Analiza izvora, uzroka i posljedica kibernetičkih napada

Soldo, Ružica

Sveučilište u Zagrebu

Ekonomski fakultet

Specijalistički diplomski stručni studij

Elektroničko poslovanje u privatnom i javnom sektoru

ANALIZA IZVORA, UZROKA I POSLJEDICA KIBERNETIČKIH NAPADA

Diplomski rad

Ružica Soldo

Zagreb, srpanj, 2023.

Sveučilište u Zagrebu

Ekonomski fakultet

Specijalistički diplomski stručni studij

Elektroničko poslovanje u privatnom i javnom sektoru

ANALIZA IZVORA, UZROKA I POSLJEDICA KIBERNETIČKIH NAPADA

ANALYSIS OF SOURCES, CAUSES AND CONSEQUENCES OF CYBERATTACKS

Diplomski rad

Student: Ružica Soldo

JMBAG Studenta: 0067571925

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, srpanj, 2023.

SAŽETAK

Prema istraživanju iz 2022. godine uporaba računala i interneta na prošlogodišnjoj je razini, međutim digitalna pismenost i korištenje digitalnih rješenja i dalje nisu na zadovoljavajućoj razini.[1] S obzirom da Republika Hrvatska nije iznimka kada je riječ o digitalizaciji i digitalnoj pismenosti, Europska unija donosi rješenje problema odnosno strategiju pod nazivom „Digitalno desetljeće Europe“ gdje su navedeni ciljevi za 2030. godinu. Cilj strategije je omogućiti poduzećima i građanima da iskoriste održiviju i prosperitetniju digitalnu budućnost u kojoj je na prvom mjestu čovjek. Od velike je važnosti osjećati se sigurno prilikom korištenja Interneta kao temelja svih ostalih digitalnih rješenja. Sigurnosni mehanizmi za zaštitu od mogućih digitalnih napada na osobne podatke nastoje pratiti digitalne promjene koje su gotovo svakodnevne. Analizom mogućih uzroka kibernetičkih napada te izvora i na kraju posljedica tih napada kroz rad su istražena moguća rješenja za poboljšanje sigurnosti te je naglasak stavljen na važnosti poznavanja načina na koji napadači pokušavaju na nezakonit način doći do povjerljivih podataka korisnika digitalne tehnologije. Provedenim istraživanjem metodom uspoređivanja triju poduzeća koja su doživjela kibernetički napad zaključuje se da se radi o prijetnjama visoke razine rizika čije aktualne metode suzbijanja nisu dovoljno efikasne zbog čega je potrebno formiranje i kontinuirano usavršavanje napredne strategije obrane od povreda digitalnog identiteta. Osim toga od velike je važnosti informiranje zaposlenika o sigurnosnim mjerama i mjerama opreza kako bi se rizik potencijalnih kibernetičkih napada sveo na minimum.

Ključne riječi: Kibernetički napadi, kibernetička sigurnost, digitalne tehnologije, IT kontrole

[1] Markuš, H. (2022.), Državni zavod za statistiku Republike Hrvatske preuzeto 20.07.2023. s https://podaci.dzs.hr/2022/hr/29624

SUMMARY

According to the research from 2022, the use of computers and the Internet is at last year's level, however digital literacy and knowledge how to use digital solutions are still not on satisfying level.[2] *Considering that Republic of Croatia is not an exception when it comes to digitalization and digital literacy, European Union brings the solution, a strategy entitled the „Digital decade of Europe „where the aims for the year 2030 are listed. The aim of this strategy is to enable companies and citizens more sustainable and prosperous digital future in which man is in the first place. It is very important to feel safe when using the Internet as the basis of all other digital solutions. Safety/security mechanisms for protection against possible digital attacks which are based on personal data try to keep up with digital changes that are almost daily. Through the analysis of the possible causes of cyberattacks, sources and ultimately the consequences of these attacks, possible solutions for improving security were researched in my thesis. Emphasis was placed on the importance of knowing how attackers try to illegally access confidential data of digital technology users. Conducted research using the method of comparing three companies which were cyber attacked it is obvious that these are high-level threats whose current suppression methods are not efficient enough so it is necessary to form and continuous improvement of an advanced defense strategy against digital identity violations. In addition, it is of great importance informing employees about safety measures and precautions in order to minimize the risk of potential cyberattacks.*

Key words: *cyberattacks, cyber security, digital technologies, IT controls*

[2] Markuš, H. (2022.), Državni zavod za statistiku Republike Hrvatske preuzeto 20.07.2023. s https://podaci.dzs.hr/2022/hr/29624

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad / seminarski rad / prijava teme diplomskog rada 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 / prijave teme nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada / prijave teme ne krši bilo čija autorska prava.

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

_____

(vlastoručni potpis studenta)

_____

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

_____

(Personal signature of the student)

_____

(Place and date)

SAŽETAK I KLJUČNE RIJEČI

SUMMARY AND KEYWORDS

SADRŽAJ

1. UVOD

1.1. Obrazloženje rada

Analizom izvora, uzroka i posljedica kibernetičkih napada provedeno je istraživanje koje je ujedno i predmet ovog diplomskog rada. Vrtoglavim razvojem i napretkom digitalizacije ubrzano raste i broj zabilježenih kibernetičkih napada kao i pokušaja napada na pojedince i poduzeća. Najveći porast zabilježen je s pojavom pandemije bolesti korona virusom SSARS-CoV-2 (Coronavirus Disease 2019) koja je posebno zanimljiva bila napadačima iz razloga što je digitalni identitet bio jedini način za identifikaciju. Cilj ovog rada je provesti istraživanje metodom uspoređivanja triju poduzeća te ustanoviti koji su bili izvori, uzroci te koje je posljedice ostavio napad na pojedino poduzeće koje je bilo žrtva kibernetičkog napada. Naglasak je stavljen i na podizanje svijesti pojedinaca o važnosti informiranja i poduzimanja mjera zaštite od mogućih kibernetičkih napada. Osim toga donošenje odluke o potrebi informiranja javnosti o pretrpljenom napadu ili odluke prešutjeti pretrpljeni napad kako se ne bi narušila reputacija poduzeća, od velike je važnosti kao i način na koji objaviti informaciju.

1.2. Metodologija rada

Podaci potrebni za izradu teorijskog dijela diplomskog rada prikupljeni su na temelju sekundarnih podataka baziranih na stručnoj literaturi, znanstvenim člancima te Internetskim izvorima pouzdanih i relevantnih stranica kao što su Hrvatske znanstvene bibliografije, Hrčak, Emerald i sl. Za potrebe empirijskog dijela rada korištene su tri različite studije slučaja na temelju kojih su provedena istraživanja i doneseni zaključci. Novo doneseni zakoni, propisi i norme preuzeti su sa Internetskih stranica Narodne Novine „Zakon o informacijskoj sigurnosti“ čiji su podaci pouzdani i redovito ažurirani.

1.3. Struktura diplomskog rada

Rad se sastoji od ukupno pet poglavlja unutar kojih je kroz svega nekoliko pod poglavlja detaljno razrađena tema diplomskog rada. Prvo uvodno poglavlje rada pobliže objašnjava temu rada te definira cilj i izvore prikupljenih podataka korištenih prilikom pisanja rada. Slijedeće poglavlje

podijeljeno je na tri pod poglavlja u kojem je teorijski obrađena tema rada. Pod poglavlja od kojih je sačinjeno poglavlje objašnjenje najvažnijih pojmova su obilježja i najčešći uzroci kibernetičkih napada, kibernetički rizici te osnove kibernetičke sigurnosti. Treće poglavlje sastoji se od najvažnijih mehanizama za zaštitu od kibernetičkih napada koji su od velike važnosti u današnjem digitalnom dobu. Navedene su posljedice koje nastaju prilikom kibernetičkog napada te vrste i obilježja IT kontrola (kontrola informatičke tehnologije). U ovom poglavlju predstavljena su tri studija slučaja na temelju kojih je u idućem poglavlju provedeno istraživanje. Prvi odabrani slučaj na temelju kojeg je provedeno istraživanje odnosi se na krađu podataka u maloprodajnom lancu Target gdje je napad otkriven tek nakon 18 dana što je začuđujuće s obzirom da se radi o najvećem američkom trgovačkom lancu. Colonial Pipeline sustav drugi je slučaj na temelju kojeg je provedeno istraživanje kao i WannaCry. Kroz navedene studije slučaja provedeno je istraživanje na temelju analize izvora, uzroka i posljedica kibernetičkih napada. Zaključak rada sastoji se od rezultata do kojih se došlo provedenom analizom, odnosnom istraživanjem odabranih studija slučajeva.

2. OBJAŠNJENJE NAJVAŽNIJIH POJMOVA

Digitalne tehnologije uvelike su utjecale na promjenu načina života, rada, poslovanja i kupnje te i dalje utječu pa čak i na promjenu društva. Koriste se kako bi se ljudima omogućio uspjeh, optimizirale sve poslovne funkcije i kako bi se poslovanje učinilo relevantnijim i profitabilnijim. Ubrzanom digitalnom transformacijom i unapređenjem virtualnog načina života i rada vrtoglavom brzinom razvijaju se i zlonamjerne radnje prisutne u online svijetu. Osim poduzeća svakodnevne mete napada su i svi ostali korisnici Interneta koji prethodno stečenim znanjem ili nažalost iskustvom hakerskog napada mogu utjecati na to da do istog ne dođe ili u slučaju da se napad i dogodi kako reagirati i koje radnje poduzeti. Nažalost ovakvih Internetskih korisnika je relativno malo zbog čega je informiranost od velike važnosti.

Neki od važnih pojmova koji pomažu u razumijevanju teme diplomskog rada su:[3]

1. Kibernetika: Kibernetika je interdisciplinarno područje koje se bavi proučavanjem sustava, kontrolnih procesa i komunikacije između ljudi i strojeva. Ova znanost uključuje primjenu matematičkih, tehničkih i računalnih principa kako bi se razumjelo ponašanje, kontrola i interakcija u složenim sustavima.
2. Kibernetički napadi: „Kibernetički napadi su zlonamjerne aktivnosti koje se provode putem računalnih mreža ili Interneta s ciljem ometanja, oštećenja ili neovlaštenog pristupa informacijskim sustavima, podacima ili resursima.“ (Spremić, 2017) Primjeri kibernetičkih napada uključuju phishing, ransomware, DDoS napade, krađu identiteta i napade na infrastrukturu.
3. Kibernetička sigurnost: Kibernetička sigurnost ima za svrhu zaštititi informacijske sustave, podatke i mreže od različitih kibernetičkih prijetnji. To podrazumijeva primjenu tehnika, mjera i postupaka kako bi se prepoznale, spriječile, otkrile i reagiralo na sigurnosne prijetnje. Glavni cilj kibernetičke sigurnosti je osigurati da informacije ostanu povjerljive, da se očuva integritet podataka te da budu dostupne samo ovlaštenim korisnicima, sprečavajući neovlašteni pristup, oštećenje ili krađu podataka. (Spremić, 2017)

[3]Ministarstvo unutarnjih poslova (2015.), Nacionalna strategija kibernetičke sigurnosti preuzeto 13.03.2023. s: https://mup.gov.hr/UserDocsImages/minstarstvo/kibernetika/strategija_kibernetika.pdf

4. Kibernetički prostor: Prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća Internet i sve sustave povezane na njega
5. Sigurnosni propusti: Sigurnosni propusti su ranjivosti ili slabosti u informacijskim sustavima koje mogu biti iskorištene za napade. To može uključivati loše konfigurirane sigurnosne postavke, zastarjele softverske zakrpe, slabe lozinke ili loše upravljanje pristupom.
6. Sigurnosna politika: Sigurnosna politika je skup smjernica, pravila i postupaka koje organizacija uspostavlja kako bi zaštitila svoje informacijske resurse. To obuhvaća definiranje sigurnosnih standarda, postupaka autentifikacije, upravljanje pristupom, sigurnosne kopije podataka i odgovornosti zaposlenika u vezi s kibernetičkom sigurnošću.
7. Etičko hakiranje: Etičko hakiranje, također poznato kao penetracijsko testiranje ili etičko testiranje sigurnosti, je proces provjere sigurnosti informacijskog sustava ili mreže putem autoriziranog hakiranja. Ovaj proces obično provodi stručnjak za sigurnost kako bi otkrio sigurnosne propuste i preporučio mjere zaštite.
8. Ransomware: Ransomware je vrsta kibernetičkog napada u kojem se zlonamjerni softver instalira na računalu ili mreži kako bi se šifrirali podaci ili onesposobio pristup sustavu. Napadači zatim zahtijevaju otkupninu (obično u kriptovaluti) za vraćanje podataka ili ponovno dobivanje pristupa. Navedeni pojam detaljnije je opisan u nastavku rada. (Spremić, 2017)
9. Phishing: Phishing je tehnika kibernetičkog napada u kojoj se napadači predstavljaju kao pouzdane osobe, organizacije ili institucije kako bi prevarili korisnike da otkriju osobne podatke, kao što su korisnička imena, lozinke, brojevi kreditnih kartica itd. Najčešće se koristi putem lažnih e-mailova, poruka ili web stranica. Navedeni pojam detaljnije je opisan u nastavku rada.
10. DDoS napadi: DDoS (Distributed Denial of Service) napadi su napadi u kojima se koristi veliki broj računala ili uređaja za preplavljivanje ciljanog sustava mrežnim prometom, čime se onemogućava pristup ili dostupnost usluge korisnicima. Navedeni pojam detaljnije je opisan u nastavku rada.

2.1. Obilježja i najčešći uzroci kibernetičkih napada

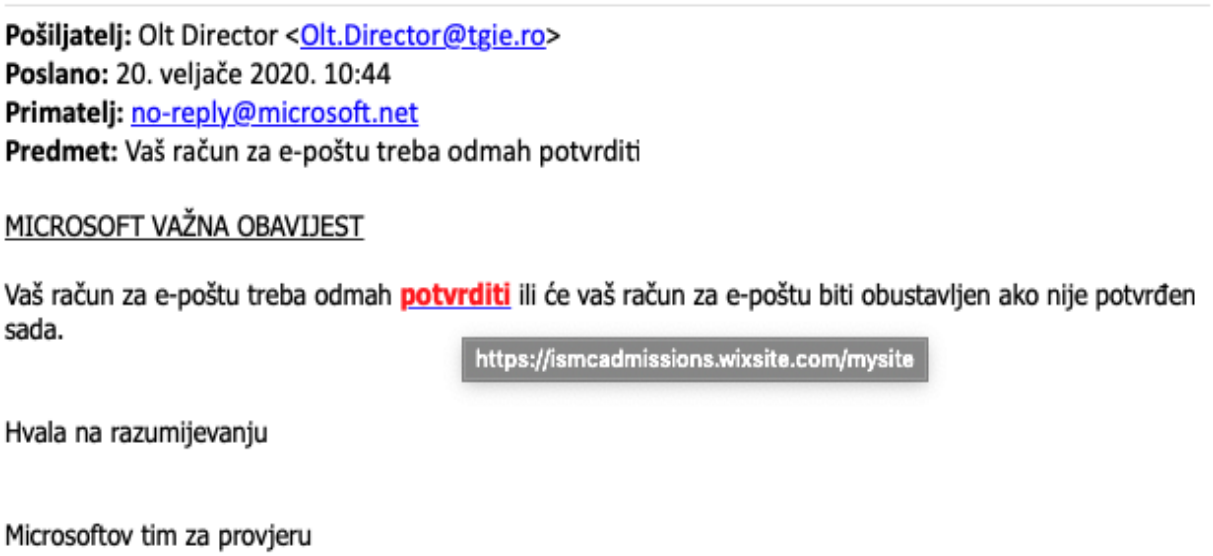
Kibernetika je znanstvena disciplina koja proučava sustave, kontrolu i komunikaciju, a često se koristi za opisivanje interakcije između ljudi i strojeva. Međutim kibernetički napadi odnose se na zlonamjerne aktivnosti koje koriste računala, Internet i druge tehnologije kako bi prodrli u informacijske sustave, krađu podataka ili uzrokovali štetu organizacijama ili pojedincima.

Riječ *phishing* dolazi od engleske riječi "*fishing*" kojom je metaforički opisan postupak kojim neovlašteni korisnici mame korisnike Interneta kako bi dobrovoljno otkrili svoje povjerljive podatke.[4] U literaturi se često susreće i pojam *Identity Theft* ili *Identity Fraud* koji se dovodi u svezu sa *phishingom*, a predstavlja termine koji se upotrebljavaju za sve tipove kriminala u kojima netko pokušava na nezakonit način doći do osobnih podataka i zlouporabiti ih u svrhu pribavljanja neke protupravne ekonomske koristi.[5] *Phishing* je samo jedna od tehnika korištenih za krađu identiteta. Ova vrsta kibernetičkog napada koristi prikrivenu e-poštu kao sredstvo napada. Cilj kampanje je krađa osjetljivih podataka poput brojeva kreditnih kartica te podataka potrebnih prilikom prijave. Tehnikama društvenog inženjeringa nastoji se prevariti primatelja e-pošte na način da isti povjeruje da je baš ta poruka ono što njemu treba. Žrtvu se nastoji navesti na čin da preda osjetljive podatke kao što su korisničko ime i lozinka kako bi ih napadač mogao koristiti za probijanje sustava ili računa.[6] Standardna procedura uključuje slanje e-pošte sastavljene tako da se poruka čini iznimno važnom, kao da ju je poslala banka ili neka velika partner firma. Osoba koja dobiva takvu e-poštu, otvara poveznicu u privitku čime nesvjesno odlazi na zlonamjerno mjesto dizajnirano da sliči web stranici te banke ili partner firme. Osoba zatim unosi potrebne podatke i dalje vjerujući da se radi o sigurnom web mjestu. Osim ostavljanja korisničkog imena i lozinke, napadači često u privitku e-pošte šalju poveznicu koja sadrži zlonamjeran softver. Ti su privitci često zip datoteke ili dokumenti Microsoft Officea u kojima je ugrađen zlonamjerni kod kojim žrtva zapravo zarazi vlastito računalo. Najčešći oblik zlonamjernog koda je *ransomware* osmišljen da iznuđuje novac blokiranjem pristupa datotekama ili računalnom sustavu dok se ne uplati

[4] Kibernetika (2020.), Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, preuzeto 14.03.2023. s https://enciklopedija.hr/natuknica.aspx?id=31381
[5] Bača, M., Ćosić, J. (2013.), Prevencija računalnog kriminaliteta. Policija i sigurnost. 22 (1), preuzeto 14.03.2023. s: https://policijska-akademija.gov.hr/UserDocsImages/onkd/1-2013/baca_cosic.pdf
[6] Fruhlinger, J. (2019). What is phishing? Preuzeto 14.03.2023. s: https://www.csoonline.com/article/2117843/what-isphishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

otkupnina iako ista ne jamči da će datoteka biti vraćena odnosno da će se moći pristupiti sustavu.[7] *Phishing* napad više je od slanja e-maila i očekivanja da će netko otvoriti poslanu poveznicu. Najjednostavniji pristup je oblikovanje zlonamjernog URL-a tako da se čini da je povezan s legitimnom web-stranicom, skraćivanje URL-a, skriveno preusmjeravanje, prikaz cijele ili samo dijela poruke kao grafičke slike i brojne druge tehnike načini su na koji hakeri djeluju kako bi njihov napad bio uspješan. Primjer *phishing* poruke prikazan je na slici 1.

Slika 1 Primjer phishing poruke



Izvor: https://csi.hr/2021/04/29/kako-prepoznati-e-mail-prijevaru-phishing-2/

Sljedeća najčešća vrsta kibernetičkih napada je *malware* odnosno napad zlonamjernih softvera koja ujedinjuje viruse, crve, trojance i druge zločudne i nedobronamjerne aplikacije s ciljem nanošenja materijalne štete pojedincima. *Malware* je računalni program koji se može samostalno umnožavati

[7] CISCO. What is Cybersecurity?, preuzeto 14.03.2023. s: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

te izvoditi radnje bez volje korisnika računala.[8] Najbolji primjer objašnjenja koliko je ovaj zlonamjerni softver zapravo opasan i koliko štete može uzrokovati je slučaj krađe podataka u maloprodajnom lancu Target. Kao što je poznato Target je jedan od najvećih američkih trgovačkih lanaca osnovan 1902. godine u Minneapolisu.[9] U prosincu 2013. godine, došlo je do provaljivanja u informacijski sustav trgovačkog lanca Target, što je rezultiralo štetom od preko 200 milijuna USD za sanaciju te padom profita za 46%. Što se zapravo dogodilo? *Fazio Mechanical* kompanija je koja je održavala rashladne sustave u *Targetovim* prodavaonicama te je imala pristup njihovom informacijskom sustavu kako bi online nadzirali temperaturu u poslovnicama. Naime napadači su hakiranjem *Fazio Mechanicala* dobili pristup *Targetovom* informacijskom sustavu, međutim kako je Target imao loše odvojene informacijske sustave, loš sustav autorizacije i zastarjele software nije bio veliki problem probiti se do POS terminala gdje je zapravo i instaliran *malware*. Na taj način napadači su krali podatke s „magnetnih traka kreditnih kartica." (Spremić, 2017) Međutim ni tu nije kraj. Prvih nekoliko dana trajalo je testiranje, a kada su shvatili da sve dobro funkcionira *malware* je instaliran na većinu preostalih prodajnih mjesta preko redovite nadogradnje POS terminala. Tek nakon 18 dana instaliran je *anti-malware* software kada je tvrtka koja ga je instalirala shvatila da se nešto čudno događa u informacijskom sustavu. Propusti do kojih je ovdje došlo definitivno su prekomjerne role, generički korisnički račun gdje svi imaju istu šifru, jednu kojom se svi mogu koristiti te ne segmentacija mreže. U nastavku rada navedeni slučaj je detaljnije analiziran i uspoređen sa sličnim vrstama kibernetičkog napada.

Osim malware, među najčešće kibernetičke napade ubraja se i neželjena pošta (engl. *spam*) koji u posljednje vrijeme predstavlja velike probleme. *Spam* ili *junk* mail koristi sustav elektroničke pošte kao cilj napada kroz koji šalje velike količine istih ili različitih poruka. S obzirom da je marketing našao mjesto u elektroničkoj pošti te da takva vrsta reklamiranja i oglašavanja donosi jako dobre rezultate odnosno najniže troškove oglašavanja, jedan veći dio kompanija odlučuje se za taj oblik oglašavanja. Upravo iz tog razloga lako dolazi do prestanka rada računalnog sustava. Jednostavnije

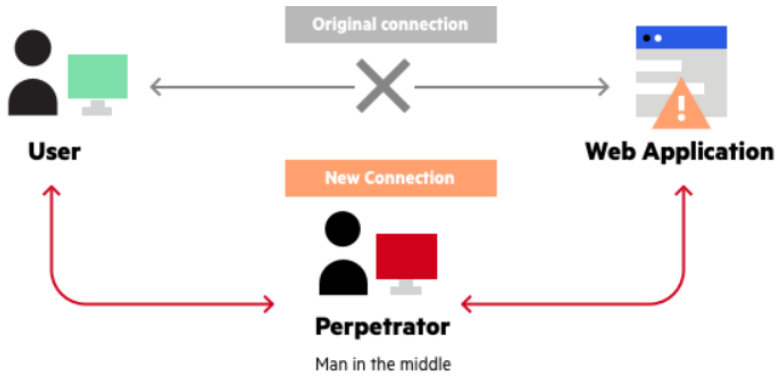
[8] Kibernetika (2020.), Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, preuzeto 14.03.2023. s: https://enciklopedija.hr/natuknica.aspx?id=31381

[9] Studija slučaja temelji se na slijedećim materijalima: Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, sveučilišni udžbenik, Ekonomski fakultet Zagreb, str. 44 i Corrin, J. (2021). Warnings (& lessons) of the 2013 Target data breach. pristupljeno 19.06.2023. preuzeto s: https://redriver.com/security/target-data-breach

rečeno, primamo poruke koje ne želimo primati i koje nas ometaju u svakodnevnom radu sa sustavom elektroničke pošte te zatrpavaju korisnikov poštanski pretinac bez njegovog dopuštenja. Osobe koje šalju neželjene poruke nazivaju se spameri (engl. s*pammers*). Da bi spameri mogli slati neželjene poruke prvo moraju prikupiti e-mail adrese potencijalnih primatelja. Adrese se prikupljaju preko *chatova*, web stranica, *newsgrupa* ili virusom zaraženih računala. Kako robotski sakupljači ne bi mogli doći do mail adresa savjetuje se izbjegavanje pisanja u izvornom obliku, odnosno kodiranje prije slanja. Prema istraživanjima danas se gotovo tri od četiri poslane elektroničke poruke smatraju neželjenima (*spam*) dok stručnjaci kažu da svega 5% poruka nije *spam*.[10]

Man-in-the-Middle (MITM) još je jedan u nizu kibernetičkih napada, a radi se o napadu prisluškivanjem. Riječ je o postavljanju zlonamjernog računalnog programa koji zaobilazi zaštitne kontrolne mjere te presreće sadržaj i šalje ga poslužitelju. Cilj ovog napada jest krađa osobnih podataka, kao što su vjerodajnice za prijavu, podaci o računu i brojevi kreditnih kartica. Slijedeća slika prikazuje primjer MITM napada.[11]

Slika 2 Primjer MITM napada



[10] Bača, M., Ćosić, J. (2013.), Prevencija računalnog kriminaliteta, Policija i sigurnost, 22 (1), preuzeto 15.03.2023. s: https://policijska-akademija.gov.hr/UserDocsImages/onkd/1-2013/baca_cosic.pdf

[11] What is MITM attack?, Imperva pristupljeno 17.03.2023. preuzeto s: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Izvor: What is MITM attack?, Imperva pristupljeno 17.03.2023. preuzeto s: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Nakon uspješnog izvršenja MITM-a slijedi presretanje i dešifriranje. Prvo se presreće korisnikov promet preko napadačeve mreže. Najčešći i najjednostavniji način za tu radnju je otvaranje slobodne Wi-Fi mreže u blizini kafića, hotela ili nekog drugog mjesta gdje je velika cirkulacija ljudi. Jednom kada se žrtva spoji na takvu žarišnu točku, napadač dobiva punu vidljivost bilo koje Internetske razmjene podataka. Nakon presretanja, svaki dvosmjerni SSL promet treba dešifrirati bez upozorenja korisnika ili aplikacije. Postoji nekoliko metoda kako bi se to moglo postići.[12] Jedna od njih je HTTPS *spoofing* koji šalje lažni certifikat žrtvinom pregledniku nakon što se napravi početni zahtjev za povezivanje sa sigurnim mjestom. Sadrži digitalni otisak prsta koji je povezan s ranjivom aplikacijom, a preglednik ga provjerava prema listi pouzdanih stranica. Napadač koristi ovaj digitalni otisak prsta kako bi pristupio svim podacima koje je žrtva unijela prije nego što se ti podaci proslijede aplikaciji. Osim toga, SSL Beast je još jedna metoda napada koja cilja ranjivost u SSL-u, posebno u verziji 1.0 TLS-a.[13] Ovaj napad omogućuje napadaču dešifriranje podataka koji se šalju preko ranjive SSL veze. U ovom slučaju žrtvino računalo je zaraženo zlonamjernim *JavaScriptom* koji presreće šifrirane kolačiće koje šalje web aplikacija. Najbolji načini za izbjegavanje ovakvih napada je ne spajanje na WiFi veze koje nisu zaštićene lozinkom, obraćanje pozornosti na obavijesti preglednika koje izvješćuju da je web mjesto nezaštićeno, trenutna odjava sa sigurne aplikacije kada nije u upotrebi te ne korištenje javnih mreža (npr. kafići, hoteli) pri provođenju osjetljivih transakcija.

SQL napadi, napadi uskraćivanjem usluge, unutarnji napadi, napadi zlonamjernog rudarenja kripto valute, eksploatacija nultog dana te napadi na pouzdano i posjećeno web mjesto još su neki od kibernetičkih napada koji su također prisutni kada je riječ o kibernetici.[14]

[12] What is MITM attack?, Imperva, pristupljeno 17.03.2023. preuzeto s: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
[13] What is MITM attack?, Imperva, pristupljeno 17.03.2023. preuzeto s: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
[14] What is MITM attack?, Imperva, pristupljeno 17.03.2023. preuzeto s: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Napadi se mogu usmjeriti na pojedince, organizacije, vlade, kritičnu infrastrukturu, financijske institucije, medicinske ustanove itd. Cilj ovisi o motivima napadača i potencijalnoj koristi koju mogu ostvariti. Bez obzira o kojoj vrsti kibernetičkog napada se radi, ne znanje odnosno ne dovoljna informiranost korisnika Internetskih mreža i raznih sustava najčešći je uzrok zbog kojeg su građani ali i korporacije žrtve računalnog kriminala. Prekomjerne role koje su dodijeljene zaposlenicima koji nemaju dovoljno znanja o mogućim rizicima također su uzrok brojnih kibernetičkih napada. Iste lozinke koje su dodijeljene većem broju zaposlenika i koje odgovaraju većem broju sustava u koje se pristupa dodatno olakšavaju probijanje u sustav neovlaštenim korisnicima. Takvi propusti u poduzeću mamac su hakerima jer bez puno truda lako pristupaju povjerljivim informacijama. Tako odgovorne osobe koje nisu svjesne da jednim pritiskom na link koji je došao sa nepoznate e-mail adrese mogu nanijeti velike financijske štete, narušiti reputaciju poduzeća te neovlaštenim osobama dodijeliti povjerljive podatke poduzeća ali i osobne podatke korisnika proizvoda ili usluga tog poduzeća. Slabe sigurnosne prakse, nedostatak ažuriranja i nadogradnje sustava, nekorištenje sigurnosnih alata i protokola, loše konfigurirane mreže i sustavi mogu stvoriti ranjivosti koje napadači mogu iskoristiti. Napadi na državne institucije, vojsku ili kritičnu infrastrukturu mogu biti motivirani političkim, vojnim ili špijunskim interesima. Napadi motivirani društvenim ili političkim uvjerenjima mogu se usmjeriti na organizacije, institucije ili pojedince koji su povezani s određenim ideologijama, sukobima ili kontroverznim temama. (Gillis 2020) Od kibernetičkog napada poduzeće se oporavlja mjesecima pa čak i godinama kako zbog financijske štete tako i zbog ne povjerenja postojećih i mogućih novih korisnika, odnosno narušavanja reputacije poduzeća. Postojeći korisnici ne osjećaju se više sigurno te traže alternativni proizvod ili uslugu, odlaze konkurentima, ali ni s potencijalno novim korisnicima situacija nije drugačija. Neadekvatne mjere zaštite i sigurnosni mehanizmi u koje organizacija ne ulaže dovoljno niti financijskih sredstava niti vremena i ne smatra da je uopće potrebno preusmjeriti fokus na sigurnost, indirektno izlažu poduzeće visokom riziku napada.[15]

[15] Gillis, A.S. (2020). What is cyber hygiene and why is it important?. Techtarget, preuzeto 26.04.2023. s: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

2.2. Kibernetički rizici

Kibernetički rizici su operativni rizici koji imaju potencijalno negativan učinak na kibernetičku sigurnost te koji nastaju kao posljedica intenzivne primjene digitalnih tehnologija kako u poslovanju tako i u svakodnevnom životu.[16] Sve intenzivnija primjena informacijskih sustava dovodi do neočekivanih i neželjenih štetnih posljedica kako financijskih tako i materijalnih šteta unutar i izvan organizacije koje mogu izravno ali i neizravno utjecati na samu organizaciju.[17] Povećanjem broja učinkovitih kontrola koje su zadužene za sprječavanje nastanka neželjenog događaja povećava se vjerojatnost da će organizacija biti sve manje i manje izložena informatičkim rizicima.[18] Dakle ako i dođe do neželjenog događaja on će vrlo vjerojatno biti manjeg intenziteta zbog djelovanje informatičkih kontrola ali i odgovornih osoba koje brzom reakcijom smanjuju štetu koju neželjeni događaj može prouzročiti. Važno je naglasiti da su informatički rizici uvijek prisutni bez obzira jesu li otkriveni zahvaljujući provođenjem redovitih kontrola ili nisu.[19] Kako zahvaljujući dobrim i kvalitetnim aktivnostima od strane kvalificiranih zaposlenika čiji je zadatak brigao o sigurnosti podataka, organizacija stvara nove poslovne prilike te bilježi konkurentsku prednost, tako i nekvalitetne mjere sigurnosti uništavaju poslovanje, odnosno stvaraju gubitke te velike štete i probleme za organizaciju. U kontekstu nekvalitetnih mjera sigurnosti misli se na nemarnost djelatnika prilikom svakodnevnih poslovnih aktivnosti bez obzira jeli zadatak tih zaposlenika briga o sigurnosti podataka ili neki skroz drugi oblik odgovornosti.

Prijetnje mogu nastati unutar ili izvan organizacije. Unutarnje prijetnje odnose se na sigurnosne prijetnje koje potječu unutar organizacije. Primjeri unutarnjih prijetnji uključuju:[20]

1. Neki oblik interne prijevare- kada zaposlenik ili član organizacije zlonamjerno djeluje kako bi naškodio organizaciji ili ostvario osobnu korist.

[16] Kovač, D. (2021.), Ulaganje u kibernetičku sigurnost. Zbornik radova veleučilišta u Šibeniku, 15 (1-2), str. 61-73.
[17] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[18] Miloš Sprčić, D. (2013.), Upravljanje rizicima: temeljni koncepti, strategije i instrumenti, Zagreb, Sinergija, str. 20
[19] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[20] ENISA Threat Landscape (2020). Insider threat. preuzeto 20.07.2023. s file:///C:/Users/user/Downloads/ETL2020%20-%20Insider%20Threat%20A4.pdf

2. Neovlašteni pristup informacijama- kada zaposlenik koristi svoje ovlasti za pristup podacima na način koji nije u skladu s pravilima organizacije ili u svrhu za koju nema ovlasti.
3. Krađa resursa informacijskog sustava- kada zaposlenik zloupotrebljava resurse organizacije, poput računala, mrežnih resursa ili softvera.
4. Greške u unosu podataka u aplikacije- nesmotrene ili nenamjerne greške zaposlenika koje mogu dovesti do sigurnosnih propusta ili oštećenja podataka.
5. Nesvjesno prenošenje povjerljivih informacija- kada zaposlenik slučajno iznosi ili dijeli povjerljive informacije s neovlaštenim osobama ili preko nesigurnih kanala komunikacije.

Uz unutarnje prijetnje, organizacije također moraju obratiti pažnju na vanjske prijetnje koje potječu izvana, kao što su kibernetički napadi, phishing, ransomware, DDoS napadi, i slično. Važno je zaštititi organizaciju od svih vrsta prijetnji kako bi se osigurala kibernetička sigurnost i zaštita podataka. Hakerski napadi, zlonamjerni računalni kod, društveni inženjering, epidemija bolesti te elementarne nepogode samo su neke od vrsta vanjskih prijetnji na organizaciju.[21]

Informatički rizici mogu se podijeliti u četiri glavne kategorije, a to su strateški (korporativni) informatički rizici, rizici provedbe informatičkih programa i projekata, rizici provedbe poslovnih procesa (operativni ili transakcijski informatički rizici) te infrastrukturni informatički rizici.[22]

„Strateški informatički rizici predstavljaju potencijalne opasnosti koje ugrožavaju strateške poslovne interese kompanije, nastale uslijed donošenja pogrešnih odluka povezanih s primjenom digitalnih i informacijskih tehnologija za inovaciju poslovnog modela i postizanje poslovnih ciljeva. Ovi rizici imaju utjecaj na najvišu razinu upravljanja u organizaciji, što znači da mogu prouzročiti velike financijske štete i gubitke. Neki primjeri informatičkih rizika uključuju rizik pogrešne strategije ili nedostatak strategije, nespremnost organizacije na promjene i digitalnu

[21] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[22] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, Zagreb

transformaciju poslovanja rizik tržišnog natjecanja, neispunjavanje zakonskih obveza, pogrešna ulaganja u informatiku i sl.“[23]

Rizici da ulaganja u informatiku neće biti ispravno vođena te da provedba tih ulaganja kroz informatičke programe i projekte neće biti učinkovita ili da neće doprinijeti stvaranju nove vrijednosti spada u kategoriju rizika provedbe informatičkih programa i projekata. Ovi rizici pripadaju kategoriji rizika provedbe informatičkih programa i projekata. S druge strane, rizici provedbe poslovnih procesa fokusiraju se na osiguranje sigurnog, neometanog i pouzdanog izvršenja poslovnih procesa. (Spremić, 2017) Primjer za ovu vrstu rizika uključuje neprekidnost poslovanja, provođenje informatičkih usluga, oporavak nakon neželjenih događaja te nedostupnost, nečitljivost i neupotrebljivost podataka nakon prekida neželjenog događaja, zajedno s mnogim drugim rizicima. (Spremić 2017) Infrastrukturni informatički rizici odnose se na rizike koji utječu na redovito funkcioniranje informatičke infrastrukture. (Spremić, 2017) Primjeri ove vrste rizika bili bi rizik komunikacijske infrastrukture, servisa elektroničke pošte te dostupnost i funkcionalnost računalne mreže.[24]

Kibernetički rizici predstavljaju opasnosti i prijetnje koje proizlaze iz korištenja informacijskih tehnologija i digitalnih sustava.[25] U suvremenom digitalnom okruženju, kibernetički rizici su sveprisutni i predstavljaju ozbiljan izazov za organizacije i pojedince. Evo nekoliko važnih kibernetičkih rizika koji se mogu pojaviti:

1. Napadi hakera: Napadi hakera predstavljaju jedan od najčešćih i najopasnijih kibernetičkih rizika. Napadači mogu pokušati provaliti u sustave, krađom ili oštećenjem podataka, ili preuzimanjem kontrole nad sustavom radi iznude ili širenja štetnih aktivnosti.

[23] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[24] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[25] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, Zagreb

2. Zloćudni računalni kod: *Malware*, uključujući viruse, trojanske konje, crve i *spyware,* predstavlja veliki kibernetički rizik. Ti zlonamjerni programi mogu se infiltrirati u sustave i nanijeti štetu, krađom podataka, ometanjem rada sustava ili širenjem daljnjih infekcija.

3. *Phishing*: *Phishing* je tehnika prijevare putem e-pošte, u kojoj se korisnici lažno potiču da otkriju osjetljive informacije poput korisničkih imena, lozinki ili bankovnih podataka. To može dovesti do krađe identiteta ili zloupotrebe računa.

4. Društveni inženjering: Društveni inženjering je tehnika manipulacije ljudima kako bi otkrili povjerljive informacije ili izvršili određene radnje. Napadači mogu koristiti psihološke trikove kako bi prevarili ljude da otkriju informacije ili izvrše zlonamjerne radnje.

5. Slabosti u sigurnosti aplikacija: Slabosti u sigurnosti aplikacija mogu omogućiti napadačima da iskoriste ranjivosti kako bi provalili u sustav ili preuzeli kontrolu nad njim. To može biti rezultat nedostataka u kodiranju ili nepotpunog ažuriranja aplikacija.

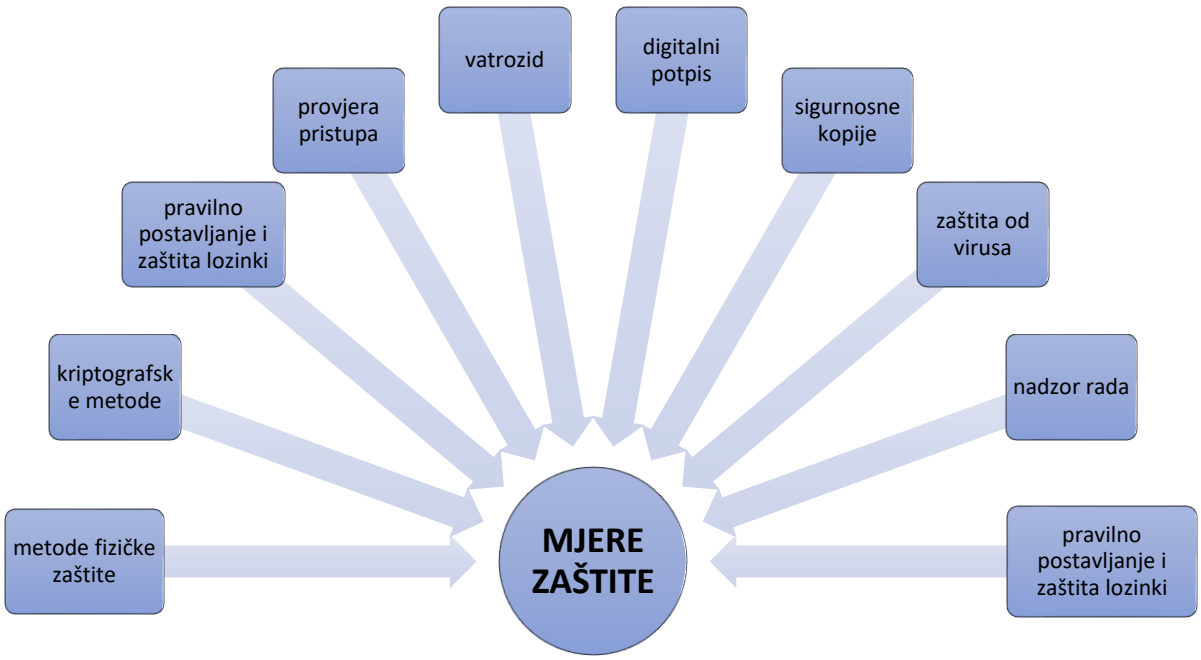
6. DDoS napadi: Napadi distribuirane usluge (DDoS) ciljaju ometanje pristupa sustavima preopterećenjem mreže ili resursa. Napadači koriste bot mreže kako bi izazvali preopterećenje i onemogućili pravilan rad sustava.

7. Interna prijetnja: Interna prijetnja potječe iz organizacije, od zaposlenika koji ima pristup povjerljivim informacijama ili sustavima. Zaposlenici mogu biti namjerni ili nenamjerni izvor kibernetičkih rizika, kroz neoprezno rukovanje podacima ili zloupotrebu privilegija pristupa.

Kako bi se neometano moglo nastaviti s poslovanjem u slučaju nekog štetnog događaja te kako bi se brzo i efikasno poduzeće oporavilo odnosno ponovno pokrenulo važno je upoznati organizaciju sa skupom aktivnosti, radnim procedurama i pravilima po kojima je važno postupati. Osim

navedenog osnovni smisao jest ustrojiti i preventivne mjere kojima će se spriječiti njihov nastanak ili smanjiti vjerojatnost takvoga ishoda. Opasnost prestanka kontinuiranog poslovanja prijeti gotovo svim kompanijama koje u poslovanju koriste informacijske sustave. Stoga, glavni je zadatak najviših tijela upravljanja ustrojiti mehanizme upravljanja kontinuitetom poslovanja, definirati potencijalne štetne i neželjene događaje koji mogu uzrokovati prekide poslovnih procesa ili dovesti do otežanog odvijanja poslovnih procesa. Određivanje kontrola, organizacijske mjere te korporacijska pravila važni su koraci kako bi se štetni događaji i njihov utjecaj smanjio ili ublažio. Slika 3 prikazuje mjere zaštite kako bi rizike sveli na najmanju moguću razinu (Dragičević, 1999.)

Slika 3 Mjere zaštite od kibernetičkih napada



Izvor: izrada autora prema Dragičević (1999.)

2.3. Osnove kibernetičke sigurnosti

Kibernetička sigurnost prema zakonu iz Narodnih Novina (64/2018) definirana je kao „sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom

prostoru.“ Republika Hrvatska može se pohvaliti brojnim zakonima kao i uredbama koje definiraju područje informacijske i kibernetičke sigurnosti, a neki od njih su Zakon o informacijskoj sigurnosti te odgovarajuća Uredba i Pravilnici, Zakon o sigurnosnim provjerama te odgovarajuća Uredba, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga s odgovarajućom Uredbom te Smjernicama, Nacionalna strategija kibernetičke sigurnosti te brojne druge. Unatoč postojanju ovih zakona i mjera, nije moguće tvrditi da su kibernetički napadi u potpunosti spriječeni ili otklonjeni. Nedovoljno ulaganje u kibernetičku sigurnost i nedostatak svijesti o njezinoj važnosti rezultiraju povećanim rizicima od napada. Posebno su se takvi rizici povećali tijekom pandemije koronavirusa, koja je prisilila organizacije na rad od kuće i povećala upotrebu cloud sustava. Tradicionalne tehnike zaštite od kibernetičkih rizika, poput tehnika zaštite od neovlaštenog pristupa, kriptografije, tehnika otkrivanja i prevencije, kao i revizija informacijskih sustava, predstavljaju važne mehanizme kibernetičke sigurnosti.[26] Ulaganje u kibernetičku sigurnost metoda je fizičke kontrole kojom se utječe na smanjenje rizika mogućeg napada s kojima se susreću poslovne organizacije. Brojke pokazuju da se ne ulaže dovoljno u kibernetičku sigurnost te da je svijest o važnosti kibernetičke sigurnosti minimalna.

Svaki informacijski sustav ima ugrađene različite kontrole kako bi postigao svoje ciljeve u funkcioniranju. Korištenjem sve učinkovitijih kontrola smanjuje se mogućnost da bi neželjeni događaji mogli izazvati rizik za poslovanje. (Spremić, 2017) Da bismo provjerili postojanje i kvalitetu tih informatičkih kontrola, te kako bismo utvrdili njihovu korisnost i pouzdanost, koristimo reviziju informacijskih sustava. (Spremić, 2017) Revizija informacijskih sustava ima zadatak provesti testiranje učinkovitosti tih kontrola, sakupiti relevantne argumente i dokaze kako bi se procijenili potencijalni rizici za poslovanje.[27] Cilj je predstaviti preporuke za smanjenje tih rizika kako bi sustav bio siguran i pouzdan. „Dakle, sigurnost informacijskih sustava, se ostvaruje osmišljavanjem i provedbom kontrola kojima se sprječavaju neželjeni događaji.“[28]

[26] Kovač, D. (2021.), Ulaganje u kibernetičku sigurnost. Zbornik radova veleučilišta u Šibeniku, 15 (1-2), str. 61-73.
[27] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[28] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, Zagreb

Najvažnija obilježja prijetnji i napada na podatke, opremu i aplikacije su napadi usmjereni na krađu identiteta korisnika u koje spadaju phishing, skimming, društveni inženjering, keystroke loggers, lažno predstavljanje i slično te napadi osmišljeni s ciljem krađe podataka i izmjene sadržaja u koje spada prisluškivanje, nasilni i neovlašteni upadi u računalne mreže, presretanje poruka i izmjena sadržaja, zlonamjerni računalni kod. (Spremić, 2017)

Zaštitni mehanizmi kao što je već navedeno imaju važnu ulogu kada je riječ o digitalizaciji, digitalnoj transformaciji te informacijskim sustavima u poslovanju. Kako bi se zaštitili od mogućih napada potrebno je provjeravati izvor e-maila te osvijestiti zaposlenike o važnosti praćenja izvora i ne otvaranja sumnjivih e-mailova. Najbolji način bio bi korištenje barem jednog standarda za provjeru autentičnosti e-pošte kao na primjer protokol *DomainKeys Identified Mail* (DKIM). Ovaj protokol omogućuje blokiranje svih poruka koje nisu kriptografski potpisane.[29] Osim toga redovito ažuriranje i izmjena lozinki još je jedan od načina prevencije kako ne bi došlo do napada. Kada je riječ o lozinkama, napadači i u ovoj sferi imaju dobre temelje. Raznim programima nastoje probiti lozinku kako bi dobili pristup podacima. Neke od vrsta napada na lozinke su napadi grubom silom, rječnikom i keylogger napadi međutim postavljanje jakih lozinki u koje spadaju interpunkcijski znakovi, brojevi te velika i mala slova u kombinaciji napadače dovodi u situaciju gdje će za probijanje lozinke ipak trebati utrošiti malo više napora. Važno je i individualno korištenje lozinke odnosno ne dijeljenje lozinke između više osoba naročito unutar neke organizacije. Aktiviranje dvofaktorske autentifikacije pruža dodatni sloj sigurnosti. Osim unosa korisničkog imena i lozinke, dvofaktorska autentifikacija zahtijeva dodatnu provjeru, poput jednokratnog koda poslanog putem SMS-a ili upotrebe aplikacije za generiranje koda.

Povjerljivost kao jedno od svojstava informacija čije narušavanje dovodi do rizika ima karakteristiku da njome raspolažu isključivo osobe koje imaju ovlaštenje za to. Narušavanjem povjerljivosti dolazi do posljedica kao što su gubitak konkurentske prednosti ali i gubitak povjerenja klijenata te financijski gubitci. Curenjem osobnih podataka klijenata krši se regulativa u području zaštite osobnih podataka što zapravo znači da se na taj način ne poštuju mjerodavni

[29] Gillis, A.S. (2020). What is cyber hygiene and why is it important?, Techtarget pristupljeno 26.04.2023. preuzeto s: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

propisi. Integritet ili cjelovitost kao drugo svojstvo informacija čije narušavanje dovodi do rizika ima karakteristiku da postoji razmjerno uvjerenje u njezinu točnost. Donošenjem pogrešnih poslovnih odluka te gubitkom povjerenja klijenta kao i nepoštivanjem mjerodavnih propisa krši se svojstvo cjelovitosti odnosno dolazi do narušavanja tog svojstva. Metodom šifriranja podataka, sigurnosnim protokolima za prijenos podataka kao što su https, ssl, end-to-end šifriranje itd ostvaruje se svojstvo integriteta. Dostupnost kao svojstvo informacije da po potrebi i u određenom roku bude dostupna ovlaštenim osobama narušava se kada dolazi do nemogućnosti isporučivanja proizvoda i usluga, prilikom nepoštivanja mjerodavnih propisa te ne ispunjavanjem ugovornih obveza.

Sigurnosni postupci kao što je redovito ažuriranje operativnih sustava, aplikacija i sigurnosnih zakrpa važni su jer se time popravljaju sigurnosne rupe koje su otkrivene. Nedostatak ažuriranja može rezultirati izloženošću ranjivostima koje napadači mogu iskoristiti. Instalacija i redovito ažuriranje antivirusnog softvera pomaže u otkrivanju i uklanjanju zlonamjernih programa (malwarea) koji mogu ugroziti sigurnost sustava. Antivirusni softver skenira računalo ili mrežu kako bi identificirao i uklonio prijetnje. Također redovno izrađivanje sigurnosne kopije važnih podataka kako bi se zaštitili od gubitka u slučaju napada ili kvara sustava. Sigurnosne kopije trebaju biti pohranjene na sigurnom mjestu i treba provjeriti njihovu ispravnost. Prilikom korištenja javne Wi-Fi mreže, preporuča se korištenje VPN (engl. Virtual Private Network) kako bi se osigurala sigurna i šifrirana veza između korisnikovog uređaja i Interneta. VPN štiti podatke od prisluškivanja i neovlaštenog pristupa. Korištenje sustava za nadzor i praćenje aktivnosti na mreži pomaže prilikom otkrivanja sumnjivih ili neobičnih aktivnosti. To može uključivati praćenje logova sustava, upotrebu softvera za detekciju prijetnji i implementaciju sustava upozorenja. Korištenje vatrozida (engl. firewall), kako na računalu tako i na mrežnoj razini, pomaže u filtriranju i blokiranju neovlaštenog pristupa mreži ili računalu. Obrambeni zidovi (engl. firewall) postavljaju granice između povjerljive interne mreže i nesigurne vanjske mreže.[30]

[30] Umberger H., Gheorghe A. (2011). Cyber Security: Threat Identification, Risk and Vulnerability Assessment. In: Gheorghe A., Muresan L. (eds) Energy Security. NATO.

3. NAJVAŽNIJI MEHANIZMI ZAŠTITE OD KIBERNETIČKIH NAPADA

3.1. Posljedice kibernetičkih napada

Bez obzira o kojem kibernetičkom napadu je riječ, tko je ciljana skupina i kojeg je intenziteta napad, iza sebe ostavlja različite štetne posljedice. Osim financijskih gubitaka koji su najčešće posljedice napada, ne povjerenje i loša reputacija slijedeći su gubitci koje poduzeće prolazi. Financijski gubitci ne odnose se samo na iznos otkupnine koju je napadač zadao kao uvjet za otključavanje zaključanih datoteka ili povrat ukradenih podataka, a koje je meta napada odlučila iz poštovati u nadi da će napadač vratiti ukradeno. Napadi poput ransomwarea mogu rezultirati enkripcijom ili brisanjem podataka, što može prouzročiti gubitak vrijednih informacija. To može imati ozbiljne posljedice za tvrtke i pojedince. Kibernetički napadi mogu imati i šire društvene i političke posljedice. Napadi na kritičnu infrastrukturu, poput energetskih mreža ili financijskih sustava, mogu utjecati na sigurnost i stabilnost društva.[31] Također, napadi na političke organizacije, vlade ili izborne sustave mogu dovesti do poremećaja političkog procesa ili dovesti u pitanje povjerenje u demokratske institucije. Ne povjerenje koje nastaje između organizacije koja je pretrpjela napad i korisnika njihovih usluga za organizaciju je također financijski gubitak. Njihovi dugogodišnji korisnici odlučuju se za konkurentsko poduzeće u nadi da su tamo njihovi podaci sigurniji. Poduzeće tada dolazi u situaciju da na mnogo teži način i uz jako puno truda dolazi do novih korisnika i vraća povjerenje postojećih. Napadi koji onesposobljavaju mreže, sustave ili usluge mogu uzrokovati prekid rada. Ovo može imati ozbiljne posljedice za organizacije, kao što su gubitak produktivnosti, prekid isporuke usluga i mogući financijski gubici. Naravno da su financijski gubitci najveća posljedica kibernetičkog napada jer osim navedenog poduzeće mora značajan novčani iznos uložiti kako bi osiguralo da se napad ne ponovi. Također i edukacija zaposlenika zahtijeva određene financijske izdatke kao i uloženo vrijeme i trud. Međutim narušena reputacija poduzeća nije nezanemariva posljedica koju kibernetički napad ostavlja iza sebe. Godine truda i rada poduzeće mora uložiti kako bi steklo povjerenje svojih korisnika i na taj način ostvarilo dobru poslovnu reputaciju koju zatim jedan zlonamjerni softver dovede kroz svega par sati na kritičnu razinu. Važno je napomenuti da su posljedice kibernetičkih napada vrlo raznolike i ovise

[31] Spremić, M., Šimunic, A. (2018). Cyber security challenges in digital economy, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, pp. 341-347, IAENG, Hong Kong.

o specifičnostima svakog pojedinog napada. Reakcija na napad, razina pripremljenosti i brza detekcija mogu umanjiti posljedice i pomoći u oporavku nakon napada.

3.2. Vrste i obilježja IT kontrola

Sve veća upotreba informacijske i digitalne tehnologije u kompanijama donosi mnoge poslovne prednosti. Međutim brojni novi rizici kojima je poslovanje izloženo kao i neželjene posljedice koje ono donosi nisu isključeni. Tako rizike intenzivne primjene informacijske tehnologije u obavljanju poslovnih aktivnosti smatramo informatičkim rizicima.[32] Toj vrsti rizika najviše su izložene kompanije koje u svom poslovanju intenzivno koriste suvremene digitalne tehnologije, što ne znači da su ostali korisnici digitalnih tehnologija sigurni od napada.[33] IT kontrole obuhvaćaju skup postupaka, politika i praksi koje organizacija primjenjuje kako bi osigurala zaštitu, integritet i dostupnost svojih informacijskih sustava i podataka. (Spremić, 2017) Ove kontrole osiguravaju da organizacija ima odgovarajuće sigurnosne mjere i mehanizme kako bi se zaštitila od potencijalnih prijetnji i ranjivosti.

Revizija informacijskih sustava igra ključnu ulogu u digitalnom poslovanju. To je proces u kojem se neovisni revizori ili timovi analiziraju informacijske sustave i prakse organizacije kako bi se ocijenila njihova učinkovitost, usklađenost s propisima i standardima, te kako bi se identificirale eventualne slabosti ili rizici. (Spremić, 2017) Revizija pomaže organizacijama da bolje razumiju svoje informacijske sustave i identificiraju područja koja zahtijevaju poboljšanje ili promjene kako bi se osiguralo uspješno i sigurno digitalno poslovanje. Najčešće se radi o procjeni učinkovitosti internih kontrola informacijskog sustava kao sastavnog dijela cjelovitog sustava internih kontrola poslovanja. (Spremić, 2007) Interne kontrole su sustav međusobno povezanih komponenata i postupaka koji se primjenjuju kako bi se sprječavali, otkrivali i otklanjali neželjeni događaji i procesi u organizaciji.[34] To je moguće postići samo ako se kontrole s obzirom na razinu upravljanja ugrade u sve dijelove i na svim razinama funkcioniranja informacijskog sustava. U kontrole s

[32] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb
[33] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, Zagreb
[34] ENISA Threat Landscape (2020). Insider threat preuzeto 20.07.2023. s file:///C:/Users/user/Downloads/ETL2020%20-%20Insider%20Threat%20A4.pdf

obzirom na razine upravljanje spadaju upravljačke kontrole, procesne i opće kontrole te aplikacijske kontrole i kontrole informatičkih servisa. (Spremić, 2007)

Upravljačke kontrole, kontrole su na najvišoj razini upravljanja i ubrajaju se u interne kontrole poslovanja.[35] Odnose se na kontrole provedbe strategije informacijskog sustava, kontrole upravljanja informatikom, kontrole prekida ili otežanog odvijanja kritičnih poslovnih procesa, kontrole procesa financijskog izvještavanja, provedbe sigurnosne politike informacijskih sustava, vođenja informatičkih projekata, kontrole procesa upravljanja rizicima intenzivne primjene informacijskih sustava, kontrole planova ulaganja u informatiku, ustrojavanje i funkcioniranje ključnih tijela zaduženih za upravljanje informatikom i sl. (Spremić, 2007)

Procesne i opće kontrole su kontrole bazirane na razvoj i kupnju poslovnih aplikacija, kontrole instalacije samih aplikacija, kontrole nad podacima koje pojedina aplikacija koristi, kontrole promjena softvera, pristupa programima i podacima te sigurnosne kontrole i kontrole kontinuiteta poslovanja ali i brojne druge kontrole koje podržavaju učinkovite kontrole nad aplikacijama koje su temelj poslovnog procesa. (Spremić, 2007)

U aplikacijske kontrole i kontrole informatičkih servisa (usluga) spadaju brojne kontrole samog poslovnog softvera za prijenos podataka, kontrole opreme nad kojom sustav radi, kontrole funkcioniranja sustava otkrivanja pogrešaka kao i kontrole otkrivanja uzroka informatičkih incidenata i sl.[36] Općenito, kontrole predstavljaju sustav međusobno povezanih komponenti i procesa koji se koriste za sprječavanje, otkrivanje i otklanjanje neželjenih događaja i procesa. U kontekstu informacijskih sustava, te kontrole igraju ključnu ulogu u osiguravanju sigurnosti, pouzdanosti i integriteta podataka, kao i zaštitu od neovlaštenog pristupa i zloupotrebe.

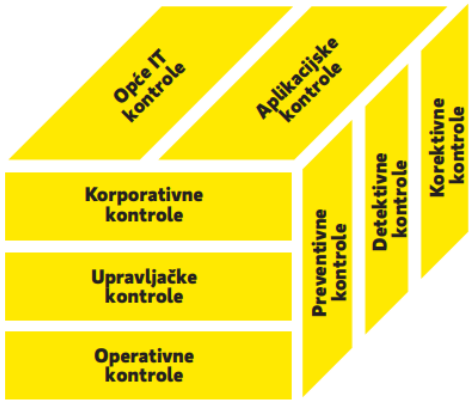
[35] ENISA Threat Landscape (2020). Insider threat. preuzeto 20.07.2023. s file:///C:/Users/user/Downloads/ETL2020%20-%20Insider%20Threat%20A4.pdf
[36] Spremić, M. (2007.), Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta u Zagrebu

Prva vrsta internih kontrola odnosi se na identifikaciju potencijalnih rizika i ranjivosti informacijskih sustava. Ovdje se provodi analiza rizika kako bi se utvrdili prioriteti i razvile odgovarajuće mjere za smanjenje ili eliminaciju identificiranih rizika. Analiza rizika uključuje procjenu potencijalnih prijetnji, ranjivosti i utjecaja koje bi neželjeni događaji mogli imati na organizaciju. Kontrole fizičke sigurnosti su usmjerene na zaštitu fizičkog prostora u kojem se nalaze informacijski sustavi. Ovo uključuje korištenje nadzornih kamera, kontrolu pristupa, zaštitu od požara i prirodnih katastrofa kako bi se osiguralo da samo ovlašteni pojedinci mogu pristupiti tim prostorima i sustavima. Druga vrsta kontrola je usmjerena na upravljanje pristupom. Kontrole pristupa osiguravaju da samo ovlašteni korisnici dobivaju pristup informacijskim sustavima i podacima. Ovo uključuje upravljanje korisničkim računima, upotrebu snažnih lozinki, dvofaktorsku autentifikaciju i praćenje aktivnosti korisnika kako bi se otkrili eventualni neovlašteni pokušaji pristupa.

Kontrole informacijskog sustava mogu se podijeliti i prema načinu djelovanja - preventivne, detektivne i korektivne kontrole. (Spremić, 2017) Preventivne kontrole imaju za cilj predvidjeti neželjeni događaj prije nego što se pojavi, primjenjujući mjere koje sprječavaju moguće propuste. To može uključivati zapošljavanje kvalificirane i obrazovane radne snage, organiziranje nadležnih tijela za nadzor rada informacijskog sustava, edukaciju zaposlenika o važnosti provedbe internih kontrola i revizija, podjelu dužnosti i odgovornosti te donošenje pravilnika o sigurnosnoj politici.[37] Detektivne kontrole koriste se za otkrivanje pogrešaka ili propusta koji su već nastali. To uključuje kontrole unosa podataka, provjeru ovlasti za rad na sustavima, praćenje točnosti rada aplikacija, procesne kontrole i sl.[38] Ovakve kontrole omogućuju organizaciji da brzo reagira i ispravi eventualne pogreške. Korektivne kontrole koriste se kako bi se minimizirao rizik i automatski ispravile identificirane pogreške. Ova vrsta kontrola osmišljena je tako da se prilikom otkrivanja problema automatski izvršava određena instrukcija za ispravak. Na primjer, sustavi automatski mogu pokrenuti sigurnosne protokole i zaštitne mjere u slučaju otkrivanja neovlaštenog pristupa. Slika 4 prikazuje podjelu informacijskih kontrola koje su prethodno bile opisane.

[37] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Ekonomski fakultet Zagreb, Zagreb
[38] Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet Zagreb

Slika 4 Podjela IT kontrola



Izvor: Spremić, M. (2017.), Digitalna transformacija poslovanja, Ekonomski fakultet, Zagreb

Kako bi se utvrdilo jesu li IT kontrole koje se koriste u kompaniji utjecale na smanjenje ključnih rizika i ako jesu u kojoj mjeri su one djelotvorne i učinkovite, provodi se „postupak revizije informacijskih sustava prema CobIT, ISO27000, PCI DSS, NIST“ itd. [39]

CobiT (engl. *Control Objectives for Information and Related Technologies*) je okvir koji se koristi za upravljanje i kontrolu informacijske tehnologije u organizacijama. (Heas, Grembergen, 2013) Razvio ga je ISACA (engl. Information Systems Audit and Control Association) kako bi pomogao organizacijama u postizanju svojih ciljeva putem učinkovitog upravljanja IT resursima. Glavni cilj COBIT-a je pružiti smjernice i strukturu za usklađivanje poslovnih ciljeva s ciljevima informacijske tehnologije. To se postiže identificiranjem ključnih procesa i kontrola te osiguravanjem da IT podržava poslovne zahtjeve, smanjuje rizike, osigurava sigurnost i pruža vrijednost organizaciji.[40]

[39] Spremić, M. (2007.), Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta u Zagrebu
[40] Haes, S., Grembergen, W. (2013) COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems. Vol. 27, No. 1 pp. 307-324 preuzeto s: https://www.researchgate.net/publication/247778781_COBIT_5_and_Enterprise_Governance_of_Information_Technology_Building_Blocks_and_Research_Opportunities

ITIL (engl. Information Technology Infrastructure Library) je okvir najboljih praksi koji se koristi za upravljanje IT uslugama u organizacijama.[41] ITIL pruža sveobuhvatan skup smjernica i postupaka za planiranje, provođenje i upravljanje IT uslugama kako bi se osigurala visoka kvaliteta, efikasnost i prilagodljivost IT procesa. (Kanapathy, Khan, 2012) Njegovi glavni ciljevi su poboljšanje isporuke IT usluga, upravljanje rizicima i troškovima te povećanje zadovoljstva korisnika. ITIL standard je osobito rasprostranjen u Europi, posebno u javnom sektoru, gdje se često koristi kao okvir za planiranje i implementaciju informatičkih usluga. Također cilj ITIL-a je osigurati da organizacije pružaju visokokvalitetne IT usluge koje su usklađene s potrebama korisnika i poslovnim ciljevima. (Kanapathy, Khan, 2012) Središnja ideja ITIL-a je da se IT usluge pružaju putem definiranih procesa koji su optimizirani za postizanje najboljih rezultata. ITIL uključuje niz publikacija koje obuhvaćaju različite aspekte upravljanja IT uslugama, uključujući upravljanje incidentima, problemima, promjenama, konfiguracijom, kapacitetom, kontinuitetom poslovanja i drugim važnim procesima. (Kanapathy, Khan, 2012) Ovaj standard također naglašava važnost kontinuiranog poboljšanja i prilagodbe IT usluga kako bi se zadovoljile promjenjive potrebe korisnika i organizacije. ITIL pristup je fleksibilan i omogućuje organizacijama da prilagode i primijene preporučene prakse u skladu s njihovim specifičnim potrebama i okolnostima. Primjena ITIL-a može donijeti brojne koristi, uključujući poboljšanu efikasnost i učinkovitost, smanjenje rizika i incidenata, bolje upravljanje resursima, veću zadovoljstvo korisnika, i jačanje odnosa između IT odjela i poslovnih jedinica. S obzirom na njegovu široku prihvaćenost i primjenu, ITIL ostaje ključan alat za organizacije koje žele postići visoke standarde u pružanju informatičkih usluga i učinkovito upravljati IT infrastrukturom. Važno je naglasiti da je ISO 20000 jedini važeći standard za upravljanje informatičkim uslugama, ali s obzirom da je on gotovo u potpunosti preuzeo svu ITIL terminologiju, onda i ITIL smatramo standardom.[42]

Sigurnosni standardi serije ISO 27000 koji su osmišljeni kao „obitelj ISO standarda“ daju smjernice za informacijsku sigurnost i predstavlja fizičke i sigurnosne prakse i postupke. ISO/IEC 27001 je sada najpriznatija međunarodna norma za sustave upravljanja informacijskom sigurnošću.

[41] Kanapathy, K., Khan, K. I. (2012) Assessing the relationship between ITIL implementation progress and firm size: evidence from Malaysia. International Journal of Business and Management

[42] Spremić, M., Zmirak, Z., Kraljević, K. (2008). IT and Business Process Performance Management: Case Study of ITIL Implementation in Finance Service Industry. Zbornik radova ITI.

dizajniran da bude kompatibilan i usklađen s drugim priznatim standardima sustava upravljanja. Stoga je idealan za integraciju u postojeće sustave i procese upravljanja. Pruža model za uspostavljanje, implementaciju, rad, praćenje, pregled i poboljšanje upravljanja informacijskom sigurnošću Sustava. Ova norma grupira zahtjeve informacijske sigurnosti u jedanaest kategorija te je svaka kategorija podijeljena u mnogo potkategorija.[43] ISO je s obzirom na uočene nedostatke prošlih normi kao i porast važnosti upravljanja informatikom, proveo reorganizaciju te uveo niz novih normi kao što su ISO 27002, ISO 27003, ISO 27004, ISO 27005.[44]

Osnovni parametri informacijske sigurnosti su povjerljivost, cjelovitost i dostupnost. Povjerljivost u kontekstu da samo ovlašteni pojedinci imaju pristup povjerljivim podacima i informacijama. Tehnikom šifriranja za zaštitu podataka nastoji se napadačima onemogućiti dešifriranje bitnih informacija ako i dođe do probijanja sustava. (Spremić, 2007) Integritetom ili cjelovitosti želi se osigurati neizmjenjivost podataka, dok dostupnost (raspoloživost) znači da mreža mora biti lako dostupna korisnicima iste što znači da mrežni administrator treba održavati hardver, redovito ga nadograđivati te imati plan prelaska ako dođe do kvara. (Spremić, 2007)

3.3. Pregled primjera kibernetičkih napada

Kao što je već i spomenuto u radu kibernetički napad na Target jedan je od primjera malware napada. Američki trgovački lanac koji je osnovan 1902. godine te koji je bilježio dobre poslovne uspjehe 2013. godine ne razmišljajući da išta može krenuti po zlu, doživljava hakerski napad. Tako je 02. prosinca 2013. godine probijanjem u Targetov informacijski sustav ukradeno 40 milijuna brojeva kreditnih kartica kupaca te preko 70 milijuna adresa, brojeva telefona i brojnih drugih osobnih podataka.[45] Nitko osim tvrtke FireEye koja je i instalirala anti-malware software nije primijetio da se išta neobično događa. Nakon 18 dana Američko ministarstvo pravosuđa obavijestilo je Target o napadu. Kompanija Fazio Mechanical posredovala je između Targeta i

[43] Meriah, I. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards, Vol 160, str. 85-92 preuzeto s: https://www.sciencedirect.com/science/article/pii/S187705091931662X
[44] Spremić, M. (2007.), Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta u Zagrebu
[45] Studija slučaja temelji se na slijedećim izvorima: Corrin, J. (2021). Warnings (& lessons) of the 2013 Target data breach. pristupljeno 19.06.2023. preuzeto s: https://redriver.com/security/target-data-breach

hakera. Navedena kompanija imala je pristup Targetovom sustavu iz razloga što su se oni održavali rashladne sustave odnosno bavili su se online nadzorom temperature u poslovnicama. Kako je Target imao slabo odvojene informacijske sustave, slabo upravljanje pristupom i zastarjele softvere, hakeri su lako prodrli do POS terminala. Tamo su instalirali zlonamjerni softver (malware) koji im je omogućio da čitaju i kradu podatke s magnetnih traka kreditnih kartica. Podatke su prikupili pomoću „RAM scraping" procesa (engl. *Random Access Memory scraping*), a to je oblik pohrane računalnih podataka kojeg koriste sustavi na prodajnom mjestu. Prvih nekoliko dana trajalo je testiranje malware. Nakon pozitivnih rezultata instaliran je na većini preostalih prodajnih mjesta preko redovite nadogradnje POS terminala. Glavni cilj hakerskog napada na osobne podatke bio je prodaja na Internetu preko hakerskih stranica, nakon čega bi se podaci pretvarali u fizičke kartice koje se mogu prodati na crnom tržištu. Zbog prespore reakcije Targeta, hakerski plan je i realiziran. Procijenjeno je da je tvrtka oštećena za preko 200 milijuna dolara, te da je zarada pala za 46% nakon napada.[46]

Nakon povrede podataka, Target je izdao *chip-and-pin* kartice koje su predstavljene kao sigurne kartice. (Corrin, 2021) Zaključeno je da sami čipovi nisu dovoljni da osiguraju mnoge kartice te da su kreditne kartice mnogo sigurnije od debitnih kartica. S kreditnim karticama lakše je poništiti transakciju ali i lažna transakcija ne ostavlja pojedinca bez novca.

Kartica "*chip-and-pin*" sama je po sebi mnogo sigurnija jer znači da netko samo sa imenom, brojem kartice i adresom ne može obavljati transakcije. Međutim to nije bilo sveobuhvatno rješenje. Ukradeno je dovoljno podataka da bi identitet potrošača potencijalno mogao biti ugrožen, bez obzira na to jesu li debitne i kreditne kartice bile osigurane. Krađa identiteta može biti puno veći problem od jedne kompromitirane kartice.[47]

[46] Spremić, M. (2017.), Digitalna transformacija poslovanja, Zagreb: Ekonomski fakultet
[47] Corrin, J. (2021). Warnings (& lessons) of the 2013 Target data breach. pristupljeno 19.06.2023. preuzeto s: https://redriver.com/security/target-data-breach

Najveći javno objavljeni kibernetički napad na kritičnu infrastrukturu u SAD-u bio je napad na Colonial Pipeline, američki sustav naftovoda koji potječe iz Houstona. Napad se odvijao u više faza protiv IT sustava, međutim operativni tehnološki sustavi naftovoda čiji je zadatak prenošenje nafte nisu bili izravno ugroženi tijekom napada. Hakerska skupina pod nazivom DarkSide 06. svibnja 2021. godine pristupila je mreži Colonial Pipeline te u roku dva sata ukrala gotovo 100 gigabajta podataka.[48] Nakon uspješne krađe podataka 07. svibnja 2021. instalirali su ransomware koji je utjecao na brojne računalne sustave pa čak i na naplatu i računovodstvo. Kao odgovor na napad, Colonial Pipeline zatvorio je cjevovod na šest dana kako bi zaustavio širenje zloćudnog softvera, a predsjednik Joe Biden proglasio je izvanredno stanje. Zatvaranje cjevovodi utjecalo je na potrošače kao i zrakoplovne tvrtke duž istočne obale. Hakerski napad shvaćen je kao prijetnja nacionalnoj sigurnosti baš zbog toga što naftovod prenosi naftu iz rafinerija na industrijska tržišta. Sjedište Colonial Pipelinea je u Alpharetti, a početak njegovog rada bilježi 1962. godina. Više od 5500 milja cjevovoda koji kreću od Teksasa pa sve do New Jerseya, rafiniranom naftom za benzin, mlaznim gorivom te uljem za kućno grijanje, opskrbljuju gotovo polovicu istočne obale. S toga je zatvaranje cjevovodi dovelo do povećanja prosječnih cijena benzina za 4 centa po galonu u pogođenim područjima. Unutar tjedan dana nakon incidenta, novinske kuće su izvijestile o povećanju cijena benzina za 18-21 cent po galonu u nekim dijelovima zemlje. Također takav potez uvelike je utjecao na zrakoplovnu industriju gdje je došlo do nestašice mlaznog goriva za mnoge prijevoznike. Zbog straha od nestašice goriva mnoge države susrele su se sa dugim redovima na benzinskim crpkama popraćenih paničnom kupnjom u toj mjeri da su se počele benzinom puniti čak i plastične vrećice. Cilj ovog napada bio je traženje otkupnine od 75 bitcoina (tada oko 4,4 milijuna dolara) što je Colonial Pipeline i ispunio kako bi dobio ključ za dešifriranje. Izabrana valuta plaćanja (bitcoin) najčešće je valuta koju hakeri ransomwareom traže iz razloga što su uvjereni da se toj valuti ne može ući u trag. Tadašnji izvršni direktor Joseph Blount objasnio je kako ne zna koliko je napad raširen te koliko će trajati obnova ugroženih sustava te je u nadi da se cijela stvar ubrza uplatio traženu otkupninu. 12. svibnja 2021. godine ponovno pokrenut rad cjevovoda, a već 07. lipnja 2021. godine na konferenciji za novinare rečeno je da se ušlo u trag

[48] Studija slučaja temelji se na slijedećim izvorima: Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget, preuzeto 26.06.2023. s: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, Cvetanov, C. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices, Economics letters. Vol 209, pristupljeno 26.06.2023. preuzeto s: https://www.sciencedirect.com/science/article/abs/pii/S0165176521003992

otkupnini koju je Colonial Pipeline platio. Vraćeno je 64 od 75 bitcoina, međutim s obzirom da je svega nekoliko dana nakon uplate otkupnine vrijednost bitcoina u protuvrijednosti dolara pala, Colonial Pipeline vraćen je dosta manji iznos.

DarkSide poznata je hakerska skupina čija je prva aktivnost prijavljena u kolovozu 2020. godine kao zlonamjerna kampanja zaraze ransomwareom. Smatra se da DarkSide djeluje iz istočne Europe ili Rusije iako nema potvrđene veze s bilo kojom aktivnošću koju sponzorira nacionalna država.[49] Jedan od načina njihovog djelovanja je ransomware-as-a-service (RaaS) kojim se i drugi napadači radije koriste nego da osmisle svoj napad.

Propust u ovom slučaju bio je uporaba zaporke koju je jedan od zaposlenika izgleda koristio i na drugim lokacijama. Napadači su u mrežu ušli preko otkrivene lozinke za račun virtualne privatne mreže (VPN) koji nije imao multifaktorsku autentifikaciju. Ponovna uporaba iste zaporke sve je učestaliji problem kao i ne postojanje drugog koraka prijave kao što je tekstualna poruka. Vlasti su povećale svoju stručnost u praćenju protoka digitalnog novca s obzirom da je ransomware postao sve veća prijetnja nacionalnoj sigurnosti.

WannaCry (WCRY) ransomware napad bio je jedan od najpoznatijih i najraširenijih kibernetičkih napada u povijesti. 12. svibnja 2017. proširio preko računala s operacijskim sustavom Microsoft Windows na oko 230.000 računala u preko 150 zemalja. Riječ je o ransomware crvu koji napada Windows računala te se širi preko mreže, a kada se nađe na računalu šifrira datoteke. Napad se proširio pomoću EternalBluea, na uređaje koji koriste staru verziju Windows Server Message Block (SMB). Zanimljivo je da ga je prvo otkrila američka Agencija za nacionalnu sigurnost (NSA) prije nego što je stigao do hakerske grupe Shadow Brokers, koja je objavila *exploit* unutar posta na blogerskoj stranici Medium. Jednostavnije rečeno objavljena je metoda kojom su napadači iskoristili ranjivost kako bi napali Windows sustave i na taj način došli do opsjetljivih podataka.

[49] Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget. pristupljeno 26.06.2023. preuzeto s: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Napadači su za početak tražili otkupninu u iznosu od 300 bitcoina kako bi se datoteke otključale, a u slučaju da se iznos ne uplati u nekom kratkom roku otkupnina raste na 600 bitcoina. Ova vrsta napada ne traži od korisnika računala da kliknu na vezu ili otvore zaraženu datoteku dok je to slučaj kod phishing napada. Pogođene su bile brojne industrije, a samo neke od njih su zdravstvo, hitna pomoć, sigurnost, logistika, telekom, plin, benzin, automobilizam, obrazovanje te oglašavanje. Značajne žrtve bile su FedEx, Honda, Nissan i Nacionalna zdravstvena služba Ujedinjenog Kraljevstva (NHS). Svega nekoliko sati nakon napada, WannaCry privremeno je neutraliziran. Britanski istraživač sigurnosti Marcus Hutchins otkrio je "kill switch" koji je u biti isključio zlonamjerni softver te zaustavio širenje virusa. Međutim, mnoga pogođena računala ostala su šifrirana i neupotrebljiva sve dok žrtve nisu platile otkupninu ili nisu uspjele poništiti enkripciju. Svega nekoliko mjeseci nakon napada WannaCry, FBI uhitio je Marcusa Hutchinsa u Las Vegasu zbog stvaranja i prodavanja vlastitog zlonamjernog softvera konkretno Kronosa, vrste zlonamjernog softvera za bankarstvo. Zahvaljujući Hutchinsu, WannaCry verzija puštena 2017. više ne funkcionira, međutim napadi se i dalje događaju. Instaliranje najnovijeg softvera moglo je spriječiti WannaCry napad. Nažalost u manjem broju su tvrtke i pojedinci koji su ažurirali svoj Windows softver koji je pušten svega dva mjeseca prije napada. Izrada sigurnosnih kopija neophodna je za zaštitu podataka. Ista bi trebala biti pohranjena izvan poslovne mreže kako bi bila zaštićena od potencijalnih napada. Veliku ulogu igra i odluka o kibernetičkoj sigurnosti posebice u današnje vrijeme kada veliki broj radnika radi na daljinu kao i svijest o opasnosti otvaranja nepoznatih privitaka koji se nalaze u e-pošti.

4. ISTRAŽIVANJE IZDVOJENIH STUDIJA SLUČAJA KIBERNETIČKIH NAPADA

4.1. Svrha i cilj istraživanja

Istraživanjem triju izdvojenih studija slučaja kibernetičkih napada uspoređeni su načini na koji napadači ostvaruju svoj cilj, kao i odgovor na napad koji je pojedino poduzeće pretrpjelo. Osim toga provedena je usporedba uzroka kibernetičkih napada na temelju promatranih studija slučaja. U prethodnim poglavljima predstavljen je napad na sigurnosni sustav maloprodajnog lanca Target kao i kibernetički napad na američki sustav naftovoda Colonial Pipeline te WannaCry ransomware crv koji napada Windows računala te se širi preko mreže. U narednim poglavljima isti napadi analizirani su na temelju čega je i provedena diskusija o načinima na koji je poduzeće trebalo postupati kako do napada ne bi ni došlo. Također predložena su rješenja za poboljšanje mjera sigurnosti kako bi se izbjegli potencijalni kibernetički napadi i kako bi poduzeća mirno i sigurno obavljala svoje poslovne obaveze. Raspravljene su i promjene i poboljšanja koja je poduzeće uvelo nakon pretrpljenog napada. U kojoj mjeri te promjene utječu na poboljšanje poslovanja te donose li financijsku korist i sigurnost za buduće poslovanje poduzeća.

4.2. Objašnjenje metodologije istraživanja i odabira studija slučaja

Usporedbom triju izdvojenih studija slučaja dolazi se do rezultata da je u sva tri slučaja cilj napadača domoći se osobnih (osjetljivih) podataka korisnika kako bi se izvukla financijska korist. U slučaju napada na Colonial Pipeline kao i kibernetički napad WannaCry napadači su tražili otkupninu u bitcoinima iz razloga što su uvjereni da je to valuta kojoj se ne može ući u trag. Kod probijanja sigurnosnog sustava poduzeća Target ukradeni su podaci s magnetnih traka kreditnih kartica pomoću POS uređaja. Na taj način napadači nisu ni morali tražiti otkupninu jer su direktno dolazili do novca preko POS terminala na koji je i bio instaliran malware. Target na taj napad odgovara nakon 18 dana instaliranjem anti-malware softvera od strane tvrtke FireEye, dok Colonial Pipeline kao odgovor na napad zatvara cjevovod na šest dana kako bi zaustavio širenje zloćudnog softvera. Zatvaranje cjevovodi utjecalo je na potrošače kao i zrakoplovne tvrtke duž istočne obale. Potrošači su se uputili prema benzinskim crpkama gdje su gorivo sipali čak u plastične vrećice kako bi osigurali još jedan dan više za odlazak na posao automobilom. Takva reakcija potrošača utječe na povećanje cijena goriva za čak 18-21 cent po galonu. Britanski istraživač sigurnosti

Marcus Hutchins zaslužan je za isključivanje zlonamjernog softvera WannaCry, tehnikom „kill switch“ te na taj način zaustavlja širenje virusa. Međutim, mnoga pogođena računala ostala su šifrirana i neupotrebljiva sve dok žrtve nisu platile otkupninu ili nisu uspjele poništiti enkripciju.

Mehanizmi za zaštitu osjetljivih podataka kao i razne mjere sigurnosti, edukacija zaposlenika o važnosti sigurnosnih mjera te načina postupanja u slučaju sumnjivih radnji postupci su koji se navode u brojnim izvorima dostupne literature kako bi se izbjegla mogućnost kibernetičkog napada.[50] Međutim u izabranim studijima slučajeva nije riječ samo o tome. Istraživanjem se dolazi do zaključka da su u slučaju hakerskog napada na Target djelatnicima dodijeljene prekomjerne role koje izgleda nisu donijele prednost poduzeću. Osim toga problem su bile i iste lozinke koje je koristilo više djelatnika te ne segmentacija mreže. Kada bi svaki korisnik imao svoju jedinstvenu lozinku koju bi samo on znao, te kada bi ta lozinka bila sačinjena od velikih i malih slova, brojeva te nekog interpunkcijskog znaka vjerojatnost kibernetičkog napada pala bi na minimum. To ne znači da bi se poduzeće na taj način sto posto zaštitilo od napada nego bi takav sigurnosni oblik otežao hakerski napad i vrlo vjerojatno napadača motivirao na napad na neko drugo poduzeće koje ima slabiji sigurnosni sustav. Osim toga multifaktorska autentifikacija također je dobar izbor sigurnosnog mehanizma. S obzirom na sve veću inovativnost i kreativnost napadača, redovita edukacija djelatnika još je jedan plus kada je riječ o postupcima sprječavanja kibernetičkog napada. Redovito ažuriranje softvera također utječe na sprječavanje napada što je konkretno bio slučaj sa WannaCry napadom. Windowsovi korisnici koji nisu na vrijeme obavili ažuriranje bili su žrtve napada, a nažalost bilo ih je 230.000.

Kao što je prethodno i navedeno poduzeća su različito reagirala na sami napad. Target je na primjer shvatio da je do napada došlo tek nakon 18 dana te ga je o tome obavijestilo Američko ministarstvo pravosuđa. U ovom slučaju dovoljno je bilo instalirati anti-malware softver kako bi se napad prekinuo. WannaCry napad primjer je napada koji je zaustavljen svega 2 sata kasnije, međutim i dalje su ostala zaključana računala korisnika koji nisu na vrijeme ažurirali novu verziju Windows softvera. Izvršni direktor Colonial Pipelinea Joseph Blount odlučio se za plaćanje otkupnine u

[50] Arbanas K., Spremić M., Zajdela Hrustek N., (2021). Holistic framework for evaluating and improving information security culture, Aslib Journal of Information Management, Vol. 73 No. 5, pp. 699-719, Emerald Publishing.

iznosu od 75 bitcoina uvjeren da će na taj način napadači vratiti ukradene podatke i da će se problem riješiti. Stručnjaci savjetuju da se napadačima nikada ne plaća otkupnina jer ona ne jamči da će oni ukradene podatke i vratiti. Osim toga plaćanjem otkupnine daje se vjetar u leđa napadaču da ponovi svoj napad kao i ostalim potencijalnim napadačima da učine isto. Tako se samo potiče još veći broj napada kao i kreativnost napadača.

4.3. Usporedba rezultata istraživanja i diskusija

Promatrajući Target koji se 2013. godine bori s malwareom te ga uspoređujući sa WannaCry crvom i ransomware napadom na Colonial Pipeline koji se dogodio 2021. godine dolazi se do zaključka da je jedino cilj napadača isti. Ne zakonit način na koji napadači dolaze do financijskih sredstava napadnutih poduzeća sve je kreativniji i opasniji. Iako se radi o različitim sektorima postoje neki ključni elementi koji se mogu usporediti. Tablica 1 prikazuje usporedbu nekih elemenata napada na poduzeća kako bi se donijeli zaključci o izvorima, uzrocima i posljedicama koji isti ostavljaju.

Tablica 1 usporedba triju pretrpljenih kibernetičkih napada

	TARGET	**COLONIAL PIPELINE**	**WANNACRY**
vrsta (oblik) kibernetičkog napada	malware	ransomware	ransomware
cilj napadača	financijska korist	financijska korist	financijska korist
ciljani sektor	Sektor maloprodaje	Sektor energetike	Širi raspon organizacija, privatni i javni sektor
datum napada	02. prosinac 2013.	07. svibnja 2021.	12. svibnja 2017.
posljedice napada	preko 200 milijuna USD, pad profita za 46%	vraćeno 64 od 75 bitcoina kojima je u međuvremenu smanjena vrijednost	zahvaćeno 230.000 računala u preko 150 zemalja

osnovna obilježja	ukradeno 40 milijuna brojeva kreditnih kartica, preko 70 milijuna adresa, brojeva telefona i dr. osobnih podataka	ukradeno 100 gigabajta podataka, kao odgovor na napad Colonial Pipeline zatvara cjevovod na 6 dana	pogođene brojne industrije (obrazovanje, zdravstvo, automobilizam…), virus se ne širi pritiskom na link kao što je slučaj kod phishing napada
rješenje problema	instaliran anti-malware	plaćena otkupnina kako bi se došlo do ključa za dešifriranje	otkriven "kill switch" koji je zaustavio širenje virusa
propusti koji su uzrokovali napad	loše odvojeni informacijski sustavi, loš sustav autorizacije, zastarjeli softveri, ne educirani zaposlenici	uporaba iste lozinke, nema multifaktorske autentifikacije	neredovito ažuriranje softvera, loš mehanizam kibernetičke sigurnosti
iznos tražene otkupnine	nema podatka o traženju otkupnine, krađa putem POS-a	75 bitcoina (4,4 milijuna dolara)	300 bitcoina u početku, kasnije 600 bitcoina
uvedena poboljšanja nakon pretrpljenog napada	sigurnije chip-and-pin kartice, kupci radije plaćaju kreditnim karticama jer je lakše poništiti transakciju	Bidenova administracija izdala je naredbu korištenja softverskog popisa materijala (SBOM)	Windows izdaje niz zakrpa koje su popravile ranjivost SMB-a, međutim to ne pomaže već zaraženim uređajima

Izvor: izrada autora

Kao što je prethodno navedeno primarni cilj napadača na osjetljive podatke te krađa istih bio je financijska korist. Izvori kojim napadači dolaze do osjetljivih podataka različiti su sve ovisno o razini sigurnosti koju pojedino poduzeće primjenjuje kako bi onemogućilo nezakonito probijanje do njih. Također različiti su i načini na koje poduzeća reagiraju na napad i mjere koje poduzimaju kako bi riješile problem koji je nastao.

Uspoređujući Target i Colonial Pipeline vidljivo je da su u oba napada zlonamjerni napadači koristili sofisticirane tehnike i zlonamjerni softver kako bi izvršili napad. U slučaju Targeta, napadači su koristili phishing e-poštu, RAM scraping malware i presretanje podataka o kreditnim karticama. Napad na Colonial Pipeline uključivao je ransomware napad, u kojem su napadači blokirali pristup i šifrirali podatke sustava kako bi iznudili otkupninu. WannaCry napad kombinirao je ransomware i širenje kroz mrežu. Ako promotrimo sektore koji su napadnuti i to kroz godine možemo zaključiti da je 2013. godine ciljan maloprodajni sektor, zatim privatni i javni sektor odnosno širi raspon organizacija (2017.), a 2021. godine sektor energetike, dakle napadi su iz godine u godinu usmjereni na sve veće i jače grane gospodarstva.

Koliko god napad trajao, iza sebe ostavlja brojne posljedice kako za pojedinca tako i za poduzeće. Poučena lošim iskustvom poduzeća se odlučuju na uvođenje promjena kako bi buduće kibernetičke napada spriječili na vrijeme. Napad na Target potaknuo je tvrtku da uloži napore u poboljšanje sigurnosti i suradnju s vlastima. Osim toga Target smatra da je uvođenje sigurnijih chip-and-pin kartica pravo rješenje za to, dok njihovi kupci radije plaćaju kreditnim karticama jer smatraju da je lakše poništiti takvu transakciju. Uvođenjem ove vrste promjena u poduzeće zasigurno se ulaže u sigurnost kada su u pitanju konkretno transakcije. Postavlja se pitanje koliko Target ulaže u druge oblike sigurnosti jer napadači koji su uspjeli doprijeti do podataka putem POS uređaja nekog poduzeća, zasigurno će doći u napast pokušati napasti poduzeće i na neki drugi način a naročito ako se prethodni napad financijski isplatio. Koliko god ulaganje u sigurnost poduzeća zvuči financijski neisplativo ili nepotrebno a posebno nakon pretrpljenog napada razmišljajući kako se zasigurno isto neće ponoviti, promatrajući poduzeće dugoročno ono je od velike važnosti. Kibernetički napadi imaju različite oblike i dimenzije s toga je svijest o sigurnosti a posebno između zaposlenika i ulaganje u njihovo educiranje kako bi djelatnici znali poduzeti sigurnosne mjere, za poduzeće vrlo važno. Napad na Colonial Pipeline doveo je do intenzivne suradnje između vlade i privatnog sektora u rješavanju krize opskrbe gorivom. Navedeni napad podigao je na noge predsjednika Joe Bidena čija je administracija izdala naredbu korištenja softverskog popisa materijala (SBOM). Riječ je o nomenklaturi na temelju koje će korisnici nekog softvera znati koliko je taj softver siguran za korištenje. Slično je kao i popis sastojaka koji se nalazi na pakiranju nekog proizvoda gdje osobe koje su alergične na neki sastojak mogu znati da određeni proizvod

sadrži baš taj sastojak te odlučuju koristiti ga ili ne. Uvedena promjena ne garantira niti proizvođačima niti kupcima nekog softvera da se napad neće dogoditi i da je isti siguran. S obzirom da mjere sigurnosti nikada neće biti 100%-tne i da napadači uvijek idu u korak s napretkom tehnologije, kakve god promjene da poduzeće uvede i razine sigurnosti ako isti nisu oprezni najviše u onim rutinskim poslovnim aktivnostima za poduzeće postoji rizik od kibernetičkog napada. WannCry napad potaknuo je međunarodnu suradnju u dijeljenju informacija i razvoju sigurnosnih alata za borbu protiv ransomwarea.

Unatoč različitim sektorima ciljanja i metodama napada, ovi napadi dijele neke ključne elemente, uključujući štetne posljedice, potrebu za jačom kibernetičkom sigurnošću, suradnju između sektora i država te podizanje svijesti o kibernetičkim prijetnjama. Oni također ističu važnost pripreme, otpornosti i odgovora na kibernetičke napade kako bi se smanjile posljedice i zaštitila kritična infrastruktura. Iako postoje sličnosti između uspoređivanih napada, važno je napomenuti da je svaki kibernetički napad jedinstven i da se odvijaju u specifičnom kontekstu organizacije ili sektora. Svaki napad zahtijeva prilagođene mjere sigurnosti i odgovore kako bi se minimizirali rizici i ublažile posljedice.

4.4. Preporuke za poboljšanje kontrola

Osim analiziranih studija slučajeva brojni su primjeri kibernetičkih napada koji kao sredstvo koriste e-mail. Pokazalo se da je phishing napad najčešći oblik kibernetičkog napada s obzirom da je mail postao najčešći kanal komunikacije u poslovnom svijetu. Po primjeru primljenih mail poruka poslovnih partnera, hakeri šalju link poveznicu koja korisnika vodi na web stranicu partnera, a zapravo sadrži zlonamjerni softver. Također jedan od češćih oblika je poruka koja sadrži novi broj računa na koji je potrebno izvršiti plaćanje. Bez obzira na sustav zaštite i automatsko slanje takvih oblika poruka u *spam,* neke svejedno nađu put do chat-a korisnika maila. Takve (sumnjive) e-mail poruke bilo bi dobro telefonski provjeriti s poslovnim partnerom da se utvrdi jeli ih zaista on poslao. Baš zbog toga što zaposlenici najčešće nisu dovoljno informirani i educirani kako bi znali uopće što je kibernetički napad te kakve posljedice ostavlja na poduzeće, napadači znaju da su im šanse za uspješan rezultat isplaniranog napada velike. Iako su zaposlenici važna karika, ostali ključni

mehanizmi kibernetičke sigurnosti odnose se na niz zaštitnih mjera i programa koje bi trebalo uključiti u sustav. Ulaganje u sigurnosni mehanizam bez kvalitetnog promišljanja o kibernetičkoj sigurnosti zapravo je investiranje u vlastitu kibernetičku ranjivost. Naknadne radnje u svrhu zaštite sustava skuplja su rješenja kojima je naposljetku i teže upravljati.

Jedan od načina na koji je moguće spriječiti kibernetički napad, a koji ne zahtijeva neko posebno znanje i iskustvo je postavljanje složenijih zaporki. Zaporke visoke razine sigurnosti su one koje sadrže kombinaciju velikih i malih slova, brojeva te interpunkcijskih znakova. Redovita promjena zaporki također je vrlo korisna taktika jer na taj način ne može doći do situacije da više osoba koristi istu zaporku. Vise faktorska autentifikacija kao što je primjer s korištenjem tokena (TOTP) još je jedan od oblika koji će svakodnevno poslovanje učiniti sigurnijim. Bez obzira radi li se o kibernetičkom napadu, kvaru tvrdog diska ili fizičkoj krađi hardvera, sigurnosna kopija podataka osigurava vraćanje podataka na uređaj korisnika. Najčešći način sigurnosnog kopiranja podataka je korištenje oblaka. Danas svaki mobilni uređaj dolazi s besplatnim pristupom oblaku s kapacitetom od 5 do 50 gigabajta, dok osobna računala s Windows 10 sustavom imaju mogućnost registriranja na Microsoft račun kako bi se dobio pristup OneDrive oblaku. Prednost ovog oblika sigurnosti podataka krije se u odabiru korisnika hoće li koristiti besplatni oblik s manje gigabajta ili će platiti veću količinu kako bi pohranio sve važne podatke. Također enkripcija podataka, kompatibilnost između računala i mobilnog uređaja kao i različita fizička lokacija naspram korisničkog računa primamljive su prednosti za korisnike. Međutim ovakav oblik sigurnosti podataka nosi nedostatak koji se krije u cijeni. Korisniku kojem je potreban veći kapacitet jeftinije je kupiti eksterni tvrdi disk.

Poduzeća koja nemaju dovoljno znanja o važnosti sigurnosnih mehanizama i općenito posljedicama koje uzrokuje takva vrsta napada najčešće angažiraju tvrtku koja se time bave te njoj prepuste brigu oko sigurnosti svog poslovanja. Neka poduzeća smatraju da je angažiranje tvrtke koja će se baviti informacijskom sigurnosti samo trošak za poslovanje. Tada bi bilo dobro barem instalirati top security antivirusni softver i endpoint zaštitu te redovito provoditi ažuriranje softvera kako bi se rizik kibernetičkog napada barem malo smanjio. Briga o redovitom provođenju ažuriranja nad operacijskim sustavima kao i antivirusnim softverima pomaže pri zaustavljanju

novijih vrsta kibernetičkih napada. Većina uređaja pruža mogućnost odabira vremena ažuriranja. Tako je korisnicima omogućeno da sami postave vrijeme ažuriranja, točno ono vrijeme koje njima najviše odgovara. Važno je ne ignorirati dostupna ažuriranja iz razloga što ona dolaze sa zakrpama te na taj način štite podatke od novih oblika kibernetičkih napada. Postavljanjem vatrozida čiji je zadatak nadgledati cijeli mrežni promet te blokirati neželjeni sadržaj, štiti se računalo korisnika od napadača ili drugog vanjskog utjecaja čiji je cilj dobiti pristup osobnom računalu.

Osim radnji koje poduzeće i pojedinci mogu poduzeti kako do napada ne bi došlo, važno je naglasiti i koje radnje bi trebalo poduzeti ako ipak dođe do neželjenog događaja. Prvi korak je identifikacija zlonamjernog softvera. Zatim slijedi analiza i procjena pogođenih strana kao i datoteka koje su ugrožene. Na samom kraju potrebno je cijeli sustav tretirati kako bi se isti mogao vratiti u prvobitno radno stanje bez dodatnog narušavanja sigurnosti. To se u glavnom odvija izračunavanjem čimbenika ranjivosti, prijetnji i rizika. Ranjivost je tada situacija koju napadač može iskoristiti, prijetnja predstavlja novi incident koji može naštetiti sustavu dok rizik počiva na potencijalnoj šteti koja nastaje kada prijetnja iskoristi ranjivost, odnosno moguće ga je definirati kao prijetnja pomnožena s ranjivošću. Rizik je moguće smanjiti stvaranjem i primjenom plana upravljanja rizikom koji sadrži ključne aspekte koji je potrebno uzeti u obzir prilikom izrade strategije. Za početak je potrebno procijeniti rizike i odrediti potrebe. Od ključne je važnosti odrediti najvažnije napade koji će se adresirati prvi.[51] Plan odaziva određuje koje je radnje potrebno poduzeti i tko iz poduzima u trenutku kibernetičkog napada. Kvalitetan plan odaziva omogućuje brzo djelovanje ali i smanjuje količinu učinjene štete. Takvi planovi većinom su usmjereni na tehnologiju i rješavanje problema kao što su krađa osobnih i osjetljivih podataka, otkrivanje zlonamjernog softvera i distribuiranje uskraćivanja usluga. Međutim, o kojoj god vrsti kibernetičkog napada da se radi, on utječe na organizaciju na više načina, tako da bi plan odaziva trebao obuhvaćati i područja kao što su financije, služba za korisnike, dobavljači i partneri, lokalne vlasti i korisnike.[52]

[51] Umberger H., Gheorghe A. (2011). Cyber Security: Threat Identification, Risk and Vulnerability Assessment. In: Gheorghe A., Muresan L. (eds) Energy Security. NATO.

[52] Cisco. What Is an Incident Response Plan for IT?. Preuzeto 11.07.2023. s https://www.cisco.com/c/en/us/products/security/incident-response-plan.html

Unatoč mnogim prednostima digitalne ekonomije, postoji rastući rizik od kibernetičkih prijetnji. Kibernetički sigurnosni incidenti su postali sofisticiraniji i ciljaniji. Napadi, kao što su hakiranje i ransomware, mogu uzrokovati značajne gubitke tvrtkama, uključujući financijske i reputacijske posljedice. Svjetski ekonomski forum identificirao je kibernetičku sigurnost kao jedan od pet najozbiljnijih rizika s kojima se svijet suočava.[53] Za upravljanje kibernetičkim rizicima, organizacije moraju primijeniti sveobuhvatan pristup. To uključuje implementaciju osnovnih i naprednih sigurnosnih kontrola kako bi se otkrile i spriječile različite razine prijetnji. Kibernetičke sigurnosne kontrole trebaju se kontinuirano procjenjivati kako bi se osigurala njihova učinkovitost. Preliminarno istraživanje provedeno u devet velikih tvrtki u Hrvatskoj povezanih s važnom nacionalnom infrastrukturom pokazalo je da su organizacije usvojile odgovarajuće sigurnosne prakse i imaju odgovorne osobe specijalizirane za kibernetičku sigurnost. (Spremić, Šimunic, 2018) Većina njih redovito izvještava izvršne razine o stanju kibernetičke sigurnosti. Kako bi se izbjegle kibernetičke prijetnje, organizacije moraju konstantno pratiti i primjenjivati nove sigurnosne metode, jer su napadači uvijek u potrazi za novim ranjivostima. Kibernetička sigurnost postaje ključna za očuvanje povjerenja kupaca, održavanje konkurentne pozicije i zaštitu kritičnih nacionalnih interesa. (Spremić, Šimunic, 2018)

[53] Spremić, M., Šimunic, A. (2018). Cyber security challenges in digital economy, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, pp. 341-347, IAENG, Hong Kong.

5. ZAKLJUČAK

Digitalnom transformacijom poslovanja posljednjih godina naročito ubrzanom pojavom pandemije Covid-19 vrtoglavom brzinom razvija se i ona lošija strana koju navedena digitalizacija donosi. Pojednostavljenjem obavljanja svakodnevnih poslovnih aktivnosti te otvaranjem mogućnosti rada na daljinu kao i ostalim prednostima koje donosi digitalizacija, opasnost od različitih oblika napada na osobne podatke prisutna je u sve većoj mjeri. Neinformiranost o vrstama, načinima i oblicima napada na osjetljive podatke kao i neulaganje u sigurnost osjetljivih podataka poduzeće svrstava u kategoriju magneta za kibernetički napad, a da toga nije niti svjesno. Prema internetskim podacima čak 95% kibernetičkih napada uzrokovano je ljudskom pogreškom.[54] Cilj ovog rada bio je analizirati izvore, uzroke i posljedice kibernetičkih napada na temelju iscrpne analize studija slučaja. Odabrana poduzeća temeljem kojih je provedeno istraživanje su Target, Colonial Pipeline i ransomware napad WannaCry koji je zarazio oko 230.000 računala te tako utjecao na zdravstvo, automobilizam i sl. Posljedice koje kibernetički napadi ostavljaju na napadnuta poduzeća nisu samo financijske prirode već i narušavanje reputacije, nepovjerenje korisnika te pad profita kao i dodatne financijske izdatke kako bi se spriječili budući napadi. Promatrani napadi imaju različite izvore kojim su se napadači koristili kako bi došli do osjetljivih podataka. Tako malware napad na Targetov informacijski sustav kao sredstvo za napad koristi POS uređaj, dok je WannaCry iskoristio propuste koje je Windows imao prije puštanja zakrpa koje oko 230.000 korisnika nije ažuriralo na svoja računala. Sve to moglo se spriječiti da su poduzeća ulagala u mehanizme za zaštitu informacijskih sustava. Edukacija zaposlenika o važnosti pridržavanja sigurnosnih mjera kao i način reagiranja u slučaju uočavanja pokušaja napada jedna je od važnijih metoda za sprječavanje kibernetičkog napada.[55] Uz to korištenje kvalitetnih lozinki kao i više faktorska autentifikacija povećavaju razinu sigurnosti osjetljivih podataka jer je takve lozinke teško probiti. Kibernetički napad dodatno otežava povremeno mijenjanje lozinki kao i praksa da svaki korisnik ima svoju jedinstvenu lozinku koju samo on zna. Vatrozid čiji je zadatak nadgledati cijeli mrežni promet te blokirati neželjeni sadržaj, također štiti računalo korisnika od napadača ili drugog vanjskog utjecaja. Redovito ažuriranje softvera čija nadogradnja sadrži zakrpe važna je jer ignoriranjem ažuriranja softver postaje meta kibernetičkog napada kao što se dogodilo 2017.

[54] Omazić, I. (2022), Cyber napadi na kompanije: Gdje se krije rizik i kako se zaštititi, preuzeto s: https://capitalia.ba/cyber-napadi-na-kompanije-gdje-se-krije-rizik-i-kako-se-zastititi/

[55] Arbanas K., Spremić M., Zajdela Hrustek N., (2021): Holistic framework for evaluating and improving information security culture, Aslib Journal of Information Management, Vol. 73 No. 5, pp. 699-719, Emerald Publishing.

godine ransomware WannaCry napadom. Antivirusni softver koji je dizajniran da otkrije, prevenira i ukloni različite vrste malware zaraza na računalima i mreži te brojne druge mjere za zaštitu osobnih i povjerljivih podataka ključ su uspješnog i sigurnog digitalnog poslovnog svijeta. Važno je istaknuti da su sigurnosne mjere u pogledu različitih programa, softvera i angažiranja najboljih tvrtki koji se bave tom vrstom osiguranja uzaludni ako se ne ulaže u zaposlenike. Edukacija i osvješćivanje zaposlenika o opasnostima i mogućim štetama koje uzrokuje ne opreznost prilikom otvaranja sumnjivih e-mail poruka može se reći da je najvažnija mjera sigurnosti koju bi svako poduzeće trebalo primjenjivati.

POPIS LITERATURE

1. Arbanas K., Spremić M., Zajdela Hrustek N., (2021): Holistic framework for evaluating and improving information security culture, Aslib Journal of Information Management, Vol. 73 No. 5, pp. 699-719, Emerald Publishing.

2. Bača, M., Ćosić, J. (2013.), Prevencija računalnog kriminaliteta, Policija i sigurnost, 22 (1), preuzeto s: https://policijska-akademija.gov.hr/UserDocsImages/onkd/1-2013/baca_cosic.pdf

3. Bosilj Vukšić, V., Ivančić, L., Spremić, M. (2019). Mastering the Digital Transformation Process: Business Practices and Lessons Learned. Technology Innovation Management Review. preuzeto s: http://doi.org/10.22215/timreview/1217

4. Cisco. What Is an Incident Response Plan for IT?. preuzeto s: https://www.cisco.com/c/en/us/products/security/incident-response-plan.html

5. Corrin, J. (2021). Warnings (& lessons) of the 2013 Target data breach. preuzeto s: https://redriver.com/security/target-data-breach

6. Cvetanov, C. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. Economics letters. Elsevier. Department of Economics, University of Kansas, Lawrence, United States of America. preuzeto s: https://www.sciencedirect.com/science/article/abs/pii/S0165176521003992

7. Derenčinović, D. (2003). Colloquy on Cyber-Crime. Hrvatski ljetopis za kazneno pravo i praksu (Zagreb)

8. Dragičević, D. (2004.), Kompjutorski kriminalitet i informacijski sustavi. Zagreb: IBS.

9. ENISA Threat Landscape (2020). Insider threat. preuzeto s: file:///C:/Users/user/Downloads/ETL2020%20-%20Insider%20Threat%20A4.pdf

10. Europska Unija (2020.), Kibersigurnost u EU-u i njegovim državama članicama. Revizije otpornosti ključnih informacijskih sustava i digitalnih infrastruktura na kibernapade, preuzeto s : https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_HR.pdf

11. Gillis, A.S. (2020). What is cyber hygiene and why is it important?. Techtarget, preuzeto s: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

12. Kazneni zakon, Narodne novine br. 125/11., 144/12., 56/15., 61/15., 101/17., 118/18., 126/19., 84/21. (2023.), preuzeto s: https://www.zakon.hr/z/98/Kazneni-zakon

13. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget. preuzeto s: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

14. Kibernetika (2020.), Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, preuzeto s: https://enciklopedija.hr/natuknica.aspx?id=31381

15. Kovač, D. (2021.), Ulaganje u kibernetičku sigurnost, u: Zlatović, D. (ur.), Zbornik radova veleučilišta u Šibeniku, Šibenik: Veleučilište u Šibeniku

16. Markuš, H. (2022.), Državni zavod za statistiku Republike Hrvatske preuzeto s https://podaci.dzs.hr/2022/hr/29624

17. Meriah, I. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards

18. Miloš Sprčić, D. (2013.), Upravljanje rizicima: temeljni koncepti, strategije i instrumenti, Zagreb, Sinergija

19. Ministarstvo unutarnjih poslova (2015.), Nacionalna staregija kibernetičke sigurnosti, preuzeto s: https://mup.gov.hr/UserDocsImages/minstarstvo/kibernetika/strategija_kibernetika.pdf

20. Ministarstvo vanjskih i europskih poslova (2016.), Kibernetička sigurnost, preuzeto s Republika Hrvatska Ministarstvo vanjskih i europskih poslova https://mvep.gov.hr/vanjska-politika/multilateralni-odnosi/medjunarodna-sigurnost/kiberneticka-sigurnost/22702 /

21. Omazić, I. (2022), Cyber napadi na kompanije: Gdje se krije rizik i kako se zaštititi, preuzeto s: https://capitalia.ba/cyber-napadi-na-kompanije-gdje-se-krije-rizik-i-kako-se-zastititi/

22. Pejić Bach, M., Spremić, M., & Suša Vugec, D. (2018). Integrating Digital Transformation Strategies into Firms: Values, Routes and Best Practice Examples. In Management and Technological Challenges in the Digital Age. Taylor & Francis Group: CRC press. Protrka, N. (2018.), Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru, doktorski rad, Sveučilište u Zadru, Zadar

23. Rouse, M., Operation Phish Phry, preuzeto s: https://searchsecurity.techtarget.com/definition/Operation-Phish-Phry

24. Službeni list Europske unije (2016.), Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Tekst značajan za EGP)., preuzeto s: https://eurlex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=HR

25. Spremić, M. (2007.), Metode provedbe revizije informacijskih sustava, Zbornik Ekonomskog fakulteta u Zagrebu

26. Spremić, M. (2017.), Digitalna transformacija poslovanja, Zagreb: Ekonomski fakultet

27. Spremić, M., Šimunic, A. (2018). Cyber security challenges in digital economy. *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018*, pp. 341-347, IAENG, Hong Kong.

28. Umberger H., Gheorghe A. (2011). Cyber Security: Threat Identification. Risk and Vulnerability Assessment. In: Gheorghe A., Muresan L. (eds) Energy Security. NATO.

29. Vuković, H. (2012.), Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, 13 (3), str. 15, preuzeto s: https://hrcak.srce.hr/100728

POPIS SLIKA

POPIS TABLICA

ŽIVOTOPIS

Ružica Soldo

Datum rođenja: 17. kolovoza 1998. | **Spol:** Žensko | **Državljanstvo**: hrvatsko

Sakrij podatke za kontakt

Mobilni telefon: (+385) 998308112

E-adresa: ruza.soldo25@gmail.com

Kućna: Ivana Vencla 3b, 10290 Zaprešić, Hrvatska

RADNO ISKUSTVO

Prodavačica

Hrvatska lutrija d.o.o.

24. rujna 2017. – 19. veljače 2023.

Zagreb, Hrvatska

Prodaja lutrijskih igara i igara na sreću

Prodaja slastičarskih proizvoda

Slastičarnica Grabar

30. lipnja 2017. – 30. kolovoza 2017.

Zaprešić, Hrvatska

Sezonski posao preko agencije, prodaja slastičarskih proizvoda

Pomoćni knjigovođa

AS FLOOR d.o.o.

20. veljače 2023. – Trenutačno

Samobor, Hrvatska

- odnosi s dobavljačima
- knjiženje IRA i URA
- isplata plaća
- prijava i odjava zaposlenika
- putni nalozi
- administrativni poslovi

OBRAZOVANJE I OSPOSOBLJAVANJE

Ekonomski fakultet Sveučilišta u Zagrebu

Stručna prvostupnica (baccalaurea) ekonomije (bacc. oec.)

02. listopada 2018. – 23. rujna 2021.

Trg Johna F. Kennedyja 6, 10000, Zagreb, Hrvatska | https://www.efzg.unizg.hr/

Srednja škola Ban Josip Jelačić

Ekonomistica

04. srpnja 2013. – 22. svibnja 2017.

Trg dr. Franje Tuđmana 1, 10290, Zaprešić, Hrvatska | http://www.ss-ban-jjelacic-zapresic.skole.hr/index.php?doc=article&docid=11

JEZIČNE VJEŠTINE

Materinski jezik/jezici

hrvatski

Drugi jezici

engleski

Slušanje	B1
Čitanje	B1
Govorna interakcija	A2
Govorna produkcija	A2
Pisanje	A2

DIGITALNE VJEŠTINE

Priprema i oblikovanje prezentacija (MS PowerPoint) | Drutvene mree | Internet | Rad na računalu | izvrsno služenje office paketom | Informacije i komunukacija | Timski rad | MS Office (Word Excel PowerPoint)

osobne vještine

Prilagodljivost | Sposobna raditi u timu | Sposobnost prilagodavanja promjenama | S lakocom prihvacam i rjesavam nove izazove kroz koje napredujem | Komunikativna | Dobro organizirana | Pristupačna i ljubazna