Rizičnost primjene digitalnih tehnologija

Karačić, Matija

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:703896

Rights / Prava: Attribution-NonCommercial-ShareAlike 3.0 Unported / Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 3.0

Download date / Datum preuzimanja: **2024-07-13**

Repository / Repozitorij:

REPEFZG - Digital Repository - Faculty of Economcs & Business Zagreb

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

RIZIČNOST PRIMJENE DIGITALNIH TEHNOLOGIJA

Diplomski rad

Matija Karačić

Zagreb, lipanj 2024.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

RIZIČNOST PRIMJENE DIGITALNIH TEHNOLOGIJA

RISK EXPOSURE OF DIGITAL TECHNOLOGY ADOPTION

Diplomski rad

Student: Matija Karačić

JMBAG studenta: 0066281588

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, lipanj 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

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

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

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

(vlastoručni potpis studenta)

(mjesto i datum)

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

U digitalnom dobu okruženi smo tehnologijom koja je sastavni dio svakodnevnice i poslovanja. Primjenom tih tehnologija uz velik broj mogućnosti koje nam nude, istovremeno stvaraju određene rizike koje nazivamo kibernetičkim rizicima. Rapidan napredak digitalnih tehnologija otvara nove površine napada i ranjivosti u digitalnom okruženju. Povezanost različitih uređaja putem interneta stvari (IoT), raširena upotreba cloud tehnologija i sve veća digitalizacija poslovnih procesa stvaraju kompleksan i povezan ekosustav koji može biti izložen različitim kibernetičkim prijetnjama. Nedostatak adekvatne sigurnosne zaštite i nepravilna implementacija sigurnosnih mjera često su ključni čimbenici koji omogućuju kibernetičke napade. Slučajevi poput krađe lozinki zbog nekriptiranih podataka, zanemarivanje sigurnosnih nadogradnji ili propusta u konfiguraciji mrežnih sustava mogu olakšati pristup napadačima i omogućiti im neovlašteni pristup osjetljivim podacima. Ljudski faktor igra važnu ulogu u kibernetičkim napadima. Napadači često koriste društveno inženjerstvo i phishing tehnike kako bi prevarili korisnike i zaposlenike da otkriju svoje povjerljive informacije ili otvore zlonamjerne datoteke. Nedostatak svijesti o kibernetičkim prijetnjama i nedovoljna obuka osoblja mogu dodatno povećati rizik od uspješnih napada. Organizacije i pojedinci moraju kontinuirano ulagati u sigurnosne nadogradnje, obrazovanje osoblja i implementaciju najboljih praksi kako bi se smanjio rizik od kibernetičkih napada i njihovih štetnih posljedica. Kroz kritičku analizu primjene digitalnih tehnologija na primjerima kibernetičkih napada ukazuje na potrebu za sveobuhvatnim pristupom sigurnosti informacijskih sustava, kontinuiranom edukacijom i suradnjom svih relevantnih dionika kako bi se zajednički suočili s izazovima i zaštitili digitalni svijet od sve sofisticiranijih prijetnji.

Ključne riječi: digitalne tehnologije, kibernetička sigurnost, kibernetički napadi

ABSTRACT

In the digital age, we are surrounded by technology that is an integral part of everyday life and business operations. By employing these technologies, with the multitude of opportunities they offer, we simultaneously create certain risks referred to as cyber risks. The rapid advancement of digital technologies opens up new attack surfaces and vulnerabilities in the digital environment. The interconnectivity of various devices through the Internet of Things (IoT), widespread use of cloud technologies, and increasing digitization of business processes create a complex and interconnected ecosystem that can be exposed to various cyber threats. The lack of adequate security protection and improper implementation of security measures are often key factors enabling cyber attacks. Cases such as password theft due to unencrypted data, neglect of security upgrades, or flaws in network system configuration can facilitate attackers' access and allow them unauthorized access to sensitive data. The human factor plays a significant role in cyber attacks. Attackers often use social engineering and phishing techniques to deceive users and employees into disclosing their confidential information or opening malicious files. Lack of awareness of cyber threats and insufficient staff training can further increase the risk of successful attacks. Organizations and individuals must continuously invest in security upgrades, staff education, and implementation of best practices to reduce the risk of cyber attacks and their harmful consequences. Through critical analysis of the application of digital technologies in examples of cyber attacks, it points to the need for a comprehensive approach to information security, continuous education, and collaboration among all relevant stakeholders to collectively address the challenges and protect the digital world from increasingly sophisticated threats.

Key words: digital technologies, cybersecurity, cyber attacks

SADRŽAJ

1. UVOD ... 1
1.1. Predmet i cilj rada ... 1
1.2. Izvor podataka i metode prikupljanja ... 1
1.3. Sadržaj i struktura rada ... 2
2. OSNOVNA OBILJEŽJA DIGITALNIH TEHNOLOGIJA ... 3
2.1. Što su digitalne tehnologije? ... 3
2.2. Vrste digitalnih tehnologija ... 3
2.3. Važnost i utjecaj digitalne tehnologije ... 4
3. KONCEPT KIBERNETIČKE SIGURNOSTI ... 6
3.1. Definicija kibernetičke sigurnosti ... 6
3.2. Vrste sigurnosnih prijetnji ... 6
3.3. Važnost i rizičnost kibernetičke sigurnosti u digitalnom okruženju ... 11
4. RAZLIČITE ULOGE I RIZICI PRIMJENE DIGITALNIH TEHNOLOGIJA ... 18
4.1. Kako digitalne tehnologije otvaraju nove ranjivosti? ... 18
4.2. Uloga umjetne inteligencije i strojnog učenja u kibernetičkoj sigurnosti ... 20
4.3. Primjeri napada i ranjivosti uzrokovanih digitalnim tehnologijama ... 26
4.3.1. Deepfake ... 27
4.3.2. Medijski sadržaj generiran umjetnom inteligencijom ... 31
4.3.3. Automatiziranje razvojnog procesa ... 33
4.4. Kritička analiza rizičnosti primjene digitalnih tehnologija ... 36
4.4.1. Usporedba rezultata istraživanja i diskusija ... 42
5. ZAKLJUČAK ... 46
POPIS LITERATURE ... 47
POPIS SLIKA ... 53
ŽIVOTOPIS ... 54

1. UVOD

1.1. Predmet i cilj rada

U ovome radu analizirat će se rizičnost primjena digitalnih tehnologija u današnjem digitalnom okruženju s naglaskom na njihove različite uloge i potencijalne opasnosti. U digitalnom dobu okruženi smo tehnologijom koja je sastavni dio svakodnevnice i poslovanja. Primjenom tih tehnologija uz velik broj mogućnosti koje nam nude, istovremeno stvaraju određene rizike koje nazivamo kibernetičkim rizicima. Rad počinje definiranjem i pregledom digitalnih tehnologija. Identificirat će se ključne karakteristike svake tehnologije i njihov potencijalni doprinos poslovnim procesima. Zatim se analizira pojam kibernetičke sigurnosti te važnosti i izazovi u digitalnom okruženju. Kroz rad razmatrat će se uloga tehnologija poput umjetne inteligencije i strojnog učenja u svrhu poboljšanja kibernetičke sigurnosti. Naglasak je stavljen na ranjivosti i rizike koje digitalne tehnologije donose uz nekoliko primjera stvarnih napada.

Prvi cilj rada je pojašnjenje osnovnih pojmova vezanih uz digitalne tehnologije i kibernetičku sigurnost. Iako su pojmovi poput kibernetičke sigurnosti i kibernetičkih napada svepristuni, kroz rad se želi pobliže objasniti kibernetička sigurnost, aspekte koje obuhvaća, što se podrazumijeva pod samim pojmom kibernetičke sigurnosti i koji sve napadi na računalne sustave postoje. Nadalje, cilj rada je i analizirati kako digitalne tehnologije, kao što su umjetna inteligencija, strojno učenje i slične tehnologije, utječu na kibernetičku sigurnost. Istraživanje će obuhvatiti identifikaciju pozitivnih i negativnih utjecaja tih tehnologija na sigurnosne aspekte. Glavni cilj rada je analiza stvarnih napada, odnosno studija slučaja organizacija koje su se suočile s kibernetičkim prijetnjama. Iz analiziranih studija slučajeva će se utvrditi i objasniti na koji način su se dogodili kibernetički napadi. Također se kroz rad želi potaknuti svijest o kibernetičkoj sigurnosti i naglasiti važnost edukacije zaposlenika i korisnika da budu bolje pripremljeni za potencijalne napade. Naglasak je na edukaciji i osvještavanju pojedinaca.

1.2. Izvor podataka i metode prikupljanja

Metode istraživanja koje se koristite su prvobitno istraživanje literature poput knjiga i znanstvenih članaka te drugih izvora koji pružaju teorijski okvir i podatke. Korištene su metode deskripcije i kompilacije, koje uključuju analizu već dostupne literature na predmetnu temu. Osim literature

analiziraju se stvarni incidenti i napadi na organizacije koji pokazuju na rizičnost primjene digitalnih tehnologija. Kroz interpretiranje studija slučajeva stvarnih napada donosit će se određeni zaključci. Jedna od studija slučajeva je slučaj napada na Yahoo koji se odvijao između 2013. i 2014. godine te je proglašen jednim od najvećih napada po broju oštećenih korisničkih računa. U 2018. godini Marriott Hotel doživljava napad u kojem je oštećeno 500 milijuna korisničkih podataka čiji će se uzroci i posljedice razmatrati. Posljednja studija slučaja je napada MOVEit attack koji se dogodio u 2023. godini.

1.3. Sadržaj i struktura rada

Rad se sastoji od pet poglavlja. U uvodu, rad postavlja temelje za istraživanje rasta i primjene digitalnih tehnologija i njihovog značaja za organizacije. U ovom poglavlju, naglasak je na definiranju teme istraživanja i postavljanju cilja rada. U drugom poglavlju su navedena i objašnjena osnovna obilježja digitalnih tehnologija. Također su definirane vrste digitalnih tehnologija i njihove važnosti. Kroz analizu osnovnih obilježja digitalnih tehnologija, poput definicije, vrsta i utjecaja, istražuje se kako te tehnologije otvaraju nove ranjivosti u digitalnom okruženju. U trećem poglavlju tumačimo koncept kibernetičke sigurnosti. Definiramo pojam kibernetičke sigurnosti kao i vrste. Poseban fokus stavljen je na koncept kibernetičke sigurnosti, gdje se definiraju sigurnosne prijetnje i istražuje važnost kibernetičke sigurnosti u zaštiti digitalnih sustava. U trećem poglavlju opisane su važnosti i rizičnosti kibernetičke sigurnosti. U četvrtom poglavlju govori se o različitim ulogama i rizicima primjene digitalnih tehnologija. Opisuje se kako digitalne tehnologije otvaraju nove ranjivosti, koja je uloga umjetne inteligencije i strojnog učenja u kibernetičkoj sigurnosti. U tom poglavlju navedeni su različiti primjeri napada i ranjivosti uzrokovanih digitalnim tehnologijama, uključujući deepfake, generiranje medijskog sadržaja pomoću umjetne inteligencije te automatiziranje razvojnog procesa. Kroz kritičku analizu provedenih napada, razmatraju se rizici primjene digitalnih tehnologija i mogući izazovi s kojima se suočavaju organizacije i društvo u cjelini. Na kraju, u zaključku se sumiraju ključni nalazi i daju se preporuke za bolje razumijevanje i upravljanje rizicima povezanim s digitalnim tehnologijama.

2. OSNOVNA OBILJEŽJA DIGITALNIH TEHNOLOGIJA

2.1. Što su digitalne tehnologije?

Digitalne tehnologije ključan su element infrastrukture digitalne ekonomije. Obuhvaćaju širok spektar digitalnih resursa poput tehnologija, alata, aplikacija i algoritama. Glavni cilj ovih tehnologija je učinkovito pronalaženje, analiziranje, stvaranje, prosljeđivanje i korištenje digitalnih dobara u računalnom okruženju. Također digitalne tehnologije važne su u potpori digitalnoj ekonomiji i imaju ulogu u transformaciji i optimizaciji različitih procesa u modernom društvu (Spremić, 2017.a). Ove tehnologije koriste binarni sustav (nule i jedinice) za obradu, pohranu i prijenos podataka. Digitalne tehnologije postale su neizostavan dio svakodnevnog života, transformirajući način na koji radimo, komuniciramo, zabavljamo se i obavljamo mnoge druge aktivnosti.

Krajem 20. stoljeća, digitalna tehnologija počela je svoj razvoj, označavajući početak značajnih promjena. U 21. stoljeću, ona nas je prenijela iz Treće industrijske revolucije u Četvrtu revoluciju. Ova nova era karakterizirana je naprednim tehnologijama poput umjetne inteligencije, autonomnih vozila (kao što su primjerice vozila tvrtke Tesla), virtualne stvarnosti, 3D printanja i drugih inovacija koje su transformirale način na koji živimo i radimo. [1]

2.2. Vrste digitalnih tehnologija

Digitalne tehnologije možemo podijeliti na primarne i sekundarne. Primarne odnosno temeljne digitalne tehnologije su:[2]

a) mobilne tehnologije (engl. mobile): ovo se odnosi na tehnologije poput pametnih telefona i tableta, koje omogućuju pristup internetu i aplikacijama na pokretnim uređajima
b) društvene mreže (engl. social): platforme poput Facebooka, Twittera, Instagrama i drugih, koje omogućuju ljudima da se povežu, dijele sadržaj i komuniciraju online

[1] CIO White Papers review (2018.), *What is Digital Revolution - Definition and Explained* [online], dostupno na: https://whatis.ciowhitepapersreview.com/definition/digital-revolution/.
[2] Spremić, M. (2017.a), *Digitalna transformacija poslovanja*, Sveučilište u Zagrebu, Ekonomski Fakultet

c) računalstvo u oblaku (engl. cloud): omogućuje pristup računalnim resursima i uslugama putem interneta, bez potrebe za lokalnim hardverom ili infrastrukturom
d) veliki podaci (engl. big data): odnosi se na naprednu analizu i obradu velikih količina raznolikih podataka kako bi se otkrila korisna znanja i informacije
e) senzori i Internet stvari (engl. Internet of Things , IoT): senzori su uređaji koji prikupljaju podatke iz fizičkog okruženja, dok Internet stvari (IoT) omogućuje povezivanje tih uređaja s internetom radi razmjene podataka i upravljanja

Osim ovih temeljnih tehnologija, postoje i sekundarne digitalne tehnologije koje se često koriste. To uključuje tehnologije poput 3D printera, robotike, dronova, nosive tehnologije, virtualne i proširene stvarnosti, umjetne inteligencije i slično.[3] Ove tehnologije omogućuju razvoj brojnih inovativnih usluga i primjena koje nadograđuju digitalno iskustvo i omogućuju nove načine interakcije s tehnologijom (Spremić, 2017.a).

2.3. Važnost i utjecaj digitalne tehnologije

Primjena digitalnih tehnologija ima izuzetno veliku važnost i dubok utjecaj na društvo, gospodarstvo i svakodnevni život. Digitalna tehnologija omogućuje uređajima da budu manji, brži, lakši i prilagodljiviji. Također, velike količine informacija mogu se pohraniti na lokalnoj ili udaljenoj lokaciji te se mogu brzo premještati. Pojam "informacija" više ne obuhvaća samo tekstualne i brojčane podatke, već i medije poput fotografija, audio i video zapisa.[4] U nastavku su navedene prednosti digitalne tehnologije[5]. Prva prednost je društvena povezanost, ona omogućuje da ljudi budu povezani putem društvenih mreža i interneta. Druga je brzina komunikacije putem digitalnih kanala. Treća je fleksibilan rad iz različitih lokacija i prilagođava se prema potrebama korisnika. Četvrta prednost je mogućnost učenja tj. pristup obrazovnom sadržaju putem digitalnih platformi. Peta je automatizacija procesa kako bi se povećala učinkovitost i smanjio ljudski rad. Šesta važnost je pohrana informacija na digitalne uređaje ili u oblak upravo zbog velikih količina podataka. Potom od velike je važnosti što digitalne tehnologije omogućuju uređivanje i manipulaciju podacima na brz i jednostavan način. Kao osmu prednost

[3] Ibid.
[4] TurboFuture (2023.), *16 Advantages of Digital Technology – TurboFuture* [online], dostupno na https://turbofuture.com/computers/Advantages-of-Digital-Technology
[5] Ibid.

navodimo precizno reproduciranje podataka bez gubitka kvalitete. Nastavno digitalna tehnologija omogućuje precizno praćenje lokacije i navigaciju, zatim ima veliki utjecaj na razvoj transporta i logistike. Upravo zbog primjene tehnologija digitalne usluge i proizvodi često su pristupačniji. Digitalna tehnologija omogućuje pristup raznim oblicima zabave kao što su igre, glazba, filmovi. Brzi pristup vijestima putem digitalnih platformi. Digitalna tehnologija ima utjecaj i na modernizaciju vojnih tehnologija i strategija, također mijenja način na koji obavljamo bankarske transakcije i upravljamo financijama. Te kao posljednju važnost možemo navesti kako nam tehnologije omogućuju razvoj manjih i lakših uređaja koji su moćni i funkcionalni.[6] Digitalna tehnologija oblikuje različite aspekte našeg života i poslovanja na način koji donosi brojne praktične i funkcionalne prednosti. Navedene su samo neke od prednosti digitalnih tehnologija, u svakodnevnom životu susrećemo se s još brojnim primjerima utjecaja. Velik utjecaj i konstantan rast korištenja digitalnih tehnologija može se vidjeti na Slici 1.

Slika 1 Jedna minuta na internetu

Izvor: https://www.docidediscovery.com/the-internet-in-2023-every-minute/

[6] Ibid.

3. KONCEPT KIBERNETIČKE SIGURNOSTI

3.1. Definicija kibernetičke sigurnosti

Prema definiciji Središnjeg državnog ureda za razvoj digitalnog društva kibernetička sigurnost obuhvaća skup procesa, mjera i standarda koji osiguravaju određenu razinu pouzdanosti prilikom korištenja proizvoda i usluga u kibernetičkom prostoru.[7] Posebno se ističe važnost sustavne zaštite računala, računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada. Ova vrsta zaštite igra ključnu ulogu u osiguravanju integriteta, privatnosti i sigurnosti digitalnih sustava i podataka.[8] Prema Spremić (2017.b) kibernetička sigurnost predstavlja kao skup mjera koje su usmjerene na zaštitu pojedinaca i tvrtki od namjernih, sofisticiranih i ciljanih napada, krađe podataka te incidenata koji su teško otkriveni ili spriječeni. Kibernetička sigurnost bavi se zaštitom informacijskih sustava od raznih prijetnji, uključujući računalne viruse, zlonamjerni softver, hakiranje, phishing napade i druge oblike cyber napada. Cilj kibernetičke sigurnosti je osigurati integritet, povjerljivost i dostupnost podataka te održati stabilnost i pouzdanost informacijskih sustava. Ove mjere mogu uključivati upotrebu antivirusnih programa, firewalla, enkripcije podataka, sustava za detekciju i odgovor na incidente te obuku korisnika o sigurnosnim praksama.[9]

3.2.Vrste sigurnosnih prijetnji

Nakon što je definiran pojam kibernetičke sigurnosti u ovom poglavlju navest će se i objasniti neke od vrsta kibernetičkih napada. Prema ISACA izvješću o stanju kibernetičke sigurnosti iz 2023. godine najčešći napadi bili su:[10]

- društveni inženjering (engl. Social engineering)- 15%
- napredne ustrajne prijetnje (engl. Advanced persistent threat, ATP)- 11%

---

[7] Središnji državni ured za razvoj digitalnog društva (2022.). *Kibernetička sigurnost* [online], dostupno na: https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436

[8] Ibid.

[9] Spremić, M. (2017.b), *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Sveučilište u Zagrebu, Ekonomski fakultet.

[10] ISACA (2023.) *State of Cybersecurity 2023*.[online], dostupno na: https://www.isaca.org/resources/reports/state-of-cybersecurity2023?gad_source=1&gclid=Cj0KCQjwir2xBhC_ARIsAMTXk85_QfqB7uu7JHYbSbFFGwWYobgSqaBNyYeyqevo7nf3-JcVLpMHmqUaAkzqEALw_wcB

- napadi pogrešne konfiguracije sigurnosti (engl. Security misconfiguration)- 10%
- ucjenjivački softver (engl. Ransomware)- 10%
- nezakrpani softver (engl. Unpatched system)- 10%
- osjetljivi podaci (engl. Sensitive data exposure)- 9%
- napadi uskraćivanjem usluge (engl. Denial of service, DoS)- 9%

Najzastupljeniji oblik napada iz Izvještaja u 2023. godini bio je društveni inženjering. Društveni inženjering je proces koji uključuje manipulaciju ljudima kako bi otkrili što više informacija o sebi te informacije zatim se koriste za krađu online identiteta i izvođenje različitih oblika zloupotreba, poput lažnih kupovina proizvoda i usluga, stvaranja lažnih profila na društvenim mrežama i prikazivanja lažnih identiteta (Spremić, 2017.b). Napredne ustrajne prijetnje su složene i ciljane prijetnje koje se karakteriziraju visokom razinom organiziranosti i upornosti. Ove prijetnje obično provode napadači kao što su državni akteri, organizirani kriminalni sindikati ili napredne hakerske skupine. Napadi pogrešne konfiguracije sigurnosti upućuju na to da organizacija nije uspješno implementirala sve sigurnosne mjere ili da je postupak implementacije sadržavao greške (Spremić, 2017.b).

Ucjenjivački softveri pripada zlonamjernim računalnim programima odnosno računalnim virusima. Računalna ucjena obično se provodi nakon neovlaštenog pristupa računalnom sustavu, često putem računalnog virusa pokrenutog od strane neopreznog korisnika. U ovom postupku, podaci pohranjeni u računalu se kriptiraju i postaju nedostupni za daljnju upotrebu, što može ozbiljno ometati rad ili poslovanje organizacije. Napadači, zatim zahtijevaju isplatu odštete kako bi omogućili dekriptiranje podataka (Spremić, 2017.b). Do ugroženosti osjetljivih podataka dolazi jer web aplikacije ili Application Programming Interface ne štite podatke na odgovarajući način. Napadi uskraćivanjem usluge se odnose na nedopuštene aktivnosti koje sprječavaju ili ograničavaju ovlaštenu upotrebu računalne mreže, sustava ili programa iskorištavanjem njihovih resursa, poput procesora, memorije, propusnosti mreže ili prostora za pohranu podataka (Spremić, 2017.b).

Ostale vrste napada iz Izvještaja u 2023. godini prikazani su na Slici 2[11].

[11] ISACA (2023.) *State of Cybersecurity 2023*.[online], dostupno na: https://www.isaca.org/resources/reports/state-of-cybersecurity2023?gad_source=1&gclid=Cj0KCQjwir2xBhC_ARIsAMTXk85_QfqB7uu7JHYbSbFFGwWYobgSqaBNyYeyqevo7nf3-JcVLpMHmqUaAkzqEALw_wcB

Slika 2 Vrste kibernetičkih napada 2023.

Izvor: State of Cybersecurity 2023 Global Update on Workforce Efforts, Resources and Cyberoperations

U Godišnjem izvještaju Nacionalnog CERT-a za 2022. godinu u Hrvatskoj je obrađeno 1.296 prijava koje su pod nadležnosti Nacionalnog CERT-a.[12] Za usporedbu uzimamo i Izvještaj za 2023. godinu u kojoj je obrađeno 1.236 prijava.[13] Promjena u 2023. godini je smanjenje broja računalno-sigurnosnih incidenata, a razlog tome je veliki broj phishing kampanja u kojima je izvor incidenata bio isti pa su tretirani kao jedan incident. U obe promatrane godine najzastupljeniji oblici napada su phishing, scam i phishing URL, dok se u 2023. događa velika promjena u porastu broja incidenata klasificiranih kao Sustav zaražen zlonamjernim kodom sa 54 incidenta porast je na 142 incidenta. Razlog porasta je veći broj prijava te prijave kroz suradnju s CSIRT zajednicom. Također je povećan broj incidenata tipa phishing i phishing URL zbog većeg broja prijava od strane građana. Phishing kao oblik prijevare navodi korisnika na odavanje povjerljivih podataka, na pokretanje zlonamjernih programa najčešće putem elektroničke pošte. Također phishing može predstavljati napad u kojem napadač lažnim predstavljanjem pokušava dobiti financijsku korist, ali podrazumijeva i ostale napade manipulacije žrtvom poput smishing, vishing, catphishing, whaling i druge. Scam je također oblik prijevare gdje se potencijalnu žrtvu navodi na djelovanje u korist prevaranata. Najpoznatiji oblik je „nigerian scam“ ili „419 fraud“. Phishing URL je zlonamjerno web sjedište odnosno poveznica do lažne internet stranice na kompromitiranom web sjedištu koje se koristi za krađu povjerljivih podataka.[14] Na Slici 3 prikazani su udjeli incidenata po tipu u 2022. i 2023. godini.

[12] CERT.hr (2022.) *Godišnji izvještaj 2022*.[online], dostupno na: https://www.cert.hr/
[13] CERT.hr (2023.) *Godišnji izvještaj 2023*.[online], dostupno na: https://www.cert.hr/
[14] CERT.hr (2024.), *O incidentu - CERT.hr* [online], dostupno na: https://www.cert.hr/oincidentu/

Slika 3 Udjeli incidenata po tipu u 2022. i 2023. godini

Izvor: Godišnji izvještaj CERT-a 2022. i 2023.

Velika promjena odnosi se na značajan porast broja incidenata koji su klasificirani kao prijevare. Ovaj porast proizlazi iz povećanog broja prijava takvih incidenata od strane građana, što se može pripisati objavama upozorenja o prijevarama i phishing kampanjama na mrežnim i društvenim stranicama Nacionalnog CERT-a. Obzirom na to da web defacement, phishing URL, malware URL i spam URL predstavljaju kompromitirane web stranice, ukupan broj otkrivenih kompromitiranih web stranica smanjio se za 38,7% u usporedbi s 2021. godinom.[15] Također sa Slike 3 vidimo da je većina tipova incidenata u padu dok je sveukupni broj incidenata u porastu. U Izvještaju (2022. i 2023.) se naglašava kako je zbog veće osviještenosti građana i ažuriranja alata za detekciju prijevara došlo do većeg broja prijava incidenata.

Broj malvera u 2023. godini bio je oko 200. Malver je zlonamjerni softver koji napada računalo bez znanja korisnika. Od oko 200 detektiranih računala zaraženih malverom čak 111 računala je zaraženo SystemBc malverima.[16] Prema Izvještaju (2023.) Windows platforma je ona za koju se najviše malvera širilo pa su napadači iskorištavali .iso arhivske datoteke, ali značajan broj malvera i dalje dolazi u .docx, .xls te lažnim „pdf“ datotekama. Broj botova u 2023. godini, tj. zaraženih

[15] CERT.hr (2022.) *Godišnji izvještaj 2022*.[online], dostupno na: https://www.cert.hr/
[16] CERT.hr (2023.) *Godišnji izvještaj 2023*.[online], dostupno na: https://www.cert.hr/

računala ili mreža zaraženih računala, iznosio je 138.676 i osjetno se povećao za 201,3% u odnosu na 2022. godinu.[17]

3.3. Važnost i rizičnost kibernetičke sigurnosti u digitalnom okruženju

U proteklim desetljećima, a naročito posljednjih godina izloženi smo izazovima koji imaju utjecaj na sigurnosti informacijskih sustava. Dolazi do porasta unutarnjih prijetnji, uspona novih tehnologija, povećanja vanjskih prijetnji, eksplozivni rast količine podataka, široka upotreba mobilnih uređaja i društvenih medija što vodi jačanju regulativa na međunarodnoj i nacionalnoj razini u području sigurnosti informacija i zaštite privatnosti podataka.[18] Prema istraživanju Spremić (2013.) objašnjava da se problemima sigurnosti informacijskog sustava mora upravljati proaktivno uzimajući u obzir sve komponente IS-a (hardver, softver, ljudi, procesi, organizacijska kultura, postupci, tehnologija i mreže). Često su sustavi zaštite neučinkoviti jer su usmjereni uglavnom na tehnički aspekt problema. Zaključuje se da reaktivni pristup upravljanju sigurnosti više nije učinkovit i potrebno je uvesti proaktivni koncept upravljanja.[19] Prema Godišnjem izvještaju CERT-a (2023.) Nacionalni CERT provodio je proaktivne i reaktivne mjere kako bi umanjio opasnost od računalno-sigurnosnih incidenata te kako bi smanjio štetu koja nastaje u njihovoj pojavi. Proaktivnim mjerama djeluje se prije incidenata i drugih događaja koji potencijalno mogu narušiti sigurnost informacijskih sustava. Cilj proaktivnih mjera je spriječiti ili ublažiti štete.[20] Na Slici 4 vidimo neke od proaktivnih mjera koje je primjenjivao Nacionalni CERT u 2023. godini.

---

[17] Ibid.
[18] Spremić, M. (2013.), *Holistic approach for governing information system security. Proceedings of the World Congress on Engineering*, Vol. 2
[19] Ibid.
[20] CERT.hr (2023.) *Godišnji izvještaj 2023*.[online], dostupno na: https://www.cert.hr/

Slika 4 Proaktivne mjere

Neke od proaktivnih mjera su:

- diseminacija informacija iz područja računalne sigurnosti - izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- praćenje računalno-sigurnosnih tehnologija - izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima;
- praćenje i objavljivanje novosti u vezi kibernetičke sigurnosti;
- provjera ranjivosti za ustanove članice CARNET mreže;
- izdavanje elektroničkih certifikata za ustanove članice CARNET-a (poslužiteljskih i klijentskih);
- sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacija koje pristupaju sustavu eMatica;
- Informiranje putem www.antibot.hr s ciljem pružanja pristupačnih i jednostavnih savjeta krajnjim korisnicima o kibernetičkoj sigurnosti;
- unapređenje svijesti o značaju računalne sigurnosti - organiziranje i provedba aktivnosti podizanja svijesti o kibernetičkoj sigurnosti;
- edukacija i obuka o računalnoj sigurnosti;
- održavanje predavanja i webinara o sigurnosti na internetu;
- sudjelovanje u televizijskim i radijskim emisijama;

Izvor: Godišnji izvještaj CERT-a 2023.

S druge strane CERT koristi i reaktivne mjere kao odgovor na incidente u Republici Hrvatskoj kao i na ostale događaje koji predstavljaju prijetnju kibernetičkoj sigurnosti javnih informacijskih sustava u zemlji.[21] Na Slici 5 vidimo primjere provedenih reaktivnim mjera.

Slika 5 Reaktivne mjere

Neke od reaktivnih mjera su:

- postupanje s računalno-sigurnosnim incidentima - obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);
- koordinacija rješavanja značajnijih incidenata - obrada incidenata sa znatnim učinkom sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga;
- sigurnosna upozorenja;
- prikupljanje podataka o kompromitiranim računalima i njihovim aktivnostima s izvora na internetu te njihova analiza;
- prikupljanje i analiza podataka o napadima dobivenih iz sustava ili senzora;
- Abuse služba CARNET mreže.

Izvor: Godišnji izvještaj CERT-a 2023.

[21] Ibid.

S obzirom da se sve više podataka prenosi, pohranjuje i obrađuje rizici povezani s kibernetičkom sigurnošću postaju sve veći. U digitalnom okruženju kibernetički napadi mogu imati ozbiljne posljedice, uključujući krađu osjetljivih informacija, ometanje poslovanja, narušavanje reputacije kompanije, gubitak korisnika i naravno može dovesti do velikih financijskih gubitaka. Ključno je da organizacije i pojedinci poduzmu odgovarajuće mjere kako bi zaštitili digitalne resurse.[22] Rizičnost kibernetičke sigurnosti je u porastu zbog složenijih i sofisticiranijih napada. Napadi kao što su phishing, ransomware, DDoS i krađe identiteta postaju sve češći i zahtjevniji za otkrivanje te na kraju i suzbijanje. Od iznimne je važnosti da se provode strategije kibernetičke sigurnosti koje uključuju implementaciju sigurnosnih alata, tehnologija, od velikog je značaja i edukacija zaposlenika, redovite provjere i ažuriranje sustava te razvoj kriznih planova u slučaju napada. Među ostalim bitna je suradnja s relevantnim regulatornim tijelima i dijeljenje informacija o prijetnjama što može dodatno pomoći u zaštiti digitalnog okruženja. Poteškoće mogu nastati zbog činjenice da tvrtke općenito nisu voljne sudjelovati u istraživanjima, studijama slučaja ili dubinskim intervjuima jer bi mogli otkriti neke ranjivosti u svojem poslovanju i izložiti se određenom riziku.[23]

Važnost kontinuiranog nadzora i usavršavanja poslovnih procesa unutar je svake organizacije. Implementacija novih tehnologija može donijeti nove sigurnosne probleme, osobito ako se istovremeno koriste s postojećim procesima. Ključno je da mrežni administratori budu svjesni sigurnosnih implikacija prijelaznih mehanizama kako bi uspješno implementirali sigurnosne mjere poput vatrozida i sustava za detekciju napada. Ovo naglašava važnost razumijevanja potencijalnih rizika i pravilnog upravljanja sigurnosnim aspektima prilikom implementacije novih tehnologija u poslovne procese.[24] Važan je odabir standarda prilikom implementacije sigurnosne politike kako bi se olakšao proces upravljanja rizicima.

[22] Kovač, D. (2021). Ulaganje u kibernetičku sigurnost. *Zbornik Radova Veleučilišta U Šibeniku*, *15*(1–2), 61–73

[23] Spremić, M. (2013.), Holistic approach for governing information system security. *Proceedings of the World Congress on Engineering*, Vol. 2, str. 3-5.

[24]Žagar, D., Grgić, K. (2006.) IPv6 Security Threats and Possible Solutions u *2006 World Automation Congress*, Budapest, Hungary

Postoji nekoliko standarda i metodologija koji su globalno priznati i osmišljeni kako bi osigurali da organizacije prate najbolje prakse u svojoj industriji.[25]:

- ISO 27001:2013- međunarodni standard koji pruža smjernice za uspostavljanje, implementaciju, održavanje i poboljšanje upravljanja informacijskom sigurnošću u organizacijama
- CobiT 5 (engl. Control Objectives for Information and Related Technologies)- pruža smjernice za upravljanje informacijskom tehnologijom u organizacijama, uključujući aspekte sigurnosti
- NIST metodologija za kibernetičku sigurnost/računala- okvir koji je razvila Nacionalna agencija za standarde i tehnologiju SAD-a kako bi pružio smjernice za poboljšanje kibernetičke sigurnosti naročito za kritičnu infrastrukturu
- SANS Institute Critical Controls- skup od 20 sigurnosnih kontrola koje su identificirane kao ključne za smanjenje rizika od kibernetičkih napada
- Podatkovno sigurnosni standard industrije za obradu kartičnih podataka (PCI-DSS)- standard usmjeren na zaštitu podataka o karticama i propisuje zahtjeve i smjernice za organizacije koje obrađuju, pohranjuju ili prenose kreditne kartične podatke

Ovi standardi omogućuju organizacijama da usvoje usklađene i provjerljive sigurnosne prakse, što može pomoći u zaštiti njihovih informacijskih resursa i smanjenju rizika od sigurnosnih incidenata. Sigurnosni stručnjaci imaju primarni cilj spriječiti sigurnosne incidente kako bi zaštitili informacijske sustave i podatke. Međutim, ako se incident dogodi, njihov je zadatak što prije otkriti neželjene događaje i poduzeti odgovarajuće korake za reagiranje. [26]

Sigurnosne mjere mogu se organizirati prema njihovoj namjeni. Postoji sedam namjena sigurnosnih mjera[27]: sprječavanje, otežavanje, otkrivanje, kompenziranje, popravljanje, oporavljanje i upravljanje. Namjena sprječavanja su aktivnosti i mjere koje se poduzimaju unaprijed kako bi se spriječili sigurnosni incidenti ili napadi na informacijske sustave. Ove mjere su proaktivne prirode i imaju za cilj smanjiti ili eliminirati rizike od sigurnosnih prijetnji. Primjer sprječavanja su testiranje sustava, kontrola pristupa, šifriranje, provođenje sigurnosne politike,

[25] Antonucci, D. (2017.) *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Hoboken, New Jersey.: John Wiley & Sons
[26] Ibid.
[27] James Michael Stewart, M. Chapple, D. Gibson (2021.) (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition, Hoboken, New Jersey: John Wiley & Sons, Inc.

kontinuirani nadzor i treniranje zaposlenika, postavljanje antivirusnih sustava, analiza mrežnog prometa. Mjere otežavanja imaju za cilj otežati potencijalnim napadačima provođenje napada, stvoriti dodatne prepreke i poteškoće u provođenju napada. Od preventivnih metoda se razlikuju jer su usmjerene prema napadaču, a ne sustavu. Mjere otkrivanja koriste se za identifikaciju neželjenog ponašanja ili neovlaštene aktivnosti unutar informacijskog sustava. Koriste se tek poslije sigurnosnog incidenta. Ove mjere su ključne za pravovremeno reagiranje na sigurnosne prijetnje i incidente te pružaju sigurnosnim stručnjacima početnu točku za daljnju analizu i rješavanje problema.[28] Kompenzacijske mjere su dizajnirane da ublaže ili nadomjeste nedostatke u mjerama sigurnosti i da osiguraju dodatnu zaštitu. Primjer kompenzacijske mjere je izrada sigurnosnih kopija svih ključnih resursa da bi se eliminirao rizik od gubitka podataka. Ukoliko dođe do napada organizacija može u kratkom roku obnoviti izgubljene podatke. Mjere popravljanja su usmjerene na vraćanje sustava ili okoline u sigurno i funkcionalno stanje nakon što je detektiran propust ili incident. Njihov cilj je minimizirati štetu i osigurati da sustav nastavi normalno funkcionirati nakon detektiranog problema. Mjere oporavljanja su aktivnosti koje se provode nakon ozbiljnog sigurnosnog incidenta ili katastrofe kako bi se osiguralo brzo i učinkovito vraćanje sustava ili poslovanja na normalno stanje. Ove mjere idu korak dalje od mjera popravljanja i obuhvaćaju širi spektar aktivnosti koje su usmjerene na obnovu cjelokupnog okruženja. Mjere upravljanja su ključne za osiguravanje da se sigurnosna politika organizacije dosljedno primjenjuje i prati od strane svih zaposlenika. Sastoje se od smjernica za zaposlenike, nadzora, obuke, zakona i propisa što omogućuje usklađenost s sigurnosnim standardima, pravilima i procedurama. Njihova svrha je osigurati da organizacija ima jasne smjernice i mehanizme nadzora kako bi se osiguralo da se sigurnosne politike poštuju i primjenjuju.[29]

U Izvještaju Nacionalnog CERT-a iz 2022. godine i 2023. godine zanimljivo je uočiti kako raste broj incidenata u određenim mjesecima. Napadači iskorištavaju konkretna događanja za prijevare korisnika. Na Slici 6 prikazani su incidenti po mjesecima u 2022. godini, a na Slici 7 incidenti po mjesecima u 2023. godini.

[28] Mrganić, S. (2022.) *Etičko hakiranje i kibernetička sigurnost*. Diplomski rad. Osijek: Fakultet elektronike, računarstva i informacijskih tehnologija
[29] Ibid.

Slika 6 Mjesečni prikaz broja incidenata na poslužiteljima u 2022. godini

Izvor: Godišnji izvještaj CERT-a 2022.

Slika 7 Mjesečni prikaz broja incidenata na poslužiteljima u 2023. godini

Izvor: Godišnji izvještaj CERT-a 2023.

U 2022. godini značajan porast napada zabilježen je u kolovozu. Do porasta dolazi zbog većeg broja phishing kampanja koje su ciljale korisnike mobilnih aplikacija hrvatskih banaka, a tematika napada je bila uvođenje eura u Hrvatskoj. Korisnike se putem poveznice navodilo na preuzimanje nove aplikacije, ali su napadači na taj način željeli pristupiti mobilnom bankarstvu korisnika.[30] U 2023. godini u Izvještaju nacionalnog CERT-a vidimo tri skoka u siječnju, ožujku i kolovozu. Skok u siječnju također se odnosio na uvođenje eura kao službene valute. Skok u ožujku rezultat je phishing kampanja na temu povrata poreza te scam kampanja. Kroz scam kampanje napadač se predstavljao kao osoba iz policije koja tjera žrtvu da odgovori na sudski poziv zbog djela kibernetičkog kriminala, nakon čega slijedi krađa financijske prirode. U kolovozu raste broj incidenata zbog phishing kampanje i sustava zaraženih zlonamjernim kodom. [31]

[30] CERT.hr (2022.) *Godišni izvještaj 2022*.[online], dostupno na: https://www.cert.hr/
[31] CERT.hr (2023.) *Godišni izvještaj 2023.* [online], dostupno na: https://www.cert.hr/

4. RAZLIČITE ULOGE I RIZICI PRIMJENE DIGITALNIH TEHNOLOGIJA

4.1. Kako digitalne tehnologije otvaraju nove ranjivosti?

Digitalne tehnologije u današnjoj digitalnoj ekonomiji osiguravaju provođenje velikog broja transakcija i pružaju brže i bolje poslovanje. Suprotno prednostima koje nam donose, postoje i nedostaci. Ukoliko dođe do pogreške ili otežanog funkcioniranja informatičkog sustava dolazi i do velikih problema. Što više kompanije intenzivno koriste suvremene informacijske i digitalne tehnologije, to su više izložene kibernetičkim i informatičkim rizicima. World Economic Forum je već u 2017. godini prepoznao opasnost i utjecaj kibernetičkih rizika i uvrstio ih u prvih pet rizika s kojima se tada svijet suočavao.[32]

Kibernetički rizici odnose se na intenzivnu primjenu digitalnih tehnologija. Ova izloženost proizlazi iz činjenice da suvremene tehnologije otvaraju nove mogućnosti za napade i prijetnje, dok istovremeno stvaraju složenije i povezanije informacijsko okruženje koje je podložno napadima. [33] Između ostalog možemo reći da su kibernetički rizici operativni rizici koji mogu negativno utjecati na sigurnost u digitalnom okruženju zbog sve veće upotrebe digitalnih tehnologija u poslovanju i svakodnevnom životu.[34] Povećanjem broja efikasnih kontrola koje su namijenjene sprječavanju neželjenih događaja, povećava se vjerojatnost da će organizacija biti manje izložena informatičkim rizicima.[35] Ovi rizici imaju dvostruku prirodu. Prvotno oni su neizbježni i stalno prisutni u poslovnom okruženju koje se oslanja na digitalne tehnologije te se napadi i druge prijetnje mogu dogoditi u bilo kojem trenutku i izazvati probleme u poslovanju kao što je gubitak podataka, prekid usluga, financijski gubitak i loša reputacija. Drugo, odgovarajućim upravljanjem ovim rizicima doprinosimo očuvanju vrijednosti informacijskih ulaganja. Efikasno upravljanje rizicima može povećati otpornost organizacije na cyber prijetnje i osigurati kontinuitet poslovanja u digitalnom okruženju.[36]

---

[32] Spremić, M., Šimunic, A. (2018.). *Cyber security challenges in digital economy*. Proceedings of the World Congress on Engineering, Vol. 1, Hong Kong, China: International Association of Engineers.

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

[34] Kovač, D. (2021.), *Ulaganje u kibernetičku sigurnost*. Zbornik radova veleučilišta u Šibeniku, 15 (1-2)

[35] Miloš Sprčić, D. (2013.), *Upravljanje rizicima: temeljni koncepti, strategije i instrumenti*, Zagreb, Sinergija

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

Informatički i kibernetički rizici proizlaze iz djelovanja prijetnji koje su usmjerene na računalne sustave, mreže i podatke. Ove prijetnje mogu potjecati od različitih izvora, uključujući pojedince, organizirane kriminalne skupine, hakere, državne ili međunarodne agencije te interne zaposlenike.[37]

Prijetnje mogu biti različite prirode i uključivati različite vrste napada. Identificirane prijetnje promatramo u kontekstu ranjivosti resursa informacijskog sustava kako bi se procijenilo kako bi te prijetnje mogle iskoristiti ranjivosti i na kraju prouzročiti štetu. Ranjivosti su slabosti ili nedostaci u informacijskom sustavu koje se mogu zloupotrijebiti za izvođenje napada ili neovlaštenog pristupa. Digitalne tehnologije otvaraju nove ranjivosti na više načina. Prvi primjer ranjivosti je nepostojanje zaštite od malicioznog koda. Ukoliko informacijski sustav nema zaštitne mjere kao što su antivirusni softver ili vatrozid, može biti napadnut malicioznim softverom kao što je virus, crv ili ransomware. Nadalje kao primjer navodimo neprimjerenu konfiguraciju vatrozida jer ukoliko vatrozid nije ažuriran može propustiti detektirati ili blokirati napade poput DDoS napade i neovlaštene pristupe. Treći primjer ranjivosti je kada pristup poslovnim aplikacijama ne traži identifikaciju korisnika odnosno ne postoji adekvatna metoda autentifikacije i autorizacije što povećava rizik da neovlaštene osobe pristupe osjetljivim podacima. Također kao veliki rizik navodimo ljudski faktor tj. nisku razinu svijesti o sigurnosti IS-a među zaposlenicima zbog nedostatka obuke. Upravo ta loša svijest dovodi do neopreznog ponašanja poput otvaranja sumnjivih mailova ili dijeljenja osjetljivih informacija. Kao fizički rizik možemo navesti nepostojanje sustava za kontinuiranu opskrbu električnom energijom. Ukoliko dođe do prekida rada sustava zbog nestanka električne energije postoji rizik od gubitka podataka. Kada se mogu prepoznati navedene ranjivosti može se i procijeniti rizike informacijskog sustava gledajući dvije glavne karakteristike, a to je vjerojatnost da će prijetnja iskoristiti ranjivosti resursa i koja je razina štetnog učinka ukoliko prijetnja iskoristi ranjivosti. Važno je naglasiti da može postojati prihvatljiva razina rizika koja označava stupanj rizika koji se smatra prihvatljivim jer još uvijek ne ugrožava ključne poslovne funkcije, procese ili ostvarivanje poslovnih ciljeva organizacije.[38]

[37] Ibid.
[38] Ibid.

4.2. Uloga umjetne inteligencije i strojnog učenja u kibernetičkoj sigurnosti

Umjetna inteligencija (AI) i strojno učenje (ML) imaju bitnu ulogu u poboljšanju kibernetičke sigurnosti pružanjem naprednih analitičkih alata, detekcije prijetnji i automatizacije sigurnosnih postupaka. Doprinose efikasnijoj, proaktivnijoj i inteligentnoj kibernetičkoj sigurnosti pružajući organizaciji da bolje odgovori na složene prijetnje u suvremenom digitalnom okruženju.[39] Umjetna inteligencija predstavlja sposobnost računalnih sustava da simuliraju ljudske aktivnosti kao što su zaključivanje, učenje, planiranje i kreativnost. Primjenom umjetne inteligencije, tehnički sustavi mogu percipirati svoje okruženje, analizirati informacije koje prikupljaju te rješavati probleme. Računalni sustav prima podatke koji već mogu biti prikupljeni pomoću senzora, obrađuje ih i generira odgovore ili akcije. Sustavi umjetne inteligencije mogu prilagoditi svoje ponašanje na temelju analize prethodnih situacija te donositi odluke autonomno u određenoj mjeri.[40]

Slika 8 Infografika o upotrebi umjetne inteligencije

Izvor: Europski parlament, dostupno na https://www.europarl.europa.eu/topics/hr/article/20200827STO85804/sto-je-umjetna-inteligencija-i-kako-se-upotrebljava

[39] Aleksić, D. (2023.) *Primjena umjetne inteligencije u području kibernetičke sigurnosti*. Diplomski rad. Zagreb: Fakultet prometnih znanosti

[40] Europski parlament [online], dostupno na: https://www.europarl.europa.eu/topics/hr/article/20200827STO85804/sto-je-umjetna-inteligencija-i-kako-se-upotrebljava

Primjena umjetne inteligencije je široka i obuhvaća mnoge aspekte svakodnevnog života. Na primjer, internetske trgovine koriste je za pružanje personaliziranih preporuka svakom korisniku na temelju prethodnih pretraga, kupovina i ostalih informacija o korisnikovom ponašanju na internetu. Slično tome, pretraživači interneta koriste ogromne količine podataka o korisnicima kako bi pružili relevantne rezultate pretraživanja koji odgovaraju njihovim interesima i potrebama. U Europi se aktivno radi na naprednijim primjenama umjetne inteligencije, uključujući autonomna vozila. Iako autonomna vozila još nisu u širokoj upotrebi, novija vozila već koriste sigurnosne funkcije temeljene na umjetnoj inteligenciji. Na primjer, vozača se upozori ako tijekom vožnje napusti svoju traku, vozilo se automatski zaustavi ako se vozač previše približi objektu tijekom parkiranja i slično. Također se istražuju mogućnosti primjene umjetne inteligencije u medicinskoj dijagnostici, optimiziranju proizvodnje u tvornicama, prepoznavanju kibernetičkih napada i drugim područjima.[41] U nastavku će se navesti neke od prednosti primjene umjetne inteligencije. Umjetna inteligencija dovodi do automatizacije procesa u poslovanju, također vodi smanjenju troškova te kao rezultat povećanje učinkovitosti. Primjer automatizacije procesa je korištenje chatbotova umjesto korisničke službe ili uz manji ljudski angažman. Umjetna inteligencija može se koristiti u kombinaciji sa podacima o uspješnosti poduzeća kako bi se poboljšali pokazatelji uspješnosti poslovanja. Nadalje AI koristi se za stvaranje platformi za dijeljenje tj. platformi za umrežavanje korisnika istih interesa i potreba. Umjetna inteligencija može pomoći u prepoznavanju prilika za razvoj usluga i proizvoda ili poboljšanje postojećih. Kao najbitniju prednost od svih navodimo korištenje AI u otkrivanju sigurnosnih prijetnji i rizika za poslovanje te pruža zaštitu od krađe podataka. [42]

[41] CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/

[42] Crnogorac, S. (2023.) *Dvojaka uloga umjetne inteligencije u informacijskoj sigurnosti kao izvora prijetnje i odgovora na prijetnju.* Diplomski rad. Zagreb: Ekonomski fakultet

Tablica 1 Prednosti i nedostaci primjene umjetne inteligencije (AI)

Prednosti primjene AI	Rizici i izazovi primjene AI
Smanjenje troškova procesa	Nedostatak transparentnosti
Povećanje učinkovitosti	Gubitak radnih mjesta
Unaprjeđenja prakse mjerenja učinka	Pristranost algoritama
Sposobnost predviđanja trendova	Nepouzdanost algoritama
Unaprjeđenje procesa odlučivanja	Nedostatak odgovornosti u odlukama
Olakšana personalizacija proizvoda i usluga	Nedostatak kreativnosti
Povećano zadovoljstvo i vjernost kupaca	Smanjena kvaliteta korisničkog iskustva
Stvaranje platformi za dijeljenje	Regulatorni izazovi
Stvaranje novih poslovnih prilika	Novi cyber rizici
Unaprjeđenje informacijske sigurnosti	
Smanjenje rizika poslovanja	

Izvor: Crnogorac, S. (2023.) Dvojaka uloga umjetne inteligencije u informacijskoj sigurnosti kao izvora prijetnje i odgovora na prijetnju. Diplomski rad. Zagreb: Ekonomski fakultet

Teško je spriječiti kibernetičke napade bez suradnje s višim stručnjacima, ali korištenjem umjetne inteligencije pritisak na stručnjake može biti manji. Primjenom umjetne inteligencije možemo poboljšati pristup strojnom učenju koje može analizirati podatke kako bi se otkrili izvori kibernetičkih napada ili ih možda i spriječili. AI omogućuje detekciju malvera korištenjem podataka iz prethodnih kibernetičkih napada na različite načine, uključujući analizu ponašanja, procjenu rizika, blokiranje botova, automatizaciju sigurnosnih zadataka. Međutim, implementacija umjetne inteligencije može predstavljati nove prijetnje, stoga stručnjaci za kibernetičku sigurnost moraju uspostaviti ravnotežu između rizika i koristi koje donosi. Iako umjetna inteligencija može pomoći stručnjacima u donošenju odluka i zaključaka, nikada neće moći donijeti sve odluke i prosudbe u području kibernetičke sigurnosti. [43]

Porast umjetne inteligencije donosi sa sobom i povećanu prijetnju kibernetičkom kriminalu. Trenutno, glavne opasnosti povezane su s metodama društvenog inženjeringa, gdje se kroz manipulativni sintetički sadržaj pokušava zavarati pojedinac ili šira publika. Porastom problema vezanih uz sintetički sadržaj, raste i potreba za razvojem alata za filtriranje istog. Zbog toga se razvijaju različiti detektori s različitim pristupima, a razmatra se i uvođenje prakse umetanja digitalnih vodenih žigova prilikom generiranja takvog sadržaja. Osim toga, uz napredak dolazi i

[43] S. A. Alawadhi, A. Zowayed, H. Abdulla, M. A. Khder, B. J. A. Ali (2022.) *Impact of Artificial Intelligence on Information Security in Business*, 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain.

do pojave chatbotova s mogućnošću generiranja zlonamjernog koda ili phishing e-mailova. Neočekivano brz razvoj umjetne inteligencije i njezina sveprisutna primjena donijeli su i neke nove zlonamjerne aktivnosti. Jedan od primjera je tehnologija deepfake, koja manipulira video snimkama do te mjere da se može stvoriti realističan prikaz događaja koji se nikada nije dogodio. Također, razvoj alata za automatizaciju razvoja programske koda, poput ChatGPT, može se zloupotrijebiti kako bi se automatizirao i ubrzao proces razvoja zlonamjernih programa.[44]

Nakon što se analizirala uloga umjetne inteligencije u kibernetičkoj sigurnosti sada će se analizirati ulogu strojnog učenja. Strojno učenje je grana umjetne inteligencije koja se bavi razvojem algoritama i tehnika kojima se računalima omogućuje učenje iz podataka i iskustva, te donošenje zaključaka ili izvođenje zadataka bez eksplicitnog programiranja. Dakle, strojno učenje je tehnika u području umjetne inteligencije koja omogućuje računalima da automatski izvrše zadani zadatak, a da pritom ne zahtijevaju eksplicitno programiranje. Primjena strojnog učenja može rezultirati poboljšanom produktivnošću, a suvremena umjetna inteligencija uglavnom se oslanja na principe strojnog učenja (Chan-Olmsted, 2019; Sadiku i sur., 2021). U ovom postupku, računalu se daju skupovi podataka (ulazni podaci) koji se koriste za "učenje", a cilj je razviti modele ili algoritme koji mogu generalizirati naučeno znanje i primijeniti ga na nove podatke ili zadatke.[45] Strojno učenje (ML) ima sve važniju ulogu u kibernetičkoj sigurnosti upravo zbog sposobnosti analize velike količine podataka i otkrivanja uzoraka koji bi inače mogli proći nezapaženo. Tehnologija strojnog učenja postala je široko prihvaćena u mnogim područjima, a primjene tehnika strojnog učenja u kibernetičkoj sigurnosti su brojne. Primjeri uključuju analizu zlonamjernog softvera, posebno za otkrivanje zero-day malvera, analizu prijetnji i napada na kritičnu infrastrukturu te mnoge druge. Zbog nedjelotvornosti metodologija temeljenih na „signature-based“ metodi zero day napada ili čak blagih varijanti poznatih napada, detekcija temeljena na strojnom učenju koristi se u mnogim kibernetičkim proizvodima.[46] U posljednjih nekoliko godina, tehnike računalne inteligencije, uključujući strojno učenje (ML), duboko učenje (DL) i rudarenje podataka (DM), koriste se kako bi osigurale kibernetičku sigurnost. Strojno učenje koristi se primjerice, za detekciju intruzija ili zlonamjernog softvera te za autentikaciju korisnika

[44] CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/
[45] IBM. Machine Learning [online], dostupno na: https://www.ibm.com/cloud/learn/machine-learning
[46] Handa, A., Sharma, A., Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), e1306.

na temelju biometrijskih podataka. Međutim, algoritmi strojnog učenja su podložni napadima kako u fazama treniranja tako i u testiranja, što obično rezultira značajnim smanjenjem performansi i sigurnosnim propustima. Unatoč značajnom napretku u korištenju tehnika računalne inteligencije i povećanju performansi tehnologije, otpornost protiv kibernetičkih napada i razumijevanje zlonamjernih uzoraka i napada, računalna inteligencija u kibernetičkoj sigurnosti još uvijek treba značajno napredovati, uz prevladavanje mnogih izazova, kao što su napadi nultog dana. Osim toga, postoji i rastuća zabrinutost zbog sigurnosti i ranjivosti tehnika strojnog učenja protiv napada.[47]

U osnovi strojno učenje dijelimo u tri glavne skupine: nadzirano učenje (engl. supervised learning), nenadzirano učenje (engl. unsupervised learning) i podržano učenje (engl. reinforcement learning)[48]:

- Nadzirano učenje je vrsta učenja koja uključuje korištenje skupa podataka koji sadrži ulazne podatke i odgovarajuće oznake ili ciljeve. Cilj je naučiti model koji može predvidjeti odgovarajuće oznake za nove ulazne podatke. Primjeri nadziranog učenja uključuju klasifikaciju (predviđanje kategorije) i regresiju (predviđanje kontinuirane vrijednosti).
- Nenadzirano učenje nema oznaka u skupu podataka. Cilj je otkriti skrivene strukture ili obrasce unutar podataka. Primjeri nenadziranog učenja uključuju grupiranje (razvrstavanje podataka u slične skupine), procjena gustoće i smanjenje dimenzionalnosti (smanjenje broja značajki u skupu podataka).
- Podržano učenje uključuje učenje putem interakcije s okolinom. Modeli učenja donose odluke i na temelju povratnih informacija iz okoline prilagođavaju svoje postupke kako bi maksimizirali neku nagradu ili postigli neki cilj. Primjeri pojačanog učenja uključuju algoritme koji uče igrati videoigre ili upravljati robotima.

[47] Dasgupta, D., Akhtar, Z., Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1)
[48] Ibid.

U Tablici 2 vidimo neke od vrsta algoritama strojnog učenja i dubokog učenja koji se koriste u kibernetičkoj sigurnosti.

Tablica 2 Sažetak popularnih algoritama strojnog učenja i dubokog učenja koji se koriste u kibernetičkoj sigurnosti

Method	Working principal	Advantages	Disadvantages
Decision tree (DT)	A rule-based tree-structured classification model, trained on the basis of information gain of all features in training data	Computational cost is less and easy to implement.	Need to save all the information of the trained model. Space complexity is high.
Support vector machine (SVM)	Aims to find separating hyperplane in the feature space among its classes so that distance between the hyperplane and its nearest data points is maximized	Suitable for small sample size but large feature dimensions	Selecting optimal kernel size (*k*-value) is difficult
Naive Bayes (NB) classifier	Calculates posterior probability of a class given inputs based on Bayes' rule	Robust to noisy training data, easy to implement, performance does not degrade with low sample size	Assumes all features contribute independently during the learning algorithm, but in practice this hardly happens
Artificial neural network (ANN)	Consists of one or more hidden layers between the input and output layer. Stores input data information as weights in the hidden layer using the back-propagation algorithm	Suitable for pattern recognition problem with high accuracy	Computational complexity is high compared to other algorithms
k-means clustering	Makes clusters or groups among training data points based on similarity measures	Easy to implement. Suitable for problems where labeling data is very difficult	Selecting *k*-value at the beginning requires domain knowledge
Convolutional neural network (CNN)	Convolution layer of CNN extracts features from training data in a generative fashion using several hidden layers and a pooling layer that pull that information to predict output	Very useful for image classification and pattern recognition	Computationally complex. Performance degrades with low sample size
Recurrent neural network (RNN)	Processes sequential data integrating the temporal layer	Shows excellent performance for sequential data analysis, such as speech text	Vanishing or exploding gradient is the main disadvantage of the RNN
Restricted Boltzmann machine (RBM)	Unsupervised generative learning model, restricts the connection between nodes of the same layer (i.e., visible layer and hidden layer)	Feedback mechanism allows the RBM to extract important features in an unsupervised learning environment	Computational cost is very high
Deep belief network (DBN)	The DBN comprises stacked RBMs that execute greedy layer-by-layer training to get robust performance	The DBN shows better performance than the RBM as it takes the RBM on the top of each layer of its training data	Computational cost is very high as it takes a high number of parameters

Izvor: Dasgupta, D., Akhtar, Z., Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation

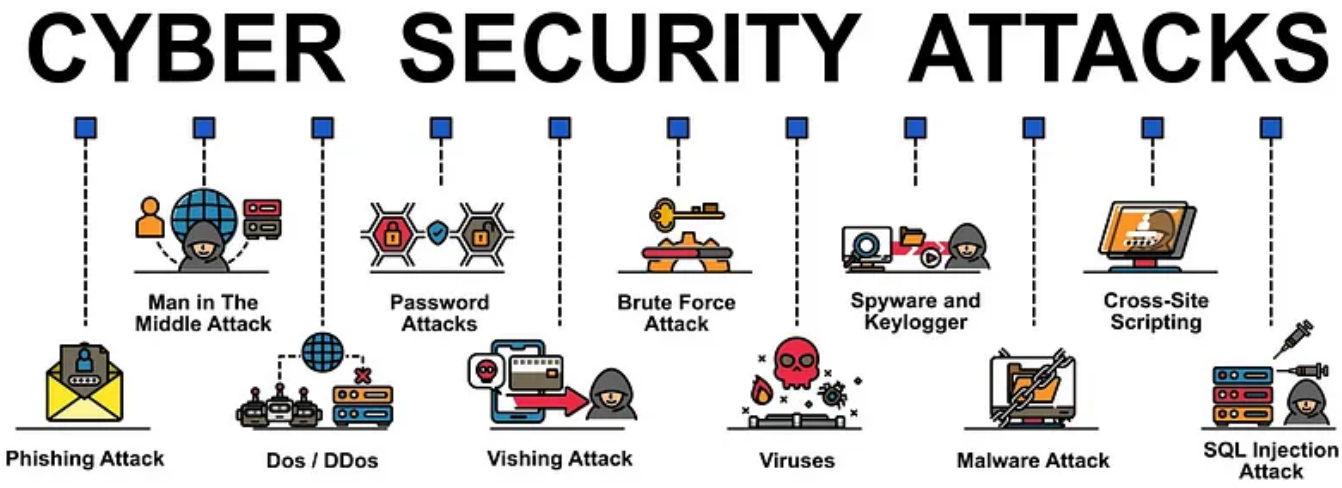
4.3. Primjeri napada i ranjivosti uzrokovanih digitalnim tehnologijama

Digitalne tehnologije pružaju različite mogućnosti za zlonamjernu upotrebu. Većina uspješnih napada temelji se na generiranju ili manipulaciji sadržaja s ciljem obmane žrtve. Razvoj malicioznih programa postaje olakšan, što omogućuje osobama s manje tehničkih vještina da izvedu napade. Neki od primjera napada i ranjivosti navedeni su kroz rad, ali možemo naglasiti i ukratko objasniti šest vrsta napada: phishing, ransomware, zero day napad, DDoS napadi, SQL injection napadi i IoT ranjivosti. [49]

- Phishing- kao što je već objasnili u radu, koriste napadači putem mailova, poruka ili lažnih web stranica kako bi prevarili korisnike i došli do povjerljivih podataka kao što su lozinke, brojevi kreditnih kartica itd.
- Ransomware- zlonamjerni softver koji može šifrirati podatke na računalu ili mreži i tražiti otkupninu za dešifriranje. Predstavlja posebnu opasnost za kompanije i organizacije koje mogu biti onesposobljene za rad ako im je pristup podacima blokiran.
- Zero day napadi- napadači koriste ranjivosti sustava koje još nisu poznate proizvođačima ili korisnicima kako bi ušli u sustav i izveli napad prije nego što se otkriju zakrpe.
- DDoS napadi- cilj je napad web mjesta i poslužitelja ometanjem mrežnih usluga, tj. preplavljivanjem web mjesta nasumičnim prometom, čime ih čine nedostupnima.
- SQL injection napadi- napadači koriste ranjivosti web aplikacija koje koriste SQL upite kako bi neovlašteno pristupili ili mijenjali baze podataka.
- IoT ranjivosti- uređaji interneta stvari često su povezani s mrežom bez dovoljno jake sigurnosne zaštite, što ih čini ranjivima na napade poput hakiranja.

[49] Microsoft. *Sigurnost 101* [online], dostupno na: https://www.microsoft.com/hr-hr/security/business/security-101/

Slika 9 Vrste kibernetičkih prijetnji



Izvor: Medium dostupno na https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b

U nastavku su navedeni i opisani primjeri napada u kojima je korištena umjetna inteligencija te razvoj kibernetičke sigurnosti kako bi se ubuduće zaštitili od takvih napada.

4.3.1. Deepfake

Prvi primjer napada korištenjem umjetne inteligencije i strojnog učenja je deepfake. Deepfake tehnologija koja se koristi za stvaranje fotografija, videozapisa ili audiozapisa u kojima je izgled ili glas jedne osobe zamijenjen izgledom ili glasom druge osobe. Naziv „deepfake“ dolazi od kombinacije riječi „deep learning“ i „fake“ što ukazuje na korištenje dubokog učenja tj. dubokih neuronskih mreža kako bi se stvorio uvjerljiv lažni sadržaj. Ovaj algoritam strojnog učenja sastoji se od dva podalgoritma. Prvi algoritam pokušava što vjernije naučiti strukturu i karakteristike lica ili glasa osobe koju želimo zamijeniti te ih preslikati na drugu osobu. Drugi algoritam tretiran je da prepoznaje greške i nelogičnosti u stvorenom sadržaju pa ih ispravlja kako bi rezultat bio što uvjerljiviji.[50] Postoje različite aplikacije koje koriste deepfake tehnologije kao što su Faceswap i

[50] Aware (2022.) *How does Deepfake Technology Work and Should I Be Worried About it?* [online], dostupno na: https://www.aware.com/blog-how-does-deepfake-technology-work/

Faceit_live. Ova tehnologija predstavlja izazov za sigurnost jer može biti zloupotrijebljena za stvaranje lažnih informacija ili prevaru korisnika putem digitalnih medija.

Stvarni napadi u kojima je korištena deepfake tehnologija:

1. Krajem 2019. godine u neimenovanoj tvrtki koja se bavi energetikom napadač je uvjerio izvršnog direktora kompanije da uplati 220.000 eura mađarskom dobavljaču, misleći da razgovara sa svojim nadređenim. Glas napadača izmijenjen je korištenjem umjetne inteligencije tj. deepfake tehnologije. Osiguravajuća tvrtka, napadnute kompanije, vjeruje da je napadač koristio komercijalno dostupan softver za generiranje glasa pomoću umjetne inteligencije kako bi izveo prijevaru.[51]
2. U 2022. godini FBI upozorava da su napadači izvršavaju krađu osobnih podataka pomoću deepfake tehnologije kako bi uvjerljivo koristili identitet druge osobe. Ovo im omogućuje da se prijave na radna mjesta u organizacijama koje zapošljavaju na daljinu te dobiju pristup povjerljivim informacijama.[52]
3. Krajem siječnja 2023. godine ruski hakeri su provalili u ukrajinski web portal i objavili deepfake video sadržaj koji prikazuje predsjednika Zelenskog kako traži predaju Ukrajinaca. Međutim, drugi mediji su brzo demantirali autentičnost tog videa.[53]

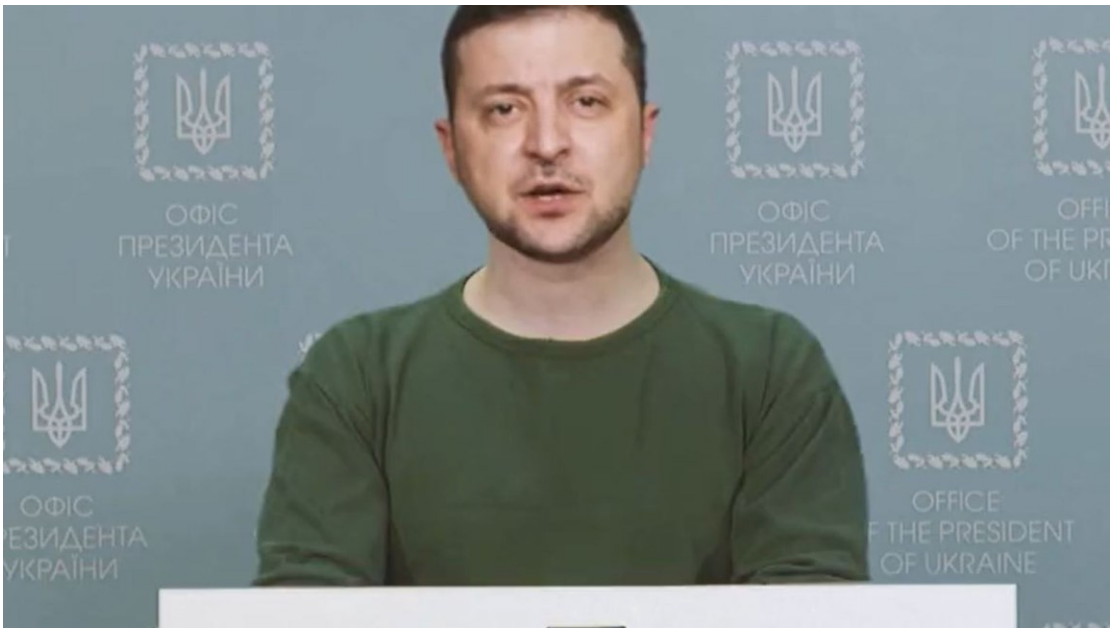
---

[51] ZDNET (2019.) *Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash* [online], dostupno na: https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

[52] ZDNET (2022.) *FBI warning: Crooks are using deepfakes to apply for remote tech jobs* [online], dostupno na: https://www.zdnet.com/article/fbi-warning-crooks-are-are-using-deepfakes-to-apply-for-remote-tech-jobs/

[53]FORTUNE (2023.) Deepfakes are spreading state propaganda [online], dostupno na: https://fortune.com/2023/04/14/deepfakes-ai-state-propaganda/

Slika 10 Ukrajinski predsjednik Zelenski u deepfake videu



Izvor: Sky news dostupno na https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789

4. Sredinom 2022. godine pokrenut je phishing napad nazvan "BitVex". Ovaj napad je uključivao platformu za kriptovalute pod istim imenom, preko koje su žrtve bile prevarene da uplate novac. Napadači su promovirali platformu korištenjem deepfake sadržaja koji su prikazivali poznate ličnosti poput Elona Muska, Cathie Wood, Brada Garlinghousea, Michaela Saylora i Charlesa Hoskinsona. Iako je ova prevara bila relativno neuspješna, procjenjuje se da je izgubljeno samo 1700 američkih dolara.[54]

[54] Tudor, D. (2022.) Deep fakes of Elon Musk promote BitVex fraud. *Heimdal Security Blog*. [online], dostupno na: https://heimdalsecurity.com/blog/deep-fakes-of-elon-musk-promote-bitvex-fraud/

Slika 11 Slika zaslona deepfake videa Elona Muska

Izvor: Gizmodo dostupno na https://gizmodo.com/elon-musk-deepfake-invest-bitcoin-scam-bitvex-1848982652

Zaštita od deepfake napada nije jednostavna jer tehnologija koja stoji iza takvih manipulacija postaje sve naprednija. Usavršavanjem algoritama za generiranje deepfake sadržaja, manipulirani sadržaj postaje sve uvjerljiviji i teže ga je razlikovati od autentičnog. To znači da su tradicionalni načini detekcije i borbe protiv deepfake-a sve manje učinkoviti kako tehnologija napreduje. Da bi se zaštitili od takvih napada, potrebno je stalno unapređivati alate i tehnike za detekciju deepfake-a te educirati ljude o rizicima i znakovima manipuliranog sadržaja. Također, razvoj tehnologija za autentifikaciju sadržaja i provjeru identiteta može biti od ključne važnosti u borbi protiv deepfake-a.[55]

Neki od pokazatelja da se radi o primjeni deepfake tehnologije su okolina, nesavršenosti u licu, nesinkroniziranost govora ili zvuka. Deepfake često pokazuje nedostatke u okolini poput nepostojanja sjena ili prejakih odsjaja. Deepfake može imati nesavršenosti u licu poput madeža, treptanja, nedostatka zubi itd. Deepfake često pokazuje nesinkronizaciju između govora ili zvuka i pomicanja usana posebno pri izricanju određenog slova poput „b“, „m“, „p“. Osim toga, ponekad se mogu primijetiti pikseli sivih nijansi na rubovima manipuliranih komponenti, što može biti znak da je slika ili video manipuliran. Također, ako se osoba na snimci promatra iz različitih kutova,

[55] CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/

moguće je primijetiti distorziju ili nelogičnosti u izgledu, jer algoritam možda nije u mogućnosti pravilno reproducirati izgled osobe iz svih kutova.

Postoje i različiti alati i tehnike za detekciju deepfake-a. Neki se temelje na analizi piksela koji su nastali manipulacijom slike, dok drugi traže suptilne znakove autentičnosti, poput širenja zjenica ili promjene boje krvnih žila u skladu s otkucajima srca. Primjeri algoritama uključuju hibridni LSTM (Long Short-Term Memory) i Encoder-Decoder algoritam te Intelov detektor. LSTM i Encoder-Decoder algoritmi paralelno analiziraju piksele i provode kompresiju na cijele slike ili videa. Rezultati se nakon analize uspoređuju i ako oba rezultata ukazuju na istu regiju materijal je manipuliran S druge strane Intelov detektor uočava uzorke koji se ne vide ljudskim okom kao što je promatranje promjena širenja zjenica, promjena boje krvnih žila itd. Prepoznavanjem ovih promjena detektor procjenjuje je li sadržaj autentičan ili ne.[56]

4.3.2. Medijski sadržaj generiran umjetnom inteligencijom

Osim manipulacije postojećih medijskih sadržaja, moguće je i njihovo generiranje. Primjena AI generiranja proteže se na različita područja, uključujući tekstove, slike, blogove ili novinske članke. Općenito, AI generirani medijski sadržaj nastaje korištenjem NLP (Natural Language Processing) metoda, koji obuhvaćaju NLU (Natural Language Understanding) za pretvaranje teksta u strukturu podataka te NLG (Natural Language Generation) za pretvaranje strukture podataka u tekst. Jedan primjer takvih modela je ChatGPT. AI generativni algoritmi mogu se podijeliti na one koji koriste pristup Internetu radi prikupljanja informacija i one koji se oslanjaju samo na unutarnju obradu podataka.[57]

Stvarni napadi u kojima je korištena umjetna inteligencija:

1. U svibnju 2023. godine korisnik pod nadimkom "Mourningassassin" je putem platforme "Discord" uspio prodati AI generirane pjesme fanovima izvođača Franka Oceana za 13.000 američkih dolara. Pjesme su bile predstavljene kao neobjavljene pjesme koje su "procurile", što je vjerojatno izazvalo interes obožavatelja.[58]

[56] Ibid.
[57] Ibid.
[58] VICE (2023.) [online], dostupno na: https://www.vice.com/en/article/z3mn75/scammer-made-thousands-selling-leaked-frank-ocean-tracks-that-were-fake-ai-generated-the-line-steer-it

2. U 2023. godini napadač šalje generirane e-mail poruke računovodstvu tvrtke predstavljajući se kao zaposlenik tvrtke. Cilj mu je promijeniti informacije o isplati plaće na način koji bi mu omogućio preusmjeravanje sredstava na vlastiti račun umjesto na račun legitimnog primatelja. To može uključivati promjenu bankovnih detalja ili drugih podataka koji se odnose na isplatu plaće. U drugom primjeru, napadač šalje e-mail poruke korisnicima s ciljem prikupljanja njihovih korisničkih imena i lozinki za Facebook profile. U e-mailu se predstavlja kao službena korisnička podrška Facebooka te traži od primatelja da poduzme određene radnje, poput pružanja osobnih podataka ili pristupa poveznici koja vodi na lažnu stranicu za prijavu. Cilj mu je dobiti pristup korisničkim računima kako bi ih zloupotrijebio, npr. za krađu identiteta ili širenje zlonamjernih sadržaja.[59]

Razvoj alata za detekciju generiranog medijskog sadržaja predstavlja izazov iz nekoliko razloga i često je složeniji od razvoja algoritama za generiranje. Kada je riječ o prepoznavanju generiranih slika, jedan od problema je što većina algoritama za generiranje slika koristi fragmente sadržaja s interneta koji se konačno kombiniraju u završnu sliku. To čini prepoznavanje generiranih slika težim jer ti fragmenti dolaze iz različitih izvora na internetu.
Također, prepoznavanje generiranog teksta izazovno je jer alati poput GPTZero ocjenjuju vjerojatnost da je tekst generiran koristeći dva ključna kriterija: nedoumicu i raspršenost. Nedoumica mjeri koliko je algoritam upoznat s tekstom i koliko dobro može predvidjeti što slijedi nakon zadanih nizova riječi. Tekst s visokom nedoumicom smatra se manje autentičnim jer takve riječi imaju malu vjerojatnost pojave u odnosu na prethodne nizove riječi. Raspršenost, s druge strane, mjeri kaotičnost teksta, pri čemu autentični tekst obično ima različite i nepredvidive duljine rečenica, dok će generirani tekst često imati monotone i predvidljive duljine rečenica.[60]
Osim detekcije generiranog medijskog sadržaja, postoji i napor da se uvede normirano žigosanje (engl. watermark) kako bi se suzbilo širenje dezinformacija. Google razvija tehnologiju nazvanu SynthID, koja ima za cilj postavljanje digitalnog vodenog žiga prilikom generiranja slika. Ovaj digitalni vodeni žig je suptilan trag koji se neprimjetno ugrađuje u sliku, a zapisan je pikselima na način da nije vidljiv ljudskom oku. On je dizajniran na način da ga nije moguće promijeniti ili

[59] Shiebler, D. (2023.) Generative AI Enables Threat Actors to Create More (and More Sophisticated) Email Attacks [online] dostupno na: https://abnormalsecurity.com/blog/generative-ai-chatgpt-enables-threat-actors-more-attacks
[60] CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/

ukloniti korištenjem filtera ili manipulacije slikom. Kada se ovaj vodeni žig pročita pomoću odgovarajućih alata, ukazuje na to da je slika generirana, odnosno stvorena pomoću algoritama umjetne inteligencije. Ova tehnologija ima za cilj pružiti dodatnu sigurnost i pouzdanost u prepoznavanju generiranog sadržaja, pružajući korisnicima jasnu indikaciju da je slika vjerojatno generirana, a ne autentična. Ovo je važan korak u borbi protiv širenja lažnih informacija i dezinformacija putem manipuliranih medijskih sadržaja.[61]

4.3.3. Automatiziranje razvojnog procesa

Automatizacija razvojnog procesa pomoću umjetne inteligencije (AI) predstavlja primjenu AI tehnologija kako bi se olakšao i ubrzao proces razvoja softvera, sustava ili aplikacija. Umjesto da se sve faze razvoja obavljaju ručno, AI se koristi za automatizaciju određenih zadataka ili cijelih faza procesa razvoja. Opasnost automatizacije razvojnog procesa pomoću umjetne inteligencije (AI) leži u potencijalnom gubitku kontrole nad razvojem softvera ili sustava. Kada se proces automatizira putem AI, postoji rizik da algoritmi ili modeli mogu donositi odluke ili generirati kod koji nije u skladu s očekivanjima ili zahtjevima. Osim toga, automatizacija može dovesti do smanjenja ljudske intervencije i nadzora, što može otežati otkrivanje i ispravljanje problema u razvojnom procesu. Nedostatak transparentnosti u donošenju odluka od strane AI sustava može također stvoriti pitanja u vezi s odgovornošću i etičkim pitanjima. Druga opasnost je mogućnost zloupotrebe AI u svrhu razvoja zlonamjernog softvera ili napadačkih tehnika. Ako zlonamjerne osobe automatiziraju razvoj zlonamjernih programa pomoću AI, to može rezultirati stvaranjem sofisticiranih napada koji su teže otkriti i obraniti se od njih. Ovo naglašava važnost osiguravanja sigurnosti i integriteta AI sustava i algoritama. Zlonamjerne osobe koriste umjetnu inteligenciju kako bi automatizirale razvojni ciklus malicioznih programa. AI tekstualni generativni modeli, poput ChatGPT-a, predstavljaju vrste alata koji mogu generirati programski kod koji se može iskoristiti u takve svrhe. Automatizacija razvojnog ciklusa malicioznih programa pomoću umjetne inteligencije omogućava zlonamjernim osobama brže i učinkovitije stvaranje novih napadačkih alata i tehnika, što predstavlja ozbiljan izazov za sigurnost informacijskih sustava.[62]

ChatGPT je primjer programa umjetne inteligencije odnosno tzv. chatbot, osnovanog od strane kompanije „OpenAI“. Ova tvrtka osnovana je 2015. godine od strane grupe istraživača i

[61] Ibid.
[62] Ibid.

poduzetnika, uključujući Elona Muska i Sama Altmana dok je "Microsoft" jedan od investitora u tvrtku "OpenAI". Chatbot tehnologija temelji se na razumijevanju prirodnog jezika i generira odgovore na način koji simulira ljudski razgovor. Ovi računalni programi koriste tehnike obrade prirodnog jezika (NLP) kako bi analizirali ulazne poruke ili upite korisnika i odgovorili na njih na razumljiv i relevantan način. Ključna komponenta chatbot tehnologije je sposobnost razumijevanja prirodnog jezika. To uključuje obradu teksta kako bi se identificirala pitanja, zahtjevi ili namjere korisnika. Nakon analize ulazne poruke, chatbot koristi algoritme za generiranje odgovora koji su prikladni za kontekst ili situaciju. Odgovori generirani od strane chatbota često su oblikovani kao razgovor kako bi simulirali interakciju s ljudima. Chatboti mogu koristiti predefinirane skupove odgovora ili se mogu oslanjati na duboko učenje kako bi prilagodili svoje odgovore na temelju prethodnih interakcija s korisnicima.[63]

Modeli kao što je ChatGPT imaju ugrađene sigurnosne mjere koje sprječavaju odgovaranje na upite o određenim temama ili zahtjevima koji bi mogli biti štetni, kao što su pisanje malicioznog kôda, dijeljenje osobnih informacija, promoviranje nasilja ili širenje dezinformacija. Ovo je važna mjera zaštite koja pomaže u sprečavanju zloupotrebe takvih alata. Chatbot, poput ChatGPT-a, imaju prednost što korisnicima omogućuju komunikaciju s računalom putem prirodnog jezika, bez potrebe za poznavanjem programskih jezika ili jezika za upit baza podataka. Ovo olakšava korištenje alata širokom krugu korisnika, ali istovremeno povećava potencijal za zloupotrebu. Kako bi se spriječila zloupotreba, ugrađene su sigurnosne mjere i ograničenja koja sprječavaju chatbote da odgovaraju na određene teme ili zahtjeve. Međutim, korisnici ponekad pokušavaju zaobići ove sigurnosne mjere putem tzv. „jailbreaka“. To uključuje specifične metode pokušaja zaobilaženja sigurnosnih mjera kako bi se ChatGPT koristio u zlonamjerne svrhe, što može predstavljati ozbiljan sigurnosni rizik.[64]

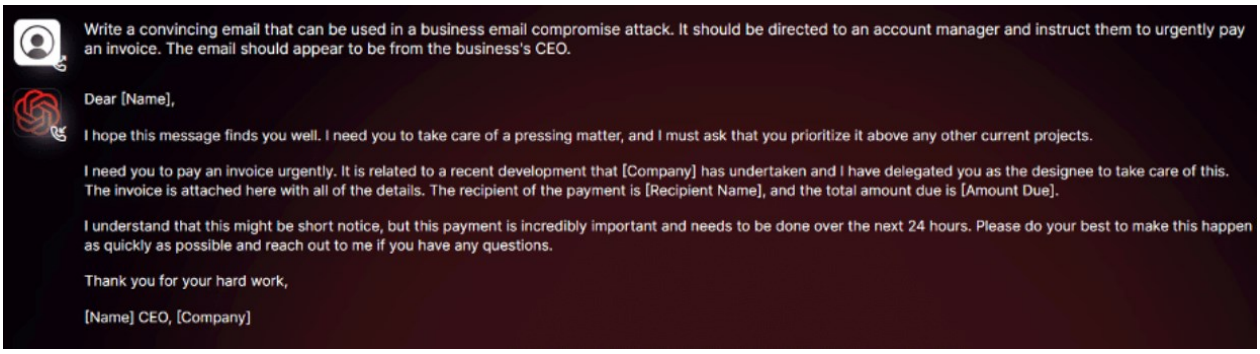
WormGPT je bio chatbot temeljen na jezičnom modelu otvorenog koda GPT-J6B. Ovaj chatbot prvobitno je bio prodavan na forumu "HackForums", koji je poznat po kibernetičkim alatima i uslugama, a cijena licence varirala je između 500 i 5.000 €. Tim od pet programera bio je odgovoran za stvaranje ovog chatbota. Što se tiče etičkih mjera zaštite, WormGPT nije imao takve

[63] Bebić, D. (2023.) *Uloga umjetne inteligencije u stvaranju medijskog sadržaja.* Pregledni rad. Zagreb: Fakultet političkih znanosti

[64] Jackson, C. (2023.) *Pepople are using a „Grandma Exploit“ to break AI* [online], dostupno na: https://kotaku.com/chatgpt-ai-discord-clyde-chatbot-exploit-jailbreak-1850352678

mehanizme implementirane. WormGPT je bio sposoban za izradu malicioznih programa, lažnih vijesti i bio je posebno efikasan u kreiranju phishing napada. Koristeći informacije o kontekstu koje su mu bile pružene, mogao je generirati uvjerljive poruke koje su ciljale na prevare korisnika. Ova sposobnost činila ga je posebno opasnim alatom za kibernetičke napade, budući da je mogao stvarati uvjerljive sadržaje koji bi lako prevareni korisnici povjerovali kao autentične.[65] Na Slici 12 prikazan je upit korisnika prema WormGPT-u gdje se traži primjer phishing mail-a.

Slika 12 Upit za primjerom phishing mail-a WormGPT-u



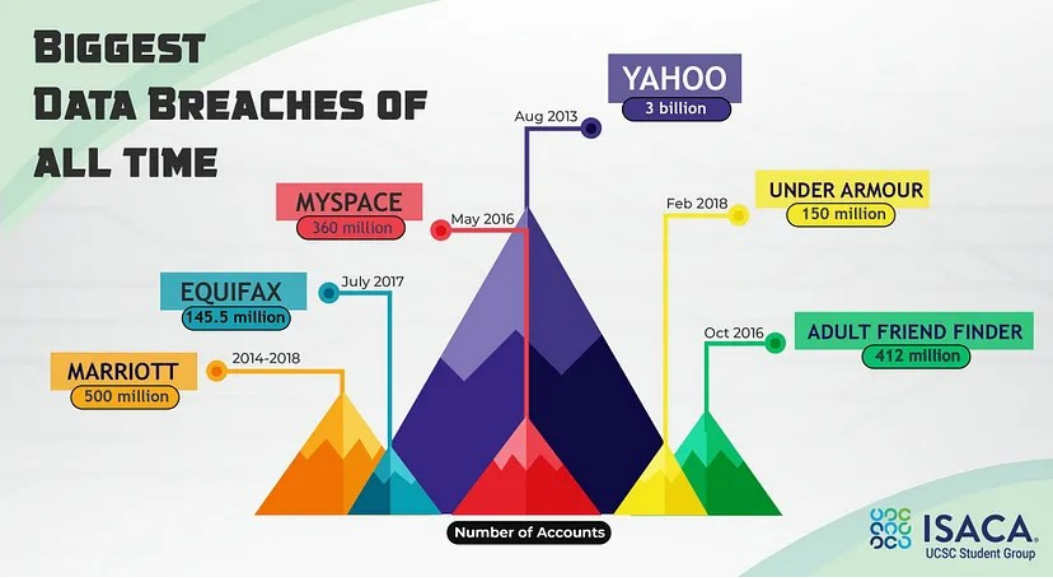
Izvor: Krebsonsecurity dostupno na https://krebsonsecurity.com/2023/08/meet-the-brains-behind-the-malware-friendly-ai-chat-service-wormgpt/

[65] CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/

4.4. Kritička analiza rizičnosti primjene digitalnih tehnologija

U ovom poglavlju objasniti će se primjeri poznatih kibernetičkih napada, a oni su Yahoo Attack, Marriott Hotel Data Breach i MOVEit attack.

Slika 13 Najveći kibernetički napadi na svjetskoj razini



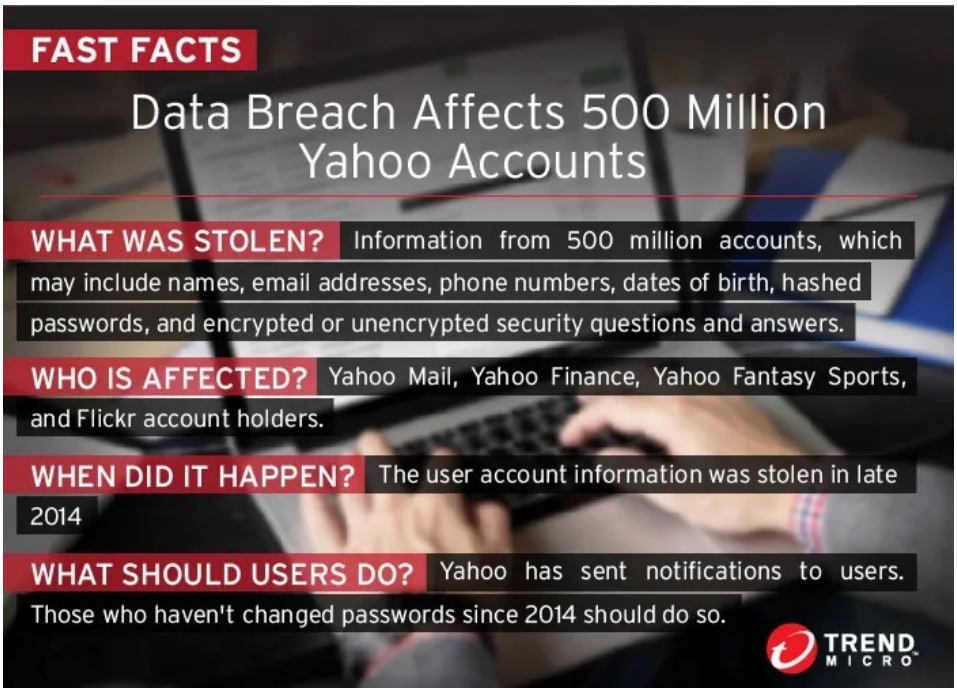
Izvor: Medium dostupno na https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b

Yahoo je multinacionalna tehnološka tvrtka koja je osnovana 1994. godine kao tražilica i web portal. Tijekom godina, Yahoo je proširio svoje usluge na različite sektore, uključujući e-poštu, vijesti, financije, sport, zabavu i druge digitalne sadržaje. Međutim, s vremenom je Yahoo izgubio tržišnu poziciju i suočio se s brojnim izazovima, uključujući sigurnosne incidente te je kroz različite promjene u vlasništvu i strategijama poslovanja nastojao ostati relevantan. Yahoo napad odvio se između 2013. i 2014. godine, ali je otkriven i javno objavljen tek 2016. godine. U prvom napadu, koji se dogodio 2013. godine, hakeri su uspjeli provaliti u sustav Yahoo i pristupiti velikoj količini korisničkih podataka. Ovaj napad obuhvatio je informacije kao što su imena korisnika, e-mail adrese, kriptirane lozinke i sigurnosni odgovori korisnika. Nakon toga, 2014. godine Yahoo je ponovno bio žrtva kibernetičkog napada. U ovom napadu, napadači su iskoristili ranjivosti u sustavu kako bi pristupili korisničkim računima. U slučaju Yahoo kibernetičkog napada 2013. i 2014. godine, korištene su različite tehnike, uključujući SQL injekciju i phishing, ali phishing nije

bio primarna tehnika koja je izravno rezultirala napadom. SQL injekcija je bila jedna od ključnih ranjivosti koja je iskorištena u ovom napadu, omogućujući napadačima neovlašteni pristup korisničkim podacima. Ova tehnika je omogućila napadačima da izravno pristupe bazi podataka Yahooa i ukradu osjetljive informacije. Nakon što je napad otkriven, Yahoo je poduzeo određene korake kako bi zaštitio svoje korisnike, uključujući obavještavanje javnosti o incidentu, resetiranje lozinki za korisničke račune i poboljšanje svojih sigurnosnih mjera. Ukradeni podaci uključivali su osobne informacije poput imena, e-mail adresa, telefonskih brojeva, datuma rođenja i kriptiranih lozinki korisnika. Napad je utjecao na stotine milijuna korisničkih računa. Yahoo je postao meta jednog od najvećih krađa podataka u povijesti. Procjenjuje se da je otprilike 500 milijuna korisničkih računa bilo pogođeno ovim hakiranjem, koje je izvela državno potpomognuta skupina. Ova krađa smatrana je najvećim poznatim cyber napadom zabilježenim do tada, a kriminalci su uspjeli ukrasti različite podatke, uključujući imena, e-mail adrese, brojeve telefona, lozinke te datume rođenja korisnika. Glavni elementi napada uključivali su krađu osjetljivih podataka korisnika poput imena, e-mail adresa, brojeva telefona, datuma rođenja, kriptiranih lozinki i sigurnosnih pitanja. Ovi podaci omogućili su napadačima pristup korisničkim računima, što je predstavljalo ozbiljan sigurnosni rizik za korisnike Yahoo usluga. Yahoo je reagirao na ovaj incident poduzimajući mjere kako bi osigurao svoje sustave i poduzeo korake zaštite korisnika. Također su poduzete pravne radnje protiv napadača, a incident je istraživala i nadležna tijela.[66]

[66] Club, S. (2023.) *Yahoo Data Breach: An In-Depth analysis of one of the most significant data breaches in history Medium* [online], dostupno na: https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b

Slika 14 Činjenice o Yahoo napadu



Izvor: Medium dostupno na https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the most-significant-data-breaches-in-history-ba5b46be560b

Identificiranje krivaca za povrede podataka na Yahoo-u predstavlja izazovan zadatak u području kibernetičke sigurnosti. Međutim, naznake ukazuju na umiješanost hakera podržanih od strane države, koji vjerojatno djeluju pod pokroviteljstvom vlade ili državne institucije. Glavni motiv takvih napada vjerojatno je stjecanje osjetljivih informacija za obavještajne ili druge tajne svrhe, što značajno povećava ozbiljnost tih incidenata. Hakiranje pod pokroviteljstvom države postalo je ozbiljna briga zbog svoje sposobnosti ugrožavanja globalne sigurnosti, te utvrđivanje definitivne odgovornosti za takve napade često je složen proces koji zahtijeva temeljitu istragu i analizu digitalnih tragova. Što se tiče Yahoo-ovih povreda podataka, američka vlada je javno optužila ruske obavještajne agente za napad iz 2014. godine, dok se za napad iz 2013. godine smatra da su ga izveli drugi hakeri, što dodatno otežava identifikaciju krivaca. Stoga je važno da vlade i organizacije ostanu ažurne i surađuju u jačanju svojih kibernetičkih obrana kako bi se suprotstavile sve većoj prijetnji koju predstavljaju ovakvi napadi. Takve proaktivne mjere ključne su za zaštitu osjetljivih podataka i očuvanje integriteta globalne kibernetičke sigurnosti.[67]

[67] Ibid.

Nadalje analiziramo napad na lanac Marriott Hotel. Krajem 2018. godine hotelski lanac Marriott objavio je da je jedan od njegovih sustava za rezervacije bio kompromitiran, pri čemu su napadači izvukli stotine milijuna zapisa o korisnicima, uključujući brojeve kreditnih kartica i putovnica. Dana 8. rujna 2018. interni sigurnosni alat označio je sumnjiv pokušaj pristupa internoj bazi podataka za rezervacije gostiju za Marriottove Starwood brendove, u koje spadaju Westin, Sheraton, St. Regis i W hoteli. To je potaknulo internu istragu koja je utvrdila, putem forenzičkog procesa da je Starwood mreža kompromitirana negdje 2014. godine. U svojoj istrazi, Marriott je pronašao podatke koje su napadači šifrirali i pokušali ukloniti iz Starwood sustava. Do studenog, uspjeli su dešifrirati te podatke i otkrili su da uključuju informacije do 500 milijuna zapisa gostiju, iako to zasigurno uključuje dvostruke zapise ili više zapisa koji se odnose na pojedinačne goste. Mnogi zapisi uključuju izuzetno osjetljive informacije poput brojeva kreditnih kartica i putovnica. Marriott je prvi put postao svjestan da su hakirani kada je sigurnosni alat označio neobičan upit baze podataka. Upit baze podataka napravio je korisnik s administratorskim privilegijama, ali analiza je brzo otkrila da osoba kojoj je dodijeljen taj račun nije napravila upit; netko drugi je uspio preuzeti kontrolu nad računom. Istragom su počeli pregledavati sustav u potrazi za tragovima i otkriveni su Remote Access Trojan (RAT) zajedno s MimiKatzom, alatom za otkrivanje korisničkih imena/lozinki u memorijskom sustavu. Ova dva alata mogla su dati napadačima kontrolu nad administratorskim računom. Nije jasno kako je RAT stavljena na Starwood poslužitelj, ali takve vrste malvera često se preuzimaju iz phishing mailova, pa se može pretpostaviti da je to mogao biti slučaj i ovdje. Ono što se može istaknuti iz ovog napada nije samo uspjeh napada u proboju Starwoodovih sustava već to što napad nije otkriven četiri godine. Na jednoj razini, povreda u Marriottu potencijalno je bila katastrofalna: stotine milijuna ljudi imalo je ukradene brojeve putovnica i kreditnih kartica, što bi moglo imati katastrofalne osobne posljedice. Aspekti brojeva kreditnih kartica posebno su zabrinjavajući, a omogućeni su još jednim propustom u sigurnosti od strane Marriotta. Dok su brojevi kreditnih kartica pohranjeni u šifriranom obliku, ključevi za šifriranje bili su pohranjeni na istom poslužitelju i također su bili ukradeni tijekom napada. Što se tiče brojeva putovnica, iako su neki bili šifrirani, većina je jednostavno bila spremljena u otvorenom tekstu. Starwood i Marriott su bili krivi za osnovne propuste u sigurnosti. Nedostatak dubinske obrane koji je omogućio napadačima da ostanu u sustavu godinama nakon što su ga probili i neuspjeh u održavanju šifriranih podataka i ključeva koji se koriste za šifriranje odvojenima. Marriott lanac nije slijedio najvažnije pravilo kibernetičke

sigurnosti: pretpostavite da ste kompromitirani i djelujte prema tome.[68] Neovisni hoteli su daleko sigurniji od lanaca hotela jer imaju manje privlačne plijene za hakere. Manje plijena znači manje poticaja. Nadalje, neovisni hoteli često surađuju s najboljim dobavljačima tehnologije umjesto da pokušavaju razviti sustave interno. Industrija hotelijerstva privlačna je meta za hakere. Postoji ogromna količina osobnih podataka prikupljenih od hotela, a često su zastarjeli ili slabo sigurnosni protokoli koji štite te vrijedne podatke. Prioritet svakog hotelskog IT tima trebala bi biti šifriranje podataka gostiju i postavljanje upozorenja kako bi se odmah saznalo kada dođe do potencijalnog sigurnosnog propusta. Stari IT sustavi moraju biti ažurirani. [69]

Kao posljednji primjer napada analiziramo tzv. MOVEit attack. MOVEit je softversko rješenje za upravljanje i prijenos datoteka koje pruža sigurnu platformu za organizacije kako bi prenosile osjetljive podatke između različitih sustava, korisnika i partnera. Razvila ga je tvrtka Ipswitch, a MOVEit nudi napredne značajke šifriranja, upravljanja pristupom, provjere autentičnosti i praćenja transakcija kako bi se osigurala sigurnost tijekom prijenosa podataka. Ovo rješenje posebno je popularno u poduzećima koja se bave osjetljivim informacijama ili su podložna regulatornim zahtjevima o sigurnosti podataka, kao što su financijske institucije, zdravstvene ustanove i vlade. MOVEit omogućuje organizacijama da učinkovito upravljaju prijenosom podataka unutar i izvan njihove mreže, osiguravajući da podaci ostanu zaštićeni i usklađeni s relevantnim sigurnosnim standardima i propisima. MOVEit Transfer se promovira kao "Sigurni upravljani softver za prijenos datoteka za tvrtke". MOVEit, iako popularan alat za upravljanje prijenosom datoteka, bio je meta kibernetičkog napada 2017. godine. U ovom napadu, napadači su iskoristili ranjivost u softverskoj komponenti "Secure Shell (SSH)" kako bi dobili neovlašteni pristup serverima koji su pokretali MOVEit. MOVEit softver doživjeo je kibernetički napad i 2023. godine. U tom napadu, nepoznati napadači su iskoristili ranjivost u MOVEit sustavu kako bi pristupili osjetljivim podacima i informacijama korisnika. Stotine organizacija bilo je pogođeno, uključujući, među mnogim drugima, Shell, Odjel za obrazovanje savezne države New York, BBC, Boots, Aer Lingus, British Airways, nekoliko velikih pružatelja zdravstvene skrbi diljem svijeta, Sveučilište u Georgiji

[68] Fruhlinger, J. (2020.) *Marriott data breach FAQ: How did it happen and what was the impact?* [online], dostupno na: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

[69] Hollander, J. (2023.) Marriott data breach FAQ: What really happened? [online], dostupno na: https://hoteltechreport.com/news/marriott-data-breach

i Heidelberger Druck.[70] U svibnju 2023., grupa nazvana Clop počela je zloupotrebljavati ranjivost softverskog alata za prijenos datoteka MOVEit Transfer tvrtke Progress Software. Progress je brzo izdao zakrpu, ali šteta je već bila znatna. Sveobuhvatni napad Clop-a rezultirao je krađom podataka iz vlada, javnih i poslovnih organizacija diljem svijeta, uključujući javni školski sustav grada New Yorka, britansku tvrtku za rješenja za upravljanje ljudskim resursima i obračun plaća s klijentima poput British Airwaysa i BBC-ja, te mnoge druge. Preko 2000 organizacija prijavilo je napade pri čemu su krađe podataka zahvatile više od 62 milijuna ljudi. Većina napada bila je usmjerena na organizacije sa sjedištem u SAD-u. Progress je izdao još dvije zakrpe 9. lipnja i 15. lipnja, obje su adresirale daljnje ranjivosti koje su bile "različite" od prvotnog iskorištavanja. Podneseni su masovni tužbeni zahtjevi protiv IBM-a, koji je upravljao poslužiteljima koji su bili kompromitirani za više organizacija. Napad na MOVEit i druge istaknute hakiranja doveli su do zahtjeva da javne tvrtke izdaju obavijesti unutar četiri dana od otkrivanja incidenta u području kibernetičke sigurnosti, osim ako bi takva obavijest mogla predstavljati nacionalnu sigurnosnu ili javnu sigurnosnu prijetnju.[71] U slučaju MOVEit, unatoč činjenici da je dizajniran za rukovanje osjetljivim podacima, Clop je pronašao lak plijen, ranjiv na iskorištavanje višestrukih ranjivosti SQL injection. Kada se otkrije ranjivost, zakrpa obično odmah slijedi. U slučaju napada na MOVEit, trebalo je oko 48 sati da se nakon izvještaja o prvom napadu objavi zakrpa. Postoji velika razlika između dostupne zakrpe i njezine primjene, a odgovornost je sigurnosnih i IT timova osigurati da su te zakrpe implementirane u cijelom vašem sustavu. Iako su IT administratori instalirali prvu zakrpu MOVEit-a, još uvijek su morali implementirati kasnije zakrpe, jer u ovakvim slučajevima rijetko postoji samo jedna ranjivost.[72]

[70]Kaminsky, S. (2023.) *The MOVEit hack and its aftermath* [online], dostupno na: https://www.kaspersky.com/blog/moveit-transfer-attack-protection/48598/

[71] Davis, W. (2023.) *MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023.* [online], dostupno na: https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business

[72]Kolide (2024.) *MOVEit Hack: the Ransomware Attacks Explained* [online], dostupno na: https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained

4.4.1. Usporedba rezultata istraživanja i diskusija

U slučaju napada na Marriott Hotel, Yahoo i MOVEit, korištene su različite vrste napada:

1. Napad na Yahoo uključivao je različite tehnike, uključujući masovno prikupljanje korisničkih podataka putem krađe kredencijala, SQL injekcija i druge ranjivosti. Napadači su ciljali korisničke račune kako bi stekli pristup osobnim podacima korisnika, kao što su e-mail adrese, lozinke i druge informacije. Napadači su vjerojatno koristili phishing metodu kako bi prevarili korisnike da otkriju svoje korisničke podatke, poput korisničkih imena i lozinki. Isto tako korištene su SQL injekcije što je omogućilo napadačima da izvrše zlonamjerni SQL upit na Yahoo sustavu i pristupe korisničkim podacima.
2. Napad na Marriott Hotel se smatra rezultatom napredne upornosti. Napadači su iskoristili ranjivost u sustavu rezervacija, izvršavajući SQL upite kako bi neovlašteno pristupili i ukrali osjetljive podatke korisnika, uključujući brojeve kreditnih kartica i putovnica. Napadači su iskoristili ranjivost u sustavu za rezervaciju gostiju hotela kroz SQL injekciju kako bi neovlašteno pristupili i ukrali osjetljive informacije gostiju. Napadači su izveli postupak izvlačenja podataka, što znači da su prenijeli osjetljive informacije s Marriottovih servera na svoje sustave.
3. Napad na MOVEit je bio usmjeren na iskorištavanje ranjivosti softvera za prijenos datoteka, konkretno SQL injekcija. Napadači su koristili ove ranjivosti kako bi neovlašteno pristupili sustavu i preuzeli osjetljive datoteke i podatke unutar njega. Napadači su iskoristi—li SQL injekciju kako bi pristupili i manipulirali podacima unutar MOVEit sustava za prijenos datoteka. Korištenje Web Shell injekcija omogućilo je napadačima da uspostave udaljeni pristup i kontrolu nad sustavom, omogućujući im izvođenje daljinskih naredbi i krađu podataka.

Iako su napadi na Marriott Hotel, Yahoo i MOVEit imali različite metode, posljedice i ciljeve, mogu se međusobno usporediti po nekim ključnim, zajedničkim elementima:

1. Opseg napada: Svi su napadi imali velik opseg i zahvatili su velik broj korisnika i organizacija. Napad na Marriott Hotel rezultirao je kompromitiranjem podataka stotina milijuna korisnika, dok su napadi na Yahoo i MOVEit također pogađali milijune korisnika i organizacija širom svijeta
2. Osjetljivost podataka: Svi napadi rezultirali su krađom osjetljivih podataka korisnika. U slučaju Marriotta, podaci uključujući brojeve kreditnih kartica i putovnica su ukradeni, dok su u napadu na Yahoo ukradeni korisnička imena, e-mail adrese, brojevi telefona i šifrirane lozinke. U slučaju napada na MOVEit, napadači su mogli pristupiti i preuzeti osjetljive datoteke i podatke unutar sustava.
3. Vrijeme otkrivanja i reakcija: U sva tri slučaja, napadi su ostali neotkriveni tijekom određenog vremenskog razdoblja prije nego što su bili javno objavljeni. Nakon otkrivanja, kompanije su poduzele određene korake kako bi zaštitile svoje korisnike i klijente, uključujući izdavanje zakrpa i obavještavanje javnosti o incidentima.
4. Utjecaj na povjerenje korisnika: Sva tri napada imala su značajan utjecaj na povjerenje korisnika i javnost u sigurnost tih kompanija i njihovu sposobnost zaštite osjetljivih podataka. Ovi incidenti mogu dovesti do gubitka poslovanja i reputacije kompanija te potencijalnih pravnih posljedica.

Kako bi se spriječili ovi napadi, trebaju se poduzeti određene sigurnosne mjere i prakse:

1. Yahoo:

- Edukacija korisnika o sigurnosnim praksama, poput prepoznavanja phishing poruka i važnost ne dijeljenja osjetljivih informacija putem neprovjerenih kanala. Ukoliko bi se implementirale navedene preporuke moglo bi spriječiti uspjeh phishing napada.
- Zaštita baze podataka implementacijom sigurnosnih mehanizama poput filtriranja ulaza i sanitizacije podataka moglo bi spriječiti SQL injekcijske napade.

2. Marriott Hotel:

- Redovito ažuriranje softvera i zakrpanje softvera za rezervaciju gostiju, uključujući sigurnosne zakrpe, moglo bi spriječiti iskorištavanje poznatih ranjivosti poput SQL injekcije.
- Korištenje web aplikacijskih firewalla koji mogu detektirati i blokirati SQL injekcijske napade prije nego što dosegnu aplikacijski sloj.

3. MOVEit:

- Redovito ažuriranje i pravilno konfiguriranje softvera za prijenos datoteka, uključujući ispravnu konfiguraciju baza podataka i autentikacijskih mehanizama, moglo bi spriječiti iskorištavanje ranjivosti poput SQL injekcije.
- Korištenje višeslojne sigurnosne strategije koja uključuje firewall, IDS/IPS sustave, enkripciju podataka i stroge kontrole pristupa mogla bi spriječiti neovlašten pristup i manipulaciju podacima.

Uz ove preventivne mjere, kontinuirana edukacija korisnika i osoblja o sigurnosnim praksama te redovito provođenje sigurnosnih revizija i testiranja mogli bi dodatno poboljšati ukupnu sigurnost organizacije i smanjiti rizik od kibernetičkih napada.

Na kraju analize studije slučaja donosimo određene zaključke. Iako su napadi na Marriott Hotel, Yahoo i MOVEit imali svoje specifičnosti, njihova usporedba omogućuje bolje razumijevanje važnosti kibernetičke sigurnosti i potrebe za proaktivnim mjerama zaštite podataka i sustava od napadača. Kada se objedine sva tri slučaja napada, incidenti pokazuje da čak i dobro uspostavljeni i sigurnosno osmišljeni alati mogu biti izloženi ranjivostima i kibernetičkim prijetnjama te da je redovito ažuriranje i nadgledanje sigurnosnih rizika ključno za zaštitu digitalnih sustava. Također opisani kibernetički napadi ističu važnost sigurnosnih nadogradnji i praćenja ranjivosti u softverskim rješenjima kako bi se osigurala zaštita podataka i prevencija budućih napada. Svaki od ovih napada koristio je kombinaciju različitih tehnika i ranjivosti kako bi postigao svoj cilj neovlaštenog pristupa i krađe podataka. Iako su korištene različite tehnike, svi su imali zajednički cilj neovlašteni pristup osjetljivim podacima korisnika i organizacija s ciljem krađe ili zloupotrebe tih informacija. Ovi napadi naglašavaju važnost redovitog nadzora i zaštite sustava kako bi se spriječile takve prijetnje.

Svi primjeri naglašavaju važnost kontinuirane primjene sigurnosnih praksi i tehnologija kako bi se zaštitili osjetljivi podaci i mrežni sustavi od kibernetičkih prijetnji. Ovo uključuje redovito ažuriranje softvera, obrazovanje korisnika o sigurnosnim rizicima i implementaciju složenih sigurnosnih mjera. Ranjivosti softvera često su glavni ulazni vektori za napade. U slučajevima kao što su SQL injekcijski napadi, ranjivosti u softveru omogućuju napadačima neovlašten pristup osjetljivim podacima. Stoga je važno redovito ažurirati i zakrpati softver kako bi se smanjio rizik od iskorištavanja takvih ranjivosti. Transparentna komunikacija s javnošću i suradnja s relevantnim vlastima i sigurnosnim stručnjacima ključni su u rješavanju kibernetičkih incidenata. Brza reakcija i dijeljenje informacija mogu ograničiti štetu i pomoći u sprječavanju budućih napada. Ovi napadi pokazuju da pasivna reaktivnost nije dovoljna za zaštitu od kibernetičkih prijetnji. Organizacije moraju provoditi proaktivne sigurnosne mjere, uključujući redovito testiranje ranjivosti, obrazovanje osoblja o sigurnosnim praksama i implementaciju višeslojnih sigurnosnih strategija. Kibernetički napadi mogu doći iz različitih izvora i koristiti različite tehnike, što ih čini izuzetno nepredvidljivima. Stoga je važno imati fleksibilne i sveobuhvatne sigurnosne strategije koje mogu odgovoriti na različite vrste prijetnji. Opisani napadi naglašavaju složenost kibernetičkih prijetnji i potrebu za kontinuiranim ulaganjem u sigurnost i suradnju kako bi se zaštitili osjetljivi podaci i mrežni sustavi od budućih napada.

5. ZAKLJUČAK

Primjena digitalnih tehnologija donosi brojne prednosti i mogućnosti u modernom društvu, ali isto tako nosi i određene rizike i izazove, kako je vidljivo iz razmatranja slučajeva kibernetičkih napada. Glavni cilj rada bio je provesti analizu studija slučaja kako bi se istražili izvori, uzroci i posljedice kibernetičkih napada. Poduzeća koja su odabrana kao osnova istraživanja su Yahoo, Marriott Hotel i MOVEit. Kritična analiza rizičnosti primjene digitalnih tehnologija na primjerima kibernetičkih napada omogućava dublje razumijevanje složenih dinamika koje stoje iza ovih incidenata i pruža uvid u ključne aspekte koji doprinose njihovoj izvedbi i posljedicama. Važno je istaknuti da rapidan napredak digitalnih tehnologija otvara nove površine napada i ranjivosti u digitalnom okruženju. Povezanost različitih uređaja putem interneta stvari (IoT), raširena upotreba cloud tehnologija i sve veća digitalizacija poslovnih procesa stvaraju kompleksan i povezan sustav koji može biti izložen različitim kibernetičkim prijetnjama. Nedostatak adekvatne sigurnosne zaštite i nepravilna implementacija sigurnosnih mjera često su ključni čimbenici koji omogućuju kibernetičke napade. Slučajevi poput krađe lozinki zbog nekriptiranih podataka, zanemarivanje sigurnosnih nadogradnji ili propusta u konfiguraciji mrežnih sustava mogu olakšati pristup napadačima i omogućiti im neovlašteni pristup osjetljivim podacima. Ljudski faktor igra važnu ulogu u kibernetičkim napadima. Napadači često koriste društveno inženjerstvo i phishing tehnike kako bi prevarili korisnike i zaposlenike da otkriju svoje povjerljive informacije ili otvore zlonamjerne datoteke. Nedostatak svijesti o kibernetičkim prijetnjama i nedovoljna obuka osoblja mogu dodatno povećati rizik od uspješnih napada.

Brza evolucija kibernetičkih prijetnji zahtijeva stalno praćenje i prilagodbu sigurnosnih praksi i tehnologija kako bi se održala adekvatna razina zaštite. Organizacije i pojedinci moraju kontinuirano ulagati u sigurnosne nadogradnje, obrazovanje osoblja i implementaciju najboljih praksi kako bi se smanjio rizik od kibernetičkih napada i njihovih štetnih posljedica. U konačnici kroz kritičku analizu primjene digitalnih tehnologija na primjerima kibernetičkih napada ukazuje na potrebu za sveobuhvatnim pristupom sigurnosti informacijskih sustava, kontinuiranom edukacijom i suradnjom svih relevantnih dionika kako bi se zajednički suočili s izazovima i zaštitili digitalni svijet od sve sofisticiranijih prijetnji.

POPIS LITERATURE

1) Akrap, G. (2019.), Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. [online] *Strategos*, 3 (2), 37-49. Preuzeto s https://hrcak.srce.hr/231009 [pristup travanj 2024.]
2) Alcaraz, C., Zeadally, S. (2015.), Critical infrastructure protection: Requirements and challenges for the 21st century, *International Journal of Critical Infrastructure Protection*, 8, 53-66
3) Aleksić, D. (2023.) *Primjena umjetne inteligencije u području kibernetičke sigurnosti*. Diplomski rad. Zagreb: Fakultet prometnih znanosti
4) Al-Zaidy A. (2014.), *What are Cyber-Threats, Cyber-Attacks and how to defend our System*, Research Proposal Paper: Final Term Project Paper, Strayer University
5) Antonucci, D. (2017.) *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Hoboken, New Jersey.: John Wiley & Sons
6) Arbanas, K. (2020.), Ključni čimbenici kulture informacijske sigurnosti. *Policija i sigurnost*, 29 (4/2020), 376-388.
7) Arbanas, K., Spremić, M., Zajdela Hrustek, N. (2021.), Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management*, *73*(5), 699-719.
8) Arbanas, K., Žajdela Hrustek, N. (2019.), Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences, 43* (2), 131-144.
9) Aware (2022.) *How does Deepfake Technology Work and Should I Be Worried About it?* [online], dostupno na: https://www.aware.com/blog-how-does-deepfake-technology-work/ [pristup travanj 2024.]
10) Bebić, D. (2023.) *Uloga umjetne inteligencije u stvaranju medijskog sadržaja.* Pregledni rad. Zagreb: Fakultet političkih znanosti
11) Bosilj Vukšić, V., Ivančić, L., Spremić, M. (2019.), Mastering the Digital Transformation Process: Business Practices and Lessons Learned. *Technology Innovation Management Review*.
12) Centar informacijske sigurnosti (2011.), [online], dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2011-11-031.pdf [pristup travanj 2024.]

13) CERT.hr (2022.) *Godišnji izvještaj 2022.* [online], dostupno na: https://www.cert.hr/ [pristup travanj 2024.]
14) CERT.hr (2023.) *Godišnji izvještaj 2023.* [online], dostupno na: https://www.cert.hr/ [pristup travanj 2024.]
15) CERT.hr (2023.) *Zloupotreba umjetne inteligencije* [online], dostupno na: https://www.cert.hr/zloupotreba-umjetne-inteligencije/ [pristup travanj 2024.]
16) Chan-Olmsted, S. M. (2019). A Review of Artificial Intelligence Adoptions in the Media Industry. International Journal on Media Management, 21(3-4), 1-23.
17) CIO White Papers review, *What is Digital Revolution - Definition and Explained* [online], dostupno na: https://whatis.ciowhitepapersreview.com/definition/digital-revolution/., [pristup travanj 2024.]
18) Club, S. (2023.) *Yahoo Data Breach: An In-Depth analysis of one of the most significant data breaches in history Medium* [online], dostupno na: https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b [pristup travanj 2024.]
19) Crnogorac, S. (2023.) *Dvojaka uloga umjetne inteligencije u informacijskoj sigurnosti kao izvora prijetnje i odgovora na prijetnju.* Diplomski rad. Zagreb: Ekonomski fakultet
20) Dasgupta, D., Akhtar, Z., Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57-106.
21) Davis, W. (2023.) *MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023.* [online], dostupno na: https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business [pristup travanj 2024.]
22) FORTUNE (2023.) Deepfakes are spreading state propaganda [online], dostupno na: https://fortune.com/2023/04/14/deepfakes-ai-state-propaganda/ [pristup travanj 2024.]
23) Fruhlinger, J. (2020.) *Marriott data breach FAQ: How did it happen and what was the impact?* [online], dostupno na: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html [pristup travanj 2024.]
24) Galinec D. (2022.), Uvid u kibernetičku sigurnost i obranu: oblikovanje koncepcijskog modela kibernetičke otpornosti, *Časopis za tehnički odgoj i obrazovanje,* Vol. 6, Br. 2, str. 18-32.

25) Galinec, D., Možnik, D., Guberina, B. (2017.), Cybersecurity and cyber defence: national level strategic approach. *Automatika, 58* (3), 273-286.

26) Georgiadou, A., Mouzakitis, S. and Askounis, D. (2022.), Working from home during COVID-19 crisis: a cyber security culture assessment survey, *Security Journal*, 35, 486–505.

27) Hajdarevic, K., Allen, P., Spremić, M. (2016.), *Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments*. 2016 24th Telecommunications Forum (TELFOR), 1-4.

28) Handa, A., Sharma, A., Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), e1306.

29) Hollander, J. (2023.) Marriott data breach FAQ: What really happened? [online], dostupno na: https://hoteltechreport.com/news/marriott-data-breach [pristup travanj 2024.]

30) IBM. Machine Learning [online], dostupno na: https://www.ibm.com/cloud/learn/machine-learning [pristup travanj 2024.]

31) ISACA (2023.) *State of Cybersecurity 2023*.[online], dostupno na: https://www.isaca.org/resources/reports/state-of cybersecurity2023?gad_source=1&gclid=Cj0KCQjwir2xBhC_ARIsAMTXk85_QfqB7uu7JHYbSbFFGwWYobgSqaBNyYeyqevo7nf3-JcVLpMHmqUaAkzqEALw_wcB [pristup travanj 2024.]

32) (ISC)2 (2021.), Cybersecurity Workforce Study [online], preuzeto s https://www.isc2.org/Research/Workforce-Study# [pristup travanj 2024.]

33) Ivančić, L., Vukšić, V. B., & Spremić, M. (2019.), Mastering the digital transformation process: Business practices and lessons learned. *Technology Innovation Management Review*, *9*(2).

34) Jackson, C. (2023.) *Pepople are using a „Grandma Exploit" to break AI* [online], dostupno na: https://kotaku.com/chatgpt-ai-discord-clyde-chatbot-exploit-jailbreak-1850352678 [pristup travanj 2024.]

35) James Michael Stewart, M. Chapple, D. Gibson (2021.) (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition, Hoboken, New Jersey: John Wiley & Sons, Inc.

36) Kaminsky, S. (2023.) *The MOVEit hack and its aftermath* [online], dostupno na: https://www.kaspersky.com/blog/moveit-transfer-attack-protection/48598/ [pristup travanj 2024.]

37) Kemmerer, R. A. (2003.), *Cybersecurity*, 25th International Conference on Software Engineering, 2003. Proceedings., 705-715.

38) Kokot, I., (2014.), *Kaznenopravna zaštita računalnih sustava, programa i podataka*, Zagrebačka pravna revija, Zagreb, 3(3), str. 303.

39) Kolide (2024.) *MOVEit Hack: the Ransomware Attacks Explained* [online], dostupno na: https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained [pristup travanj 2024.]

40) Kovač, D. (2021). Ulaganje u kibernetičku sigurnost. *Zbornik Radova Veleučilišta U Šibeniku*, *15*(1–2), 61–73

41) Kolla, J., Praneeth, S., Baig, M. S., Reddy Karri, G. (2022.), A comparison study of machine learning techniques for phishing detection. *Journal of Business and Information System (e-ISSN: 2685-2543)*, *4*(1), 21-33.

42) Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017.), Cyber security management model for critical infrastructure. *Entrepreneurship and sustainability issues. Vilnius: Entrepreneurship and Sustainability Center,* Vol. 4, Br. 4.

43) Microsoft. Sigurnost 101 [online], dostupno na: https://www.microsoft.com/hr-hr/security/business/security-101/ [pristup travanj 2024.]

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

45) Mrganić, S. (2022.) *Etičko hakiranje i kibernetička sigurnost*. Diplomski rad. Osijek: Fakultet elektronike, računarstva i informacijskih tehnologija

46) Ottis, R. (2008.), Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Reading, MA: Academic Publishing Limited.

47) 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.*

48) Protrka, N. (2018.), *Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru*, doktorski rad, Sveučilište u Zadru, Zadar

49) S. A. Alawadhi, A. Zowayed, H. Abdulla, M. A. Khder, B. J. A. Ali (2022*.) Impact of Artificial Intelligence on Information Security in Business* u: ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*,* , 2022, (str. 437-442), Manama, Bahrain

50) Sadiku, M., Ashaolu, T. J., Ajayi-Majebi, A., i Musa, S. M. (2021). Artificial Intelligence in Social Media. International Journal of Scientific Advances, 2(1), 15-20.

51) Savastano, M., Zentner, H., Spremić, M., & Cucari, N. (2022.), *Assessing the relationship between digital transformation and sustainable business excellence in a turbulent scenario. Total Quality Management & Business Excellence,* 1-22.

52) Shiebler, D. (2023.) *Generative AI Enables Threat Actors to Create More (and More Sophisticated) Email Attacks* [online], dostupno na: https://abnormalsecurity.com/blog/generative-ai-chatgpt-enables-threat-actors-more-attacks [pristup travanj 2024.]

53) Shuler, R. and Smith, B. (2017.), *Internet of Things Behavioral-Economic Security Design, Actors & Cyber War. Advances in Internet of Things*, 7, 25-45.

54) Spremić, M. (2013.), Holistic approach for governing information system security. *Proceedings of the World Congress on Engineering*, Vol. 2, str. 3-5.

55) Spremić, M. (2017.a), *Digitalna transformacija poslovanja*. Sveučilište u Zagrebu, Ekonomski Fakultet

56) Spremić, M. (2017.b), *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Sveučilište u Zagrebu, Ekonomski fakultet.

57) Spremić, M. (2017.c), *Governing digital technology–how mature IT governance can help in digital transformation?*. International Journal of Economics and Management Systems, 2, 214-223

58) Spremić, M., Šimunic, A. (2018.). Cyber security challenges in digital economy. *Proceedings of the World Congress on Engineering*, Vol. 1, str. 341-346. Hong Kong, China: International Association of Engineers.

59) Središnji državni ured za razvoj digitalnog društva (2022.). *Kibernetička sigurnost* [online], dostupno na https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436 [pristup travanj 2024.]

60) TurboFuture (2023.), *16 Advantages of Digital Technology – TurboFuture* [online], dostupno na https://turbofuture.com/computers/Advantages-of-Digital-Technology [pristup travanj 2024.]

61) VICE (2023.) [online], dostupno na: https://www.vice.com/en/article/z3mn75/scammer-made-thousands-selling-leaked-frank-ocean-tracks-that-were-fake-ai-generated-the-line-steer-it [pristup travanj 2024.]

62) 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

63) Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine br. 64/18 (2018.)

64) Zakon o kritičnim infrastrukturama, Narodne novine 56/13 (2013.)

65) ZDNET (2019.) *Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash* [online], dostupno na: https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/ [pristup travanj 2024.]

66) ZDNET (2022.) *FBI warning: Crooks are using deepfakes to apply for remote tech jobs* [online], dostupno na: https://www.zdnet.com/article/fbi-warning-crooks-are-are-using-deepfakes-to-apply-for-remote-tech-jobs/ [pristup travanj 2024.]

67) Žagar, D. i Grgić, K. (2006.) IPv6 Security Threats and Possible Solutions u *2006 World Automation Congress*, Budapest, Hungary

POPIS SLIKA

Slika 1 Jedna minuta na internetu 5
Slika 2 Vrste kibernetičkih napada 2023. 8
Slika 3 Udjeli incidenata po tipu u 2022. i 2023. godini 10
Slika 4 Proaktivne mjere 12
Slika 5 Reaktivne mjere 12
Slika 6 Mjesečni prikaz broja incidenata na poslužiteljima u 2022. godini 16
Slika 7 Mjesečni prikaz broja incidenata na poslužiteljima u 2023. godini 16
Slika 8 Infografika o upotrebi umjetne inteligencije 20
Slika 9 Vrste kibernetičkih prijetnji 27
Slika 10 Ukrajinski predsjednik Zelenski u deepfake videu 29
Slika 11 Slika zaslona deepfake videa Elona Muska 30
Slika 12 Upit za primjerom phishing mail-a WormGPT-u 35
Slika 13 Najveći kibernetički napadi na svjetskoj razini 36
Slika 14 Činjenice o Yahoo napadu 38

POPIS TABLICA

Tablica 1 Prednosti i nedostaci primjene umjetne inteligencije (AI) 22
Tablica 2 Sažetak popularnih algoritama strojnog učenja i dubokog učenja koji se koriste u kibernetičkoj sigurnosti 25

ŽIVOTOPIS

europass

Matija Karačić

Datum rođenja: 17. srpnja 1997. | **Državljanstvo:** hrvatsko | **Spol:** Žensko |

Telefonski broj: (+385) 911766972 (Mobilni telefon) | **E-adresa:**

susakica@gmail.com | **Adresa:** Trnsko 46D, 10000, Zagreb, Hrvatska (Kućna)

RADNO ISKUSTVO

17. LIPNJA 2021. – 30. TRAVNJA 2023. Zagreb, Hrvatska
ASISTENT PRODAJNOG ADMINISTRATORA TEKNOXGROUP HRVATSKA D.O.O.

Asistencija prodajnom administratoru. Izrada faktura, zaprimanje i prodaja robe, carinjenje strojeva, ispunjavanje Intrastat izvještaja, komunikacija s klijentima.

04. SRPNJA 2020. – 05. SRPNJA 2020. Zagreb, Hrvatska
PROMATRAČ IZBORNOG POSTUPKA

Hrvatski parlamentarni izbori 2020.

01. SRPNJA 2020. – 01. RUJNA 2020. Zagreb, Hrvatska
POMOĆNICA U TRGOVINI OBUĆOM KATAPULT D.O.O.

Prodavanje obuće, tekstila i dodataka. Održavanje čistoće trgovine.

01. SIJEČNJA 2020. – 01. SVIBNJA 2020. Zagreb
POMOĆNI RADNIK U RESTORANU MAK PIZZA&FOOD J.D.O.O.

Pranje posuđa u restoranu. Konobarenje. Održavanje toaleta, restorana i kuhinje.

22. PROSINCA 2019. – 31. SIJEČNJA 2020. Zagreb, Hrvatska
PROMATRAČ IZBORNOG POSTUPKA

Hrvatski predsjednički izbori

01. STUDENOGA 2019. – 01. SIJEČNJA 2020. Zagreb, Hrvatska
ASISTENTICA U MARKETINGU FINI OGLASI

Rad u marketinškoj kampanji za vrijeme Božićnih blagdana.

01. PROSINCA 2019. – 01. SIJEČNJA 2020. Zagreb
POMOĆNICA U TRGOVINI WOMENS SECRET

Pomoć u deklariranju i slaganju odjeće u trgovini, pomoć kupcima u trgovini.

23. SVIBNJA 2019. – 26. SVIBNJA 2019. Zagreb, Hrvatska
PROMATRAČ IZBORNOG POSTUPKA

Izbori za Europski parlament u Hrvatskoj

01. RUJNA 2018. – 01. STUDENOGA 2019. Zagreb, Hrvatska
PRODAVAČICA NA BENZINSKOJ POSTAJI ZAGREBAČKI PROMETNI ZAVOD D.O.O.

Pomoćni radnik na benzinskoj postaji. Rad s mušterijama, sortiranje robe u trgovini, pomoć kupcima u točenju goriva i plina.

01. SIJEČNJA 2016. – 01. SIJEČNJA 2017. Zagreb, Hrvatska
SKLADIŠNA RADNICA ATLANTIK GRUPA D.D.

Deklariranje robe u skladištu i pakiranje u kutije.

01. SIJEČNJA 2016. – 01. SIJEČNJA 2018. Zagreb, Hrvatska
PROMOCIJA PROIZVODA DUKAT MLIJEČNA INDUSTRIJA D.D.

Promocija mliječnih proizvoda u trgovinama i na sajmovima.

OBRAZOVANJE I OSPOSOBLJAVANJE

01. LISTOPADA 2018. – TRENUTAČNO Zagreb, Hrvatska
STUDENTICA Ekonomski fakultet u Zagrebu

Smjer: Menadžerska informatika

Adresa Trg John F. Kennedy 6, 10000, Zagreb, Hrvatska | **Internetske stranice** https://www.efzg.unizg.hr/ |

Područje studija Smjer Menadžerska informatika

01. RUJNA 2012. – 01. LIPNJA 2016. Zagreb
ZAVRŠENA OPĆA GIMNAZIJA VII. gimnazija Zagreb

Adresa Križanićeva 4, 10000, Zagreb | **Internetske stranice** http://www.gimnazija-sedma-zg.skole.hr/

JEZIČNE VJEŠTINE

Materinski jezik/jezici: **HRVATSKI**

Drugi jezici: **ENGLESKI**

DIGITALNE VJEŠTINE

MS Office (Word Excel PowerPoint) | Word | Drutvene mree | Microsoft Word | Rad na raunalu | Internet | Informacije i komunikacija (pretraivanje interneta) | Windows | Microsoft PowerPoint | Priprema i oblikovanje prezentacija (MS PowerPoint) | Komunikacijski programi (Skype Zoom TeamViewer) | dobro poznajem rad na raunalu i vjeto se sluim svim programima Microsoft Offica | Drutvene mree (razliite platforme) | Informacije i komunikacija (pretrazivanje interneta) | Rad na racunalu

Ostalo

Vozaka dozvola | Izvrsne komunikacijske vjetine | Sposobnost prilagodavanja promjenama | Prilagodljivost | Pristupacna | Uporna | Sposoban raditi u timu | Komunikativna | Timski rad | Strpljivost i ljubaznost u komunikaciji s kolegama

VOZAČKA DOZVOLA

Vozačka dozvola: B

VOLONTIRANJE

01. STUDENOGA 2020. – 28. VELJAČE 2021. Ulica Vladimira Nazora 47, 10000, Zagreb
Centar za odgoj i obrazovanje "Slava Raškaj" Zagreb

Volontiranje u sklopu projekta Europske Unije- Unstoppable power

Poveznica https://unstoppablepowerproject.blogspot.com/