve teži za poduzimanje s rastućom složenošću informacijskih sustava. Postoje automatizirani alati za reviziju koji značajno olakšavaju postupak.[138]

4.2.5. Odnos između unutarnje i vanjske IT revizije

U IS-u postoje dvije vrste revizora i revizija: unutarnji i vanjski. Revizija informacijskog sustava obično je dio računovodstvene interne revizije, a često je obavljaju korporativni interni revizori. Vanjski revizor provjerava nalaze interne revizije kao i ulaze, obradu i izlaze informacijskih sustava. Eksternu reviziju informacijskih sustava prvenstveno provode certificirani revizori informacijskog sustava, kao što su CISA, certificirana od strane ISACA, udruga za reviziju i kontrolu informacijskih sustava ostale certifikate od strane renomirane organizacije za reviziju IS-a. [139]

[136] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 47
[137] Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 47
[138]Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48., str. 47
[139] Alwashah, A., M., & Al-karabsheh, F. I. (2021). The role of internal and external audit in reducing the risk of

Revizija IS-a razmatra sve potencijalne opasnosti i kontrole u informacijskim sustavima. Usredotočuje se na pitanja kao što su operacije, podaci, integritet, softverske aplikacije, sigurnost, privatnost, proračuni i rashodi, kontrola troškova i produktivnost. Dostupne su smjernice za pomoć revizorima u njihovim poslovima, poput onih iz Udruge za reviziju i kontrolu informacijskih sustava.[140]

U praksi, vanjski IT revizori komuniciraju s internim IT revizorima, u formi čitanja formalnog izvještaja unutarnje IT revizije ili kroz neformalni razgovor. Takav razgovor može biti dobar pokazatelj stanja informacijskog sustava i eventualnih problematičnih područja. No, na temelju provedene unutarnje IT revizije, vanjski revizori ne donose nikakve zaključke, već provode svoje testiranje i cjelokupnu reviziju opisanu iznad, te tek na temelju toga donose svoje zaključke.[141]

Najčešće manjkavosti informacijskih sustava se pronalaze u segmentu upravljanja korisnicima, pod koje spada dodjela pristupa bez formalnog zahtjeva, ne ukidanje pristupa kod zaposlenika koji je dao/ dobio otkaz i postavke lozinki koje nisu u skladu sa sigurnosnim naputcima iz prakse.[142]

4.3. Benfordov zakon

Benfordov zakon je matematičko opažanje koje pokušava predvidjeti vjerojatnost pojave znamenki. Ovaj zakon objašnjava da u mnogim primjerima iz stvarnog života, znamenke prvih devet brojeva nisu jednako raspoređene. Odnosno, da što je broj manji, veća je vjerojatnost da će se pojaviti.[143]

---

accounting information systems (from the estimation of the internal and external auditor). *Journal of Management Information and Decision Sciences*, 1-16.

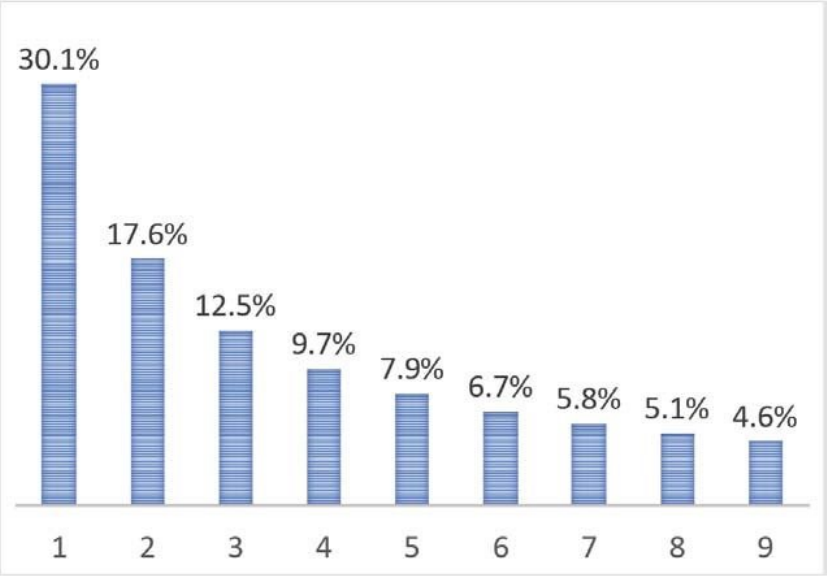
[140] Alwashah, A., M., & Al-karabsheh, F. I. (2021). The role of internal and external audit in reducing the risk of accounting information systems (from the estimation of the internal and external auditor). *Journal of Management Information and Decision Sciences*, 1-16.

[141] Intervju sa stručnjakom iz područja IT revizije (Ivanščak, M.: Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (proveden 5. srpnja 2022., ispitivač D. Krnić)

[142] Intervju sa stručnjakom iz područja IT revizije (Ivanščak, M.: Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (proveden 5. srpnja 2022., ispitivač D. Krnić)

[143] Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas.

Slika 3.: Očekivana distribucija Benfordovog zakona[144]



Na primjer, kada bi se uzeo telefonski imenik, racionalno bi bilo razmišljati da je svaki broj od jedan do devet jednako zastupljen, odnosno negdje oko 11 posto. Prema Benfordovom zakonu su stvari drukčije – on tvrdi da je broj jedan najzastupljeniji s čak više od 30 posto. Provedena su brojna istraživanja koja potvrđuju tu teoriju i na kompleksnijim primjerima od telefonskog imenika.[145]

Benfordov zakon je našao primjenu u raznim područjima, poput nuklearne znanosti, udara gromova, pa čak i aktivnosti Jehovinih svjedoka. U reviziji je Benfordov zakon također pronašao svoj značaj.[146]

Kao što je već spomenuto, za razne setove podataka se očekuje da će imati Benfordovu distribuciju brojeva, uz manja odstupanja. Kada su odstupanja značajnija, to ukazuje na anomaliju, analizom tih anomalija utvrđuje se razlog njihovog nastajanja, koji nerijetko može biti manipulacija podacima. Revizori često testiraju fakture u potraži za duplikatima, često se to radi ručno, što može biti vremenski iscrpljujuće. Benfordov zakon je unaprjeđenje toga, s obzirom da on gleda cijeli račun poduzeća. Samim time ako je odstupanje veće od

[144] Khosravani, A., & Rasinariu, C. (2018). Emergence of Benford's law in music. *Journal of Mathematical Sciences*, 11-24.
[145] Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas., str. 164
[146] Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas., str. 165

procijenjene standardne devijacije, postoji osnovana sumnja da poduzeće manipulira brojevima i transakcijama. [147]

Na primjer, unutarnji revizori zbog olakšanja poslovanja mogu postaviti granicu za testiranje na 1000 kuna. Određene osobe u poduzeću mogu znati tu informaciju, te si na račun isplaćivati 999 kn. U tom slučaju će biti narušena Benfordova distribucija, te će revizor imati osnovanu sumnju za dodatno testiranje transakcija unutar poduzeća.[148]

[147] Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas., str. 165
[148] Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas., str. 165

5. Studije slučaja primjene digitalnih tehnologija i IT revizije u otkrivanju i sprječavanju poslovnih prijevara

5.1. Objašnjenje metodologije studije slučaja

U ovom dijelu rada će se međusobno usporediti značajne studije slučaja poslovnih prijevara, zatim će se međusobno usporediti njihovi konačni rezultati, njihov utjecaj i jačina, te će se u posljednjem poglavlju napraviti kritička analiza uzroka i posljedica prijevara iz studija slučaja. Cilj je obuhvatiti različite vrste prijevara, poput *phishinga*, kartičarskih prijevara, *data leakagea* itd. kako bi se dobio što veći uvid u vrste prijevara u stvarnom svijetu, koje su već opisane u teoretskim poglavljima.[149]

5.2. Analiza studija slučaja iz poslovne prakse

5.2.1. Krađa podataka u maloprodajnom lancu Target

Target spada pod vodeće maloprodajne lance u Sjedinjenim Američkim državama. Prema broju od 350 tisuća zaposlenih, zauzeo je šesto mjesto po broju zaposlenih u SAD-u. S obzirom na veličinu, očekivano je da takvo poduzeće ima besprijekorne digitalne tehnologije i implementirane kontrole.[150]

U prosincu 2013. hakiran je sustav, te je ukradeno čak 40 milijuna brojeva kreditnih kartica, također je ukradeno 70 milijuna adresa, telefonskih brojeva i ostalih osobnih, odnosno povjerljivih podataka. Napad je hakerima bio iznimno olakšan, s obzirom na loše kontrole koje je poduzeće koristilo. Napadači su hakirali poduzeće Fazio Mechanical, koje kontrolira rashladne uređaje u Targetu. Fazio Mechanical je imao pristup Targetovom sustavu jer je online kontroliralo temperature u prodavaonicama. S obzirom na zastarjele sustave u Targetu, napadači su vrlo brzo došli do POS terminala, gdje su instalirali *malware* koji je omogućio krađu podataka s magnetnih traka na POS terminalu. Cijela krađa je trajala nevjerojatnih 18 dana, jedini tko je primijetio da se događa nešto neobično je poduzeće FireEye, koja je instaliralo *anti-malware software*, oni su pravovremeno obavijestili Target, ali oni su se

[149] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[150] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

oglušili na upozorenja. Na posljetku je napad ipak uočen, ali je već bila prouzročena šteta od 300 milijuna dolara i 70 milijuna oštećenih kupaca.[151]

Naknadnom revizijom, otkriveni su propusti poput preslabih lozinki, zastarjeli i nedovoljno odvojeni sustavi, previše osoba s pristupom u sustav i loša enkripcija podataka na POS terminalima.[152]

5.2.2. Wirecard

Wirecard je jedno od najvećih njemačkih poduzeća u području financijske tehnologije, odnosno pružanju digitalnih platformi za financijsku trgovinu. U lipnju 2020. godine, poduzeće je obznanilo da nije solventno, te da je 1.9 milijardi eura, jednostavno nestalo s računa poduzeća. Nedugo nakon toga je uhićen CEO, pod optužbama za manipuliranje tržišta i lažno izvještavanje. Top-management poduzeća je lažno izvještavalo i skrivalo gubitke kako bi povećalo cijenu dionica, te ispunilo očekivanja dioničara i interesnih skupina. U ovom slučaju je velika greška nadzornog odbora, čiji je glavni zadatak bio osigurati da se sve radi u koristi *stakeholdera*. Usprkos tome što su se podizale sumnje, nadzorni odbor nije napravio internu istragu u kojoj se prijevara mogla ranije uočiti. S obzirom da je poduzeće šest godina prije poslovalo sa značajno dobrim rezultatima, koji su se na kraju ispostavili lažnima postavlja se pitanje što se za to vrijeme događalo s revizorima i kako su se uspješno izdavali financijski izvještaji. Kroz devet godina je revizorsko društvo Ernst and Young provodilo reviziju društva, gdje je po njima uglavnom sve bilo uredu, uz manje ispravke u poslovnici u Singapuru. Kada je nakon toga došlo društvo KPMG, oni su nakon godina „uspješne“ revizije otkrili da nešto nije uredu s financijskim izvještajima društva, te da su potvrde o 1.9 milijardi eura u Filipinskim bankama bile lažne.[153]

Primarna uloga vanjskih revizora je zaštita interesa dioničara i evaluacija usklađenosti organizacije s narodnim i međunarodnim propisima i standardima. Revizija financijskih izvješća organizacije povećava transparentnost financijskih izvješća. Vanjski revizori također pomažu olakšati učinkovitiji nadzor procesa financijskog izvješćivanja od strane nadzornog odbora surađujući s internim revizorima. U slučaju Wirecarda, EY nije ispunio svoje dužnosti

[151] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[152] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[153] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.

da zaštiti sve *stakeholdere* i dioničare. EY je izdao nekvalificirane revizije Wirecarda tijekom ovih godina unatoč sve češćim pitanjima o sumnjama na računovodstvene nepravilnosti od strane novinara i *short sellera*. Budući da EY nije proveo odgovarajući revizijski postupak koji je mogao otkriti značajnu prijevaru u Wirecardu između 2016. i 2018., EY se suočava sa zajedničkom tužbom u Njemačkoj koju su pokrenuli investitori Wirecarda.[154]

5.2.3. Crelan Bank

2016. godine napadači su na meti imali banku Crelan u Belgiji. Pomoću *phishing* e-mailova su se predstavili kao osoba iz top-managementa, te su delegirali prijenos novca na razne račune diljem svijeta, koji su prouzročili štetu od 75.8 milijuna dolara. Za razliku od dva primjera objašnjena gore, tijekom unutarnje revizije poduzeća je otkrivena prijevara. Unatoč značajnom gubitku, banka je izvrsno poslovala, te je iz rezervi uspjela povratiti izgubljeni iznos.[155]

Pozitivna komponenta ovog slučaja je to što se cijela prijevara uspjela zadržati samo na razini banke i krajnji korisnici nisu pretrpjeli gubitke.[156]

5.2.4. Bernie Madoff

Bernie Madoff je jedna od najpoznatijih modernih implementacija već opisane Ponzijeve scheme. U konačnici, izvedba je bila poprilično jednostavna. Madoff je napravio račun na kojem je njegova investicijska tvrtka prikupljala sredstva od klijenata i s kojeg je isti novac korišten za plaćanje onih klijenata koji su htjeli likvidirati svoje posjede. Specifična strategija ulaganja koju je plasirao ulagačima bila je *collar*, također poznat kao konverzija *split-strike*. U takvoj strategiji će se pozicija sastojati od vlasništva nad 30 do 35 dionica S&P 100, koje imaju najveću korelaciju s tim indeksom, prodaje *call* opcija na indeks dionica koje nisu u

[154] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.
[155] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022.
[156] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022

novcu i kupnje *put* opcija na dionice koje također nisu u novcu – na taj način se novac stavlja na S&P 100 indeks. [157]

Strategija je omogućila Madoffu da prikrije svoju prijevaru, izbjegne daljnje ispitivanje ulagača i pruži ulagačima i drugim zainteresiranim stranama objašnjenje kako je uspio postizati određene stope povrata dosljedno, godinu za godinom. Ograničivši svoje portfelje samo na dionice s najvećom vrijednošću, Madoff je mogao lako dobiti povijesne podatke o trgovanju kako bi izvršio obrnuti inženjering kojim bi trgovinama njegova tvrtka morala trgovati kako bi postigla navedenu stopu povrata za račune svojih klijenata. S obzirom da je teško procijeniti kada je ova schema započela, teško je i procijeniti koliko su novca izgubili investitori, no procjenjuje se da je riječ o 40 godina i oko 65 milijardi dolara.[158]

5.2.5. First American Financial Corporation

U svibnju, 2019. godine je sigurnosni istraživač Brian Krebs izvijestio o otkriću više od 885 milijuna osjetljivih dokumenata koje je online izložio osiguravajući div First American Financial Corporation. Te datoteke pohranjene na web stranici tvrtke, firstam.com, sadržavale su brojeve bankovnih računa, bankovne izvode, evidenciju hipoteka, porezne dokumente, račune o bankovnim transferima, brojeve socijalnog osiguranja (što je u Hrvatskoj ekvivalentno OIB-u) i fotografije vozačkih dozvola. Sve te informacije, koje datiraju iz 2003. godine, bile su dostupne bez ikakve zaštite i moglo im se pristupiti bez ikakve zaporke - sve dok je osoba znala gdje tražiti, odnosno imala točno tu web adresu. Ovaj slučaj je posebno zanimljiv, s obzirom da se nije dogodio hakerski napad, već je podacima mogao pristupiti bilo tko. Naravno, iako hakeri nisu direktno napravili napad, iskoristili su situaciju i preuzeli više od 885 milijune osjetljivih dokumenata. U ovom slučaju je kreirana poveznica na web-stranicu s osjetljivim informacijama i namijenjena je da je vidi samo određena strana, ali ne postoji metoda za provjeru identiteta osobe koja gleda vezu. Kao rezultat toga, svatko tko otkrije poveznicu na jedan dokument može ga vidjeti—i može otkriti bilo koji drugi dokument smješten na stranici jednostavnom izmjenom veze. Za ovaj slučaj ne postoje

[157] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/
[158] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/

službena izvješća kolika je financijska šteta prouzročena, no iz kvartalnih izvješća je vidljivo da je FAFC drugi kvartal 2019. završila s dobitkom[159].

5.2.6. ComAir

Sustav informacijske tehnologije američke zrakoplovne tvrtke ComAir Inc. 2004. godine, nakon akvizicije od strane Delta Aira Lines Inc. ComAir je bio prisiljen zatvoriti svoje poslovanje na nekoliko dana zbog preopterećenog naslijeđenog sustava upravljanja posadom, kao i sustav za online rezervacije. Naime, za vrijeme gužva na aerodromima u vrijeme Božićnih praznika, sustav je jednostavno prestao raditi. Iz tog razloga je konačni rezultat bio 3.900 otkazanih ili odgođenih letova, gotovo 200.000 putnika koji su propustili let i gubitak od 20 milijuna dolara operativnih troškova. Ne samo da je sustav premašio svoj kapacitet (ComAirov posao je godinama zdravo rastao), također je trpio od dodavanja slojeva i slojeva aplikacija. Ipak ComAirov IT odjel kontinuirano nadograđivao sustav, iz razloga što su korisnici naviknuli na to sučelje. Da stvar bude gora, ova akvizicija je stvorila dodatne komplikacije: stroga ograničenja kapitalnih izdataka i netrpeljivosti između zaposlenika ComAira i njihovih novih vlasnika umanjili su efikasnost IT odjela. Ovaj kombinacija tehnoloških i organizacijskih složenosti stvorila je savršenu priliku za unutarnji kolaps.[160]

5.2.7. Hakiranje automobila Jeep Cherokee

2015. godine hakeri su preuzeli kontrolu nad funkcijama Jeepa s 15 kilometara udaljenosti putem jednostavne 3G veze iskoristivši ranjivost u Uconnectu, sustavu koji kontrolira navigaciju i podrška je u mnogim automobilima. Posljedice su bile ozbiljne. Hakeri su uspjeli preuzeti kontrolu nad kočnicama i upravljačem, zbog čega se automobil zaustavio na autocesti. Ovaj slučaj sugerira da hakiranje automobila ima potencijal izravnije ugroziti živote od drugih kibernetičkih prijetnji, poput internetske krađe osobnih podataka. Naravno, nije uopće potrebno spominjati sigurnosne probleme koje takav hakerski napad uzrokuje. U ovom slučaju je opozvano 1.4 milijuna vozila, kao i troškovi popravljanja šteta, te promjenu

[159] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.
[160] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.

regulatornih i industrijskih pravila. Važno je naglasiti da ovaj tim hakera serijski hakirao vozila, što je zabrinjavajuće s obzirom da se auti koji sam voze smatraju budućnošću.[161]

[161]Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.

5.3. Diskusija i usporedba rezultata studija slučajeva

Tablica 1: Usporedba rezultata studija slučajeva

Varijabla	**Target**	**Wirecard**	**Crelan Bank**	**Bernie Madoff**	**FAFC**	**ComAir**	**Jeep Cherokee**
Vrsta	hakerski napad, instaliranje *malwarea*, krađa podataka	lažiranje računa, lažno izvještavanje	*phishing*	Ponzijeva schema	*data leakage*	nedovoljna veličina IT sustava, s obzirom na obujam poslovanja	hakerski napad
Oštećenik	osobe koje su u Targetu plaćale karticama	Wirecardovi stakeholderi, zaposlenici, vlasnici dionica	Crelan Bank	investitori	osiguranici	korisnici online rezervacija zaposlenici ComAira	Vozači (i Jeep)
Počinitelj	Hakeri	Wirecard, revizori	Hakeri (i Crelan Bank)	Bernie Madoff	FAFC i hakeri	ComAir (Delta AirLines)	hakeri
Prouzročena šteta	40 milijuna brojeva kartica i 70 milijuna osjetljivih podataka	pad cijena dionica, izgubljeno povjerenje korisnika	obzirom da je banka svojom krivicom doživjela prijevaru, te nisu bile uključene treće osobe, šteta je isključivo financijska.	40.000 oštećenika	885 milijuna osjetljivih podatak	3.900 otkazanih letova, 200.000 putnika koji su propustili let	1.4 povučenih automobila
Šteta u novcu	30 milijuna dolara	1.9 milijardi eura	75.8 milijuna dolara	65 milijardi dolara	nepoznato	20 milijuna dolara	nepoznato
Što je poduzeće moglo napraviti da spriječi događaj?	Poduzeće je s obzirom na svoju veličinu trebalo imati bolji sustav sigurnosti Također, sumnja na krađu podataka je bila prijavljena, ali se Target oglušio, te je u takvim slučajevima bolje istražiti uzbunu koja može biti lažna, nego dovesti u mogućnost ovakav događaj.	Poduzeće je svjesno lažno izvještavalo, te se dogodio i značajan propust revizora. Sigurno su postojale osobe koje se nisu slagale s ovakvim načinom poslovanja, stoga je idealno rješenje bilo bolja implementacija unutarnjih kontrola.	Banka je mogla provoditi dvostruku autentikaciju e-mailova, kao i bolju edukaciju zaposlenika vezanu uz *phishing*.	U ovom slučaju je teško reći što je poduzeće moglo napraviti bolje, s obzirom da je svjesno radili prijevaru. Sugestija je da je poduzeće moglo imati bolje interne kontrole od strane top-managementa i nadzornog odbora. Odnosno, menadžeri i stakeholderi su trebali bolje bratiti događaje unutar poduzeća.	FAFC je zakazalo u zaštiti podataka svojih korisnika, što je veliki problem s obzirom da se radi o instituciji koja koristi vrlo povjerljive podatke svojih korisnika. Za financijsku instituciju je ovakva pogreška veliki propust.	Poduzeće je trebalo više ulagati u IT, kao i testirati sustav za situacije poput ove, npr. Božićni praznici.	Industrija koja se bavi vozilima koja mogu sama voziti bi trebala koristiti naprednji *firewall* i općenito naprednije načine za sprječavanje ovakvih vrsta napada.

Izvor: sistematizacija autora

5.3.1. Analiza i usporedba studija slučaja prema oštećeniku i počinitelju

U gornjoj tablici su sažeti već opisani slučajevi iz prethodnog potpoglavlja. Cilj je bio sistematizirati događaje, odnosno studije slučajeva po varijablama, te na taj način uočiti sličnosti i razlike između odabranih slučajeva. S obzirom da su namjerno odabrani slučajevi različitih vrsta, zbog prikaza što više različitih prijevara koje su teoretski obrađene. Stoga su tu hakerski napadi, instaliranje *malwarea*, lažno izvještavanje, *phishing*[162]

Kako su opisane razne prijevare, može se generalizirati da napad ima dvije vrste oštećenika, prvi je kada je poduzeće meta napada, te je ono izloženo i najviše oštećeno, kao i njegovi korisnici, te s druge strane – poduzeće koje direktno i/ili indirektno stvara štetu za svoje korisnike, investitore ili *stakeholdere*. Kao što je vidljivo u tablici, poduzeće je ponekad svrstano kao i oštećenik i počinitelj, s obzirom da je pravilnom upotrebom digitalnih tehnologija i adekvatnim poslovanjem moglo spriječiti ili umanjiti efekte incidenta.[163]

U slučaju Targeta, poduzeće je bilo oštećenik, s obzirom na financijske gubitke koje je hakerski napad prouzrokovao, s druge strane poduzeće se može smatrati i počiniteljem, naravno uz hakere. Target je krivac s obzirom da svojim korisnicima i kupcima nije pružao adekvatnu zaštitu.[164]

Kod Wirecarda je situacija bila slična, samo što je top-management Wirecarda svjesno radio protiv zaposlenika i *stakeholdera*. Također, u ovom slučaju i revizorska kuća Ernst and Young snosi odgovornost, dok je druga revizorska kuća , KPMG ustvari pomogla razotkriti prijevaru. I dalje nije potpuno istraženo jesu li revizori desetak godina bili svjesni događaja u Wirecardu, no u bilo kojem slučaju, revizori nisu ispunili svoje dužnosti, a već je spomenuto da su vanjski revizori zaduženi za transparentnost i kredibilnost financijskih izvještaja.[165]

Belgijska banka Crelan je nasjela na *phishing* e-mailove koji su joj prouzročili značajne financijske gubitke. Banka se može u ovom slučaju smatrati krivcem, uz hakere. Olakotna okolnost za banku je što nije direktno oštetila svoje korisnike, te je sama snosila svoje financijske gubitke. *Phisheri* su na posljetku iznudili veliku sumu novca, ali ju je srećom, banka uspjela povratiti.[166]

---

[162] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[163] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[164] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[165] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.
[166] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help

Bernie Madoff je po većini navoda 40 godina provodio svoju Ponzijevu schemu iza koje je načelno stajao on, oštetio je tisuće ljudi, dok je sebi, svojoj kompaniji i suradnicima narušio uzgled.[167]

First American Financial Corporation je značajno oštetila svoje osiguranike, te je glavni krivac upravo korporacija. Ovaj slučaj se niti ne može nazvati hakiranjem, s obzirom da je pristup web-stranici imao svatko. Naravno, neovlašteno preuzimanje je kažnjivo, ali je svima bilo dostupno.[168]

U slučaju ComAira, poduzeće nije pretrpjelo nikakav vanjski napad, ali je svojim načinom poslovanja značajno oštetio svoje putnike i korisnike.[169]

Hakiranje Jeepa je možda najrizičnija od prikazanih studija slučaja, s obzirom da su bili ugroženi ljudski životi. Kao i u već nekim spomenutim slučajevima, haker je glavni krivac, ali u ovakvoj vrsti industrije, gdje se radi o ljudskim životima, *firewallovi* bi trebali biti neprobojni, te puno bolje zaštićeni od hakerskih napada.[170]

Analizom i usporedbom je vidljivo da u slučajevima hakerskih napada ili prijevara od strane trećih osoba, često poduzeće primjenjuje loše poslovne prakse i nedovoljno brine o opasnostima digitalnog doba. Poduzeća se mogu smatrati supočiniteljima, pogotovo jer svojom poslovnom praksom otvaraju put za prijevare, te su krajnji korisnici kolateralne žrtve napada na poduzeće. S druge strane, iz primjera možemo vidjeti da su nerijetko i poduzeća oštećena.[171] Također, nerijetko su opet njihove kontrole i digitalizacija, kao i korištenje, odnosno ne korištenje istih upravo razlog zašto predstavljaju dobrog kandidata za prijevaru i napad. U prikazanim studijama slučaja, prave žrtve su „obični ljudi“ koji su npr. u slučaju Targeta[172] samo počini transakciju na njihovom POS-u, ili u slučaju FAFC-a koristili usluge osiguranja.[173]Ljudi nisu velike korporacije, i naravno da nemaju znanja i ne koriste kontrole kao poduzeća. Iz tog razloga bi poduzeća trebala pružiti zaštitu svojim korisnicima.[174]

Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022.

[167] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/ Pristupljeno 12.07.2022

[168] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.

[169] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.

[170] Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.

[171] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

[172] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

[173] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It*

5.3.2. Analiza i usporedba studija slučaja prema šteti

U tablici je učinjena šteta podijeljena u dvije kategorije. Prva vrsta štete je iskazana kao kvantitativna varijabla, ali ne u novcu, već u šteti koja se odnosi na krađu osobnih podataka i slično, koja je najviše pogađala korisnike. Druga kategorija štete je financijska šteta, koja više pogodila poduzeća, s obzirom da su oni patili od direktne krađe, kao i od kasnije plaćenih penala. Teško je odrediti koja je od ove dvije vrste šteta „veća" obzirom da je to subjektivno, jer ne vrijedi svakome jednako 40 milijuna brojeva kartica i 30 milijuna dolara.[175]

U Targetovoj krađi brojeva kartica i osobnih podataka, ukradeno je oko 40 milijuna brojeva kartica i 70 milijuna osjetljivih podataka, dok je šteta za Target iznosila 30 milijuna dolara, u plaćenim troškovima, kao i implementaciji novih sustava i kontrola.[176]

Wirecard je nakon otkrivene prijevare za početak izgubio povjerenje svih investitora i *stakeholdera,* što se odrazilo i na pad cijena dionica s oko 100 dolara na tek nekoliko dolara, dok danas (30. lipnja, 2022.) iznosi samo 0.0045 dolara. S druge strane, prouzročena šteta je 1.9 milijardi eura, što nikako nije zanemarivo.[177]

Crelan Bank je svojom greškom, prouzročila velike gubitke kada su nasjeli na *phishinga* prijevaru. Srećom, nisu bili otkriveni nikakvi podaci korisnika usluga banke. Stoga je u ovom slučaju, jedina i najveća šteta 75.8 milijuna eura koje je banka prebacila na račun *phishera*.[178]

Bernie Madoff je kroz 40 godina provodio svoju modernu verziju Ponzijeve scheme. Teško je procijeniti ukupnu štetu, ali procjenjuje se da je Madoff prevario 40.000 ljudi, za oko 65 milijardi dolara. S tolikom financijskom štetom, ovo je najveća prijevara od promatranih studija slučajeva, ali također i jedna od najpoznatijih u svijetu.[179]

Happen And What Does It Mean? Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.

[174] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135

[175] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135

[176] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135

[177] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.

[178] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022.

[179] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.

Financijska šteta koja je zadesila FAFC nije iskazana, no 885 milijuna osobnih podataka se može smatrati značajnom štetom.[180]

U slučaju aviokompanije ComAir, može se istaknuti velika šteta lošeg publiciteta, koji je u takvoj industriji iznimno važan. Kod avioprijevoznika jedna nepravilnost ili incident mogu rezultirati u velikim gubitcima, pa čak i propadanjem kompanije. U jednom danu je ComAir otkazao 3.900 letova, uz to se zbog njihove greške 300.000 ljudi nije ukrcalo na svoj let. Uz to, naknadno su nastali troškovi modernizacije digitalnog sustava online rezervacija. Usprkos tome, da se s ComAir uspješno oporavio nakon ove situacije, splet drugih okolnosti je zaključio njegovo poslovanje.[181]

Hakiranje samo-vozećeg automobila Jeep bi se moglo izdvojiti kao potencijalno najopasnije, s obzirom da su ostale prijevare i napadati rezultirali ukradenim novcem ili podacima, ovdje se ipak radilo o ljudskim životima. Jeep je na vrijeme shvatio probleme s automobilima koji su ga snašli, te je na svoju štetu povukao 1.4 milijuna vozila iz prodaje i onih koji su već bili na cestama. Pravi iznos financijske štete je nedostupan, ali s obzirom da je riječ o industriji pametnih automobila, može se pretpostaviti da je riječ o milijardama.[182]

Teško je kvantificirati ovakve štete, s obzirom da nisu sve izražene u novcu, te je takve efekte teško kategorizirati. Također, u kategoriji izgubljenih podataka, veću težinu ima broj kreditne kartice, nego samo ime i prezime.[183] U drugu ruku, financijski gubici se lakše uspoređuju, i najznačajnija financijska šteta od promatranih slučajeva je u slučaju Bernie Madoff, gdje su investitori oštećeni za ukupno 65 milijardi dolara.[184]

5.3.3. Analiza i usporedba studija slučaja prema reakciji poduzeća

U studiji slučaja u Targetu je vrlo jasno da maloprodajni lanac nije reagirao pravovremeno, već tek nakon 18 dana kada su ukradeni milijuni podataka. S druge strane, ova pogreška je

[180] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.
[181] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.
[182] Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.
[183] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[184] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/

imala pozitivan utjecaj na dodatnu digitalizaciju Targeta, te su nakon tog implementirali nove kontrole i unaprijedili zaštitu svog sustava.[185]

Wirecardov top-management nije trebao biti iznenađen kada su prijevare otkrivene, s obzirom da su oni svjesno lažno izvještavali. S druge strane, nakon incidenta s Wirecardom su revizorske kuće odlučile obratiti posebnu pozornost na testiranje bankovnih izvoda i transakcija, kao i konfirmacija banaka.[186]

Nepoznato je što je banka Crelan napravila po otkriću prijevare, s obzirom da je riječ o depozitarnoj instituciji. No pretragom dostupnih izvora je vidljivo da se nikakav incident nije ponovio, stoga se može zaključiti da je CB ipak poradila na kontrolama i zaštiti podataka.[187]

U slučaju Bernie Madoff je jedini logični slijed događaja bio da se poduzeće zatvori, te je na posljetku i Madoff osuđen na 150 godina zatvora. Dobra strana svega je to što su kroz suđenje, oštećenici uspjeli povratiti dio svog novca.[188]

First American Financial Corporation je poslije vlastitog propusta instalirala odgovarajuću autentikaciju i zaštitila svoju stranicu, samim time i podatke svojih korisnika. Problem je što je velika šteta već počinjena i *social security number* (ekvivalentno OIB-u) nije lako promijeniti kao što je deaktivirati ukradenu kreditnu karticu.[189]

ComAir je jedna od promatranih kopanija koja je na posljetku propala. Ovaj incident nije prethodio tome, ali ukazuje na loše poslovanje ovog avioprijevoznika. Naravno, poslije pada sustava online rezervacija, ComAir je unaprijedio i modernizirao svoj sustav. Ipak, tržište avioprijevoznika je specifično i može se karakterizirati kao mješavina oligopola i nesavršene konkurencije, stoga je jedna pogreška, odnosno ovakav incident dovoljan da se putnici priklone drugom prijevozniku.[190]

---

[185] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[186] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.
[187] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022.
[188] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/ Pristupljeno 12.07.2022.
[189] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.
[190] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.

Hakiranje samo-vozećeg automobila Jeep Cherokee je primjer odgovornog ponašanja nakon ovakvog napada. Poslije je Jeep odlučio povući sve automobile tada napravljene, stavljajući veliki trošak na sebe, ali time pokazujući da je zadovoljstvo i sigurnost imperativ tog poduzeća.[191]

5.4. Kritička analiza uzroka i posljedica poslovnih prijevara

Kada bi se sagledale promatrane studije slučaja i pokušale generalizirati, može se pretpostaviti da je glavni uzrok svih studija slučaja bila nepažnja i nepripremljenost. Naravno razlozi su puno širi i dublji od navedenih i treba ih sve kritički sagledati.[192]

Target je u ovom slučaju napada pokazao da umreženost informacijskih sustava nije uvijek pozitivna stvar. S obzirom da su hakeri prvo izvršili napad na poduzeće koje je kontroliralo klima-uređaje u trgovinama, zatim preko njihovog sustava došli do POS aparata. Naknadnim testiranjem kontrola, revizori su došli do zaključka da se čak može hakirati i POS aparat kroz vagu za voće i povrće. Primarna greška, odnosno propust Targeta je bio to što je sustav bio „previše umrežen“, odnosno za prelaženje iz jednog sektora poslovanja u drugo je bila premala zaštita, što je znatno olakšalo proces hakiranja. S druge strane, problematično je to što je poduzeće ignoriralo upozorenja da je moguća prijevara u tijeku. Takva upozorenja i ako se ispostave lažna, imaju puno manje posljedice i štetu, nego kad se ona prava ignoriraju. Kritički gledano, poduzeću se dogodio ovakav napad zbog nedovoljnih kontrola i prevelike lakoće prelaženja između sustava poduzeća. Posljedica za Target je bila nepovratno izgubljeno povjerenje kupaca, kao i veliki financijski gubici. Usprkos tome, Target se uspješno oporavio iz krize, te nastavio s uspješnim poslovanjem.[193]

Wirecard je jedna od najpoznatijih prijevara u 2020. godini. Problematika Wirecarda je bila nedovoljna, odnosno lažna transparentnost. Wirecardov top-management je činio prijevare, koje revizori nisu pravodobno primjećivali, te postoji mogućnost da su ih svjesno ignorirali. Nije potrebno objašnjavati zašto su prijevare loše i da ih poduzeća ne bi trebala raditi, ali u ovom slučaju se stavlja pod upitnik i kredibilitet revizora koji je provodio reviziju. Nakon dugog niza godina, revizori se mogu ulijeniti i misle da im više ništa ne može promaknuti, stoga ta kombinacija nepažnje i samouvjerenosti može napraviti velike probleme. Zakon

[191] Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.
[192] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135
[193] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu., str. 135

Republike Hrvatske nalaže da se revizor mijenja svakih sedam godina.[194] Takav zakon je sastavljen u cilju da zaštiti poduzeće, *stakeholdere* i ostale interesne skupine, kao i da poveća transparentnost. Vidljivo je da kada je Wirecard angažirao još jedno revizorsko društvo, prijevara je bila otkrivena. Posljedica ovog na otkrivanje i sprječavanje prijevara je što se stavio dodatan naglasak na testiranje transakcija i računa poduzeća.[195]

Belgijska banka Crelan je svojom pogreškom, izgubila svoj novac. Što se u moru prikazanih studija slučajeva čini i najbezazlenije. Srećom, Banka nije kompromitirala podatke svojih korisnika, koji su iznimno osjetljivi, s obzirom da je riječ o depozitarnoj instituciji. Kritički gledano, institucija poput banke, trebala bi imati jače *antiphishing* mehanizme implementirane u e-mail sustave.[196] Ovaj put nisu odane povjerljive informacije klijenata, no *phisheri* i hakeri svakodnevno smišljaju nove načine i prijevare. Također, da je poduzeće imalo dvostruku autentikaciju, odnosno da dvije osobe delegiraju prebacivanje novca ili dvije osobe unose PIN za pristup računu, šansa za napad i prijevaru bi bila smanjena. Različiti poslužitelji e-maila koriste različite metode za analiziranje primljene e-maila. To se postiže ili usporedbom s već pohranjenim podacima u bazi podataka za otkrivanje neželjene pošte ili odabirom specifičnih značajki. Najnovije implementirane metode su *Random Forest*, neuronske mreže, *Naive Bayes* i Vektorski strojevi za klasifikaciju.[197]

Bernie Madoff je slučaj koji iskače od ostalih promatranih studija slučaja s obzirom da je on sam provodio Ponzijevu schemu, dok su njegovi zaposlenici mislili da pomažu u stvarnom investicijskom poslu. Uvriježeno je mišljenje da ako su stope povrata na investiciju prevelike, sluti na prijevaru. Madoff je svoje stope držao u normalnim raznima, stoga nitko nije posumnjao čak 40 godina. On nije nikome dopuštao pristup financijama poduzeća, stoga nije bilo puno prilika za pravovremenu detekciju prijevare. S obzirom da je Madoff počeo s prijevara 70-ih godina prošlog stoljeća, sustavi, a pogotovo oni digitalni nisu bili toliko razvijeni. Stoga je naivno za očekivati da bi u to doba digitalne tehnologije i implementacija digitalnih kontrola pomogle, odnosno da su uopće bile prisutne u opsegu u kojem ih poznajemo danas. S druge strane, danas bi poduzeća trebala imati implementirane kontrole,

[194] *Zakon o reviziji*. (1. Siječanj 2018). Dohvaćeno iz Zakon.hr: https://www.zakon.hr/z/417/Zakon-o-reviziji Pristupljeno 13.07.2022.
[195] Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.
[196] Zorz, Z. (26. Siječanj 2016). *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ Pristupljeno 12.07.2022.
[197] Ssebulime, T. (2022). *Email Classification Using Machine Learning Techniques.* Bournemouth: Faculty of Science and Technology Bournemouth University.

kao i eksternu reviziju. S boljim regulacijama i modernijim sustavima, ovakva prijevara bi se sigurno puno brže otkrila. Kao što je već naglašeno, većinu prijevara digitalizacija ne iskorjenjuje, već joj daje novo ruho. Posljedice Ponzijevih schema mogu biti razne, s obzirom da prvi ulagači ipak ostvaruju velike prinose, dok zadnji koji ulaze u schemu imaju velike gubitke.[198]

Za razliku od ostalih prikazanih slučajeva, u slučaju First American Financial Corporation je teže uspostaviti uzročno-posljedičnu vezu s obzirom da su kroz godine bili dostupni podaci osiguranika, te se s brojem osobnih podataka od čak 885 milijuna moglo manipulirati na razne načine. S vrstom podataka poput imena i prezimena, broja kartice, detalja o hipoteci i *social security numberom* se može vrlo lako manipulirati, te su mogućnosti za izvršenje prijevare beskonačne. S ovakvim podacima se mogu napraviti i „bezazleni" lažni profili na društvenim mrežama, ali i puno opasnije podizanje kredita.[199]

ComAir je pod akvizijom DeltaAirlinesa doživio vrlo turbulentno razdoblje. Naravno da DeltaAirlines nije kriv za to, već nespremnost ComAira da se prilagodi tržištu koje se digitalizira i modernizira, te samim time ima nove izazove. ComAir usprkos povećanoj digitalizaciji nije bio spreman nadograđivati svoj sustav za online rezervacije, zbog toga što nije želio zbunjivati svoje putnike. Kao što je već objašnjeno u teorijskom dijelu, sustave je važno gotovo svakodnevno testirati i po potrebi mijenjati. Da je poduzeće pravovremeno testiralo situacije preopterećenosti sustava, na vrijeme bi uočilo probleme te izmijenilo svoj sustav i prilagodio ga većem obujmu poslovanja, kao što je ovdje bio slučaj – na Božić. Posljedica svega je bilo što je ComAir 2022. godine prestao letjeti. Pad sistema tog Božića nije bio razlog propasti poduzeća, ali taj incident pokazuje poslovnu etiku ComAira, odnosno zastarjelost sistema i kako tržište tretira takva poduzeća.[200]

Kao što je već spomenuto, situacija s automobilom Jeep Cherokee je imala potencijalne najveće posljedice, s obzirom da su hakeri manipulirali s ljudskim životima. Industrija pametnih automobila bi svakako trebala imati jače razvijene kontrole i bolji *firewall.* Evidentno je da se radi o iskusnim hakerima koji su hakirali nekoliko vrsta automobila. No, s

---

[198] *Bernie Madoff's Ponzi Scheme*. (21. rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/

[199] Dellinger, A. (26. Svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f Pristupljeno 12.07.2022.

[200] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.

obzirom da je riječ o vrlo ozbiljnom slučaju, i najmanja pogreška može biti kobna. Posljedice ipak nisu bile kobne kao što su mogle biti, no poslije ovakvih incidenata povećane su kontrole i testiranje ovakve vrste automobila.[201]

[201] Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.

6. Zaključak

U modernom dobu, odnosno 21. stoljeću kada su digitalni trendovi na najvišoj razini, mnoge svakodnevne aktivnosti su olakšane i digitalizirane, poput odlaska u trgovinu. S druge strane, ta razina digitalizacije stvara savršeni teren za svakodnevne prijevare, s obzirom da je potencijalna žrtva prijevare svaki korisnik interneta.[202]

Imperativ digitalizacije je učenje iz grešaka i težnja najefikasnijem i optimalnom sustavu. Stoga se implementiraju kontrole, revizije računalnih sustava i razni algoritmi koji ga unaprjeđuju.[203]

Prijevare mogu biti razne, ciljane i neciljane, s ciljem iznuđivanja novca ili informacija ili čak iz čiste zlobe. Pregledane su glavne vrste prijevara digitalnog doba, poput *phishinga*, prijevara kreditnim karticama, Ponzijeva schema, *malware*[204] Kao i algoritmi i sustavi koji se svakodnevno koriste u otkrivanju i sprječavanju istih. Neki od alata su modernizirana teorija igara[205] ili umjetni imunološki sustavi, takvi alati su nerijetko izvedeni iz svakodnevnih pojednostavljenih načina funkcioniranja stvari.[206]

S druge strane, poduzeća u cilju sprječavanja prijevare koriste unutarnju i vanjsku IT reviziju. Redovito revidiranje informacijskih sustava pruža kredibilnost i transparentnost poduzeću. Dok je korištenje algoritama i programa za otkrivanje i sprječavanje prijevare uglavnom automatizirano, revizija ima značajniji ljudski faktor koji je ponekad neophodan za otkrivanje prijevare.[207] Može se reći da su automatizirani procesi i/ili algoritmi komplementarni s ljudskim faktorom, odnosno u svom radu se savršeno nadopunjuju.[208]

Pregledom teorijskih podloga uočavanja i sprječavanja poslovnih prijevara stvara se odlična podloga za kritički osvrt na prijevare iz stvarnog svijeta. Odabrano je sedam studija slučaja koje se ciljano razlikuju po vrsti kako bi se napravio što bolji kritički osvrt na njih.[209]

---

[202] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[203] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[204] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[205] Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782.
[206] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[207] Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu.
[208] Qadi, A. M., & Varol, A. (2020). The Role of Machine Learning in Digital Forensics. Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).
[209] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

Kada bi se jednostavno pokušalo generalizirati, može se reći da su poduzeća sama krivci za poslovne prijevare, s obzirom da se mogu izolirati dva slučaja: kada poduzeće svjesno vrši prijevaru i kada poduzeće svojom nepažnjom i nedovoljnim korištenjem prednosti digitalizacije otvara put napadačima. Naravno, u stvarnom poslovnom svijetu su stvari puno složenije.[210]

Analizom i usporedbom su vidljive sličnosti, poput činjenice da poduzeće u isto vrijeme može biti supočinitelj prijevare, ali i oštećenik. Uz to sličnost je kako je u svim promatranim slučajevima primarni razlog bio nedostatak kontrola, kao i praćenje najnovijih digitalnih trendova. U drugu ruku, ovi slučajevi se razlikuju po svojim učincima, negdje su financijske štete bile veće, dok su u nekim slučajevima financijske štete zanemarive, te je naglasak na kompromitiranim podacima.[211] Također sudbine poduzeća su se razlikovale, neka poduzeća, poput Madoffa[212] i ComAira[213] su propala. Dok u slučaju Targeta, poduzeće je naučilo iz naučene prijevare i krize, te je iskoristilo propust kako bi poradilo na implementaciji efikasnijih kontrola i poboljšanju digitalnih sustava.[214]

Kao što je već spomenuto, žrtva prijevare može biti bilo tko i bilo kada, stoga je potrebno uvijek primjenjivati stečena znanja, kao i biti svjestan najnovijih digitalnih trendova koji se svakodnevno mijenjaju. Od (pokušaja) prijevare je nemoguće pobjeći, ali zato treba staviti poseban naglasak na edukaciju poduzeća i „običnih ljudi“ o prijevarama, te kako reagirati i pravovremeno ih uočiti i tako spriječiti.[215]

[210] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[211] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[212] *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/
[213] Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.
[214] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.
[215] Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Ekonomski fakultet u Zagrebu.

Izvori

1. Alwashah, A., M., & Al-karabsheh, F. I. (2021). The role of internal and external audit in reducing the risk of accounting information systems (from the estimation of the internal and external auditor). *Journal of Management Information and Decision Sciences*, 1-16.
2. Apriliana, S., & Agustina, L. (2017). The Analysis of Fraudulent Financial Reporting Determinant through Fraud Pentagon Approach. *Jurnal Dinamika Akuntansi*, 154-165.
3. Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *Crypto Valley Conference on Blockchain Technology*, Caligari.
4. Bejaković, P. (1997). Pranje novca. *Financijska praksa*, 461-466.
5. *Bernie Madoff's Ponzi Scheme*. (21. Rujan 2021). Dohvaćeno iz International Banker: https://internationalbanker.com/history-of-financial-crises/bernie-madoffs-ponzi-scheme-2008/
6. Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, V. (2013). Visions and Voices on Emerging Challenges in Digital Business Strategy. *Fox School of Business Research Paper*, 1-31.
7. Bonabeau, E. (2007). *Understanding and managing complexity risk.* Cambrig: MIT.
8. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Westford: Software Engineering Institute.
9. Chien, E. (2005). *Techniques of Adware and Spyware.* VB2005 Conference.
10. Cindori, S. (2007). The Money Laundering Prevention System. *Financial theory and practice*, 59-76.
11. Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., & Romano, L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing*, 754-762.
12. Delamaire, L., Abdou, H., & Pointon, J. (2008). *Credit card fraud and detection techniques: a review* . Huddersfield: University of Huddersfield.

13. Dellinger, A. (26. svibanj 2019). *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* Dohvaćeno iz Forbes: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=26baafd1567f

14. Donning, H., Eriksson, M., Martikainen, M., & Lehner, O. M. (2019). Prevention and detection for risk and fraud in the digital age – the current situation. *ACRN Journal of Finance and Risk Perspectives*, 86-97.

15. Fox, P. (2020). Phishing attacks., Nastavni materijal Khan Academy

16. Gupta, S., Singhal, A., & Kapoor, K. (2016). *A Literature Survey on Social Engineering Attacks:.* International Conference on Computing, Communication and Automation (ICCCA2016).

17. Hadfield, J. (n.d.). *WHAT'S THE DIFFERENCE BETWEEN AN INTERNAL AND EXTERNAL AUDIT?* Preuzeto 30. lipanj 2022 iz Menzies: https://www.menzies.co.uk/helping-you/audit-compliance/what-is-an-audit/internal-audit-vs-external-audit/

18. Hoje, J., Hsu, A., Llanos-Popolizio, R., & Vergara-Vega, J. (2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business and Management Research*.

19. Ivanščak, M. (5. srpanj 2022). Plan vanjske IT revizije i među ovisnost unutarnje i vanjske revizije. (D. Krnić, Ispitivač), Intervju sa stručnjakom za IT reviziju

20. Khosravani, A., & Rasinariu, C. (2018). EMERGENCE OF BENFORD'S LAW IN MUSIC. *Journal of Mathematical Sciences*, 11-24.

21. King-Fung Pun, J. (2011). *Improving Credit Card Fraud Detection using a Meta-Learning Strategy.* Toronto: University of Toronto.

22. Kshetr, N. (2022). *Scams, Frauds and Crimes in the Nonfungible Token Market.* Greensboro: University of North Carolina.

23. Lee, S.-O. (2019). *Hackers on the highway: Are we prepared?* Chicago: Chicago Policy Review.

24. Matsumura, E. M., & Tucker, R. R. (1992). Fraud Detection: A Theoretical Foundation. *American Accounting Association*, 753-782.

25. Papić, M., Vudrić, N., & Jerin, K. (2017). *Benfordov zakon i njegova primjena u forenzičkom računovodstvu.* Zagreb: Zbornik sveučilišta Libertas.

26. Qadi, A. M., & Varol, A. (2020). *The Role of Machine Learning in Digital Forensics.* Beirut: 2020 8th International Symposium on Digital Forensics and Security (ISDFS).

27. Rainter, K. R., & Cegielski, C. G. (2011). *Introduction to information systems.* Danvers: John Wiley & Sons, Inc.

28. Reeves, M. (11. Srpnja 2022). *Corporate fraud*. Dohvaćeno iz Investopedia: https://www.investopedia.com/terms/c/corporate-fraud.asp

29. Samonas, S. (2005). *Insider fraud and routine activity theory.* Las Vegas: 12th Annual Security Conference.

30. Spremić, M. (2017). *Digitalna transformacija poslovanja.* Zagreb: Ekonomski fakultet u Zagrebu.

31. Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Zagreb: Ekonomski fakultet u Zagrebu.

32. Ssebulime, T. (2022). *Email Classification Using Machine Learning Techniques.* Bournemouth: Faculty of Science and Technology Bournemouth University.

33. Stolfo, S. J., Fan, D. W., Lee, W., & Prodromidi, A. L. (1997). *Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results.* New YorK City: Columbia University.

34. Suduc, A.-M. (2010). Audit for Information Systems. *Informatica Economică*, 43-48.

35. Tuo, J., Red, S., Lid, W., Li, X., Li, B., & Lei, L. (2004). *Artificial Immune System for Fraud Detection.* 2004: IEEE International Conference on Systems, Man and Cybernetics.

36. *Zakon o reviziji*. (1. siječanj 2018). Dohvaćeno iz Zakon.hr: https://www.zakon.hr/z/417/Zakon-o-reviziji

37. Zorz, Z. (2016): *Belgian bank Crelan loses €70 million to BEC scammers*. Dohvaćeno iz Help Net Security: https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ (26. siječanj 2016).

Popis slika

Popis tablica

Životopis studenta

Daria Krnić rođena je 13. siječnja 1999. godine u Zagrebu. Pohađala je srednju školu XV. Gimnazija, International Baccalaureate program. 2017. godine upisala je Ekonomski fakultet u Zagrebu, integrirani preddiplomski i diplomski studij Poslovne ekonomije. 2019. godine upisala je smjer Analiza i poslovno planiranje. Za vrijeme srednje škole volontirala je u raznim aktivnostima poput čišćenja školskih prostora, Božićnog sajma i na trkačkim utrkama. U akademskoj godini 2019/2020 bila je demonstrator na katedri za marketing kod profesora Vlašića. Za vrijeme studiranja, dvije godine je radila kao asistent u agenciji za odnose s javnošću. Od rujna 2021. stažira u revizorskoj kući Ernst and Young. Trenutno je u Ernst and Youngu stalno zaposlena kao asistent u reviziji s fokusom na reviziju financijskih institucija i poduzeća koje kotiraju na burzi.

U govoru i pismu se aktivno služi engleskim jezikom, te pasivno njemačkim jezikom. Za vrijeme studentskih poslova je ovladala alatima MS Office, kao i R Studiom. Posjeduje vozačku dozvolu B kategorije.