Kibernetičko pravo, sigurnost i zaštita osobnih podataka

Tipurić, Mateo

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

KIBERNETIČKO PRAVO, SIGURNOST I ZAŠTITA OSOBNIH PODATAKA

Mentor: dr. sc. Melita Milenković, mag. iur.

Student: Mateo Tipurić univ. bacc. ing. traff
JMBAG: 0117229712

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

KIBERNETIČKO PRAVO, SIGURNOST I ZAŠTITA OSOBNIH PODATAKA

CYBER LAW, SECURITY AND PROTECTION OF PERSONAL DATA

Mentor: dr. sc. Melita Milenković, mag. iur.

Student: Mateo Tipurić univ. bacc. ing. traff
JMBAG: 0117229712

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 28. travnja 2023.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Telekomunikacijska legislativa i standardizacija**

DIPLOMSKI ZADATAK br. 7301

Pristupnik: **Mateo Tipurić (0117229712)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Kibernetičko pravo, sigurnost i zaštita osobnih podataka**

Opis zadatka:

U uvodnom dijelu rada je potrebno obrazložiti pojam kibernetičkog prava. Također, u navedenom poglavlju je potrebno navesti povijest kibernetičkog prava u Republici Hrvatskoj i EU te objasniti što uključuje područje kibernetičkog prava. U sljedećem poglavlju je potrebno obrazložiti kibernetičku sigurnost te na koji način ista predstavlja zaštitu internetski povezanih sustava kao što su hardver, softver i podataka od kibernetičkih prijetnji. Nadalje, u istom poglavlju je potrebno nabrojiti i opisati vrste prijetnji, kao i poznatije kibernetičke napade kroz noviju povijest. U radu je potrebno navesti uredbe i direktive ENISA-e i Opću uredbu o zaštiti podataka 2016/679 (GDPR) te spomenuti Cybersecurity Act. U sljedećem poglavlju potrebno je navesti čemu služi računalstvo u oblaku te pitanje sigurnosti i privatnosti korisnika računalstva u oblaku, a time i njihova zakonska prava prilikom korištenja samog računalstva u oblaku. Potrebno je opisati prednosti i nedostatke računalstva u oblaku, potencijalne prijetnje i načine zaštite računalstva u oblaku. U posljednjem poglavlju rada je potrebno obrazložiti kako je ugrožena sigurnost osobnih podataka fizičkih osoba. Potrebno je nabrojati zakone o sigurnosti podataka u Republici Hrvatskoj i EU te sukladnost s GDPR-om i na koji način je moguće zaštititi krajnje korisnike i njihove osobne podatke.

Mentor:

dr. sc. Melita Milenković

Predsjednik povjerenstva za diplomski ispit:

Sadržaj

1. UVOD

Kibernetičko pravo bitno je u današnjem kontinuiranom porastu korisnikovog korištenja interneta za svakodnevne aktivnosti i poslovanja putem interneta. Kao što je korištenje tehnologije u sve većem porastu, tako je i sve veći broj kriminalaca na internetu koji to pokušavaju iskoristiti.

Cilj ovog diplomskog rada je upoznati prava i zakone korisnika interneta, upozoriti na moguće prijetnje te pokazati kako se zaštiti od istih. Ovaj diplomski rad opisat će pojam kibernetičkog prava, njegovu povijest u Europi i Republici Hrvatskoj i definirati područje kibernetičkog prava. Također, opisat će kibernetičku sigurnost i vrste prijetnji i zaštite korisnika protiv malicioznih napada kibernetičkih kriminalaca. Nadalje, obradit će područje računalstva u oblaku kao jedno od poznatih platformi za kriminalce na internetu. Na kraju rada, biti će opisana sigurnost osobnih podataka koja je ključna za korisnike kako bi zaštitili svoje podatke.

Ovaj diplomski rad strukturiran je kako slijedi. Nakon uvodnog poglavlja, drugo poglavlje govori o kibernetičkom pravu i zakonima koji obrađuju navedenu tematiku, povijest kibernetičkog prava na području EU i u Republici Hrvatskoj. Sljedeće, treće poglavlje, objašnjava kibernetičku sigurnost, moguće prijetnje i način zaštite protiv istih. Četvrto poglavlje opisuje računalstvo u oblaku, prednosti i nedostatke, prijetnje, sigurnost i zaštitu računalstva u oblaku. U šestom poglavlju pojašnjava se sigurnost osobnih podataka, vrste sigurnosti osobnih podataka, opisuju se zakoni o sigurnosti osobnih podataka u Republici Hrvatskoj te njihova sukladnost sa Općom uredbom o zaštiti podataka 2016/679 (dalje: GDPR).. Na kraju diplomskog rada dan je kratak zaključak te pregled korištene literature.

2. KIBERNETIČKO PRAVO

Kibernetičko pravo korisnicima interneta omogućuje pravnu zaštitu od mnoštva složenih i pravnih problema koji se pojavljuju. Jedno je od najnovijih područja pravnog sustava jer se internetska tehnologija razvija jako brzo. Kibernetički zakon pruža pravnu zaštitu ljudima koji koriste Internet, a uključuje fizičke osobe (pojedince) i pravne osobe (tvrtke, poduzeća i sl.). Razumijevanje zakona od najveće je važnosti za svakoga tko koristi Internet. Kibernetički zakon se također naziva i zakon interneta [1].

Kibernetički zakoni pomažu u smanjenju ili sprječavanju ljudi od kibernetičkih kriminalnih aktivnosti u velikim razmjerima uz pomoć zaštite pristupa informacijama od neovlaštenih osoba, slobode govora u vezi s korištenjem interneta, privatnosti, komunikacije, e-pošte, web stranica, intelektualnog vlasništva, hardvera i softvera, kao što su uređaji za pohranu podataka. Budući da se internetski promet ubrzano povećava iz dana u dan, to je dovelo do većeg postotka pravnih problema u cijelom svijetu. Kibernetički zakoni razlikuju se ovisno o zemlji i nadležnosti, kazna se kreće od novčane do zatvora, a provedba je izazovna [2].

Studija za procjenu utjecaja komunikacije na kibernetički kriminal identificirala je slične probleme na razini Europske unije i posebno naglasila sve veću ranjivost na rizike kibernetičkog kriminala za društvo, poslovanje i građane te povećanu učestalost i sofisticiranost kibernetičkog kriminala. Također je primijećen nedostatak koherentne politike i zakonodavstva na razini EU-a za borbu protiv kibernetičkog kriminala. [3]

Zakon kibernetike nudi pravnu zaštitu za ljude koji koriste internet, kao i internet poslovanje. Za korisnike interneta najvažnije je poznavati lokalno područje i kibernetičke zakone svoje zemlje prema kojima mogu znati koje su aktivnosti na mreži legalne, a koje nisu. Također, mogu spriječiti nesvjesni rad neovlaštenih aktivnosti [2].

Tri su glavne kategorije kibernetičkog kriminala. Te kategorije uključuju [1]:

- Zločini protiv ljudi - iako se zločini događaju na internetu, oni utječu na živote ljudi. Neki od tih zločina uključuju internetsko uznemiravanje i uhođenje, distribuciju dječje pornografije, razne vrste lažiranja, prijevare s kreditnim karticama, trgovinu ljudima, krađu identiteta i klevetu povezanu s internetom;

- Zločini protiv imovine - neki mrežni zločini događaju se protiv imovine, poput računala ili poslužitelja. Ovi zločini uključuju DDOS (eng. *Distributed denial of service*) napade, hakiranje, prijenos virusa, računalni vandalizam, kršenje autorskih prava i kršenje prava intelektualnog vlasništva;
- Zločini protiv vlasti - kad je kibernetički zločin počinjen protiv vlade, to se smatra napadom na suverenitet te nacije i ratnim činom te čak i činom terorizma. Kibernetički zločini protiv vlade uključuju hakiranje, pristup povjerljivim informacijama, kibernetičko ratovanje, kibernetički terorizam i piratski softver.

Ako neka osoba prekrši kibernetički zakon, protiv te osobe će se poduzeti mjere temeljem vrste kibernetičkog zakona koji je prekršio, države u kojoj živi, odnosno u kojoje je prekršio zakon. Postoji mnogo situacija kršenja zakona kao što je zakon koji se prekrši na web stranici. Tada će račun biti zabranjen ili suspendiran i blokirana IP (eng. *Internet Protocol*) adresa korisnika. Najvažnije je kazniti kriminalce ili ih dovesti iza rešetaka, jer većina kibernetičkog kriminala prelazi granicu kriminala koji se ne može smatrati uobičajenim kriminalom [2].

Slika 1. Kibernetičko pravo[1]

[1] Izvor: Norwich University. Career Paths in Information Security: What is Cyber Law?.Preuzeto sa: https://online.norwich.edu/academic-programs/resources/cyber-law-definition [Pristupljeno: lipanj 2023.]

U tijeku je revolucija u kriminalnim aktivnostima. To stvara velike probleme za provedbu zakona u gotovo svakom dijelu svijeta, probleme koji su rijetko bili tako sustavni i sveprisutni. Revolucija leži u načinima na koje umrežena računala i druge tehnologije dopuštaju počinjenje zločina na daljinu, putem interneta i bežičnih komunikacija. Zločinac više ne mora biti na mjestu zločina da bi lovio svoju žrtvu. Gotovo svakom zločinu dodana je mogućnost međunarodnog elementa, što znači da glomazni mehanizmi međunarodne suradnje mogu usporiti ili izbaciti iz kolosijeka mnogo više istraga nego ikad prije. Budući da se sve, od banaka preko telefonskih sustava do kontrole zračnog prometa i vojske, toliko oslanja na umrežena računala, malo je pojedinaca i institucija otpornih na ovu novu i prijeteću kriminalnu aktivnost [3].

Kibernetičko pravo svake godine postaje sve važnije. To je zato što je kibernetički kriminal u porastu. Za borbu protiv ovih zločina postoje nedavni trendovi u kibernetičkom zakonu. Takvi trendovi uključuju nove i strože propise, jačanje postojećih zakona, povećanje svijesti o pitanjima privatnosti, računalni oblak, osjetljivost virtualne valute na kriminal te korištenje analitike podataka. Stvaranje svijesti o ovim problemima bit će primarni fokus vlada i agencija za kibernetičko pravo u vrlo bliskoj budućnosti [1].

2.1 Povijest

U Republici Hrvatskoj, prvo pravo kazneno djelo računalnog kriminaliteta uvedeno je 1997. godine reformom hrvatskog kaznenog zakonodavstva. Kazneni zakon, NN 110/1997, čl. 223. pod nazivom „ Oštećenje i uporaba tuđih podataka“[2] navodi četiri odluke u slučaju kršenja zakona:

1) Tko ošteti, izmjeni, izbriše, uništi ili učini neuporabljivim tuđe automatski obrađene podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

2) Tko unatoč zaštitnim mjerama neovlašteno pristupi automatski obrađenim podacima ili računalnom programu, kaznit će se novčanom kaznom do sto pedeset dnevnih dohodaka ili kaznom zatvora do šest mjeseci.

[2] Oštećenje i uporaba tuđih podataka, NN 110/1997, čl. 223. [Izvor: https://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_110_1668.html, Pristupljeno: Svibanj 2023.]

3) Kazneni postupak za kazneno djelo iz stavka 1. ovoga članka, ako se ne radi o obrađenim podacima ili računalnim programima državnog tijela, pokreće se povodom prijedloga.
4) Posebne naprave i sredstva kojima je počinjeno kazneno djelo iz stavka 1. i 2. ovoga članka oduzet će se.

Iste te godine, Vijeće Europe osnovalo je Odbor stručnjaka za kriminalitet u kibernetičkom prostoru kako bi se suzbijao kriminalitet. Razlog tome bio je nagli razvoj informacijsko-komunikacijskih tehnologija, odnosno interneta, a time i kaznenih dijela na internetu[4].

Hrvatsko kazneno zakonodavstvo radi u skladu s Konvencijom o kibernetičkom kriminalu Vijeća Europe (NN - Međunarodni ugovori, broj 9/02 i 4/04). To je prvi prihvaćeni i potpisani multilateralni sporazum koji je posebno usmjeren na probleme računalnog kriminala [5].

Zakonom o izmjenama i dopunama Kaznenog zakona iz 2004. godine objavljenim u NN 105/2004[3] unijela je u kazneno zakonodavstvo novela članka 223. čime se promijenio naziv u „ Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava“. Velika kaznenopravna reforma u Republici Hrvatskoj dogodila se 2011. godine kada je donesen novi Kazneni zakon, objavljen u NN broj 125/11[4], koji je stupio prvim danom 2013.godine pod nazivom „Kaznena djela protiv računalnih sustava, programa i podataka[4].

Kaznena djela prema Hrvatskom kaznenom zakonodavstvu (NN broj 125/11) se nalaze u kaznenim djelima protiv računalnih sustava, programa i podataka (od 266. do 274. članka) [5], a obuhvaćaju:

- Neovlašten i nezakonit pristup tuđem računalnom sustavu ili računalnim podacima,
- Ometanje rada računalnog sustava,
- Oštećenje računalnih podataka,
- Neovlašteno presretanje računalnih podataka,
- Računalno krivotvorenje,
- Računalna prijevara,

[3] Narodne Novine, broj 105/11, [Izvor: https://narodne-novine.nn.hr/clanci/sluzbeni/2004_07_105_2027.html, Pristupljeno: Svibanj 2023.]
[4] Narodne Novine, broj 125/11, [Izvor: https://www.zakon.hr/z/98/Kazneni-zakon, Pristupljeno: Svibanj 2023.]

- Zlouporaba naprava,
- Djela protiv računalnih sustava, programa i podataka,

Međunarodna zajednica vidjela je da se opasnost od računalnog kriminala pojavljuje od 1980-ih, ali možda nije predvidjela njegov puni potencijal. Vijeće Europe napravilo je, vjerojatno ispred svog vremena, prvi pokušaj usklađivanja materijalnih zakona o računalnom kriminalu 1989. godine izdavanjem smjernica nacionalnim zakonodavcima u svojim državama članicama i preporuke da se razmotri minimalni popis kaznenih djela specifičnih za računala kako bi se osigurala jedinstvena europska kaznena politika u ovom području. Popis je uključivao osam kaznenih djela dopunjenih izbornom listom koja su sadržava dodatna četiri kaznena djela [3].

Osam kaznenih djela bili su:

- prijevara u vezi s računalom;
- računalno krivotvorenje;
- oštećenje računalnih podataka ili računalnih programa;
- računalna sabotaža;
- neovlašteni pristup;

- neovlašteno presretanje;
- neovlaštena reprodukcija zaštićenog računalnog programa;
- neovlaštena reprodukcija topografije)

Dopunjena izborna lista koja sadržava 4 dodatna kaznena djela su:

- izmjena računalnih podataka ili računalnih programa;
- računalna špijunaža;
- neovlaštena uporaba računala;
- neovlaštena uporaba zaštićenog računalnog programa).

Razvoj interneta i širenje računalne tehnologije stvorio je nove mogućnosti za one koji bi se bavili ilegalnim aktivnostima. Uspon tehnologije i internetske komunikacije nije samo proizveo

dramatičan porast učestalosti kriminalnih aktivnosti, već je rezultirao i pojavom onoga što se čini kao nova vrsta kriminalnih aktivnosti. Povećanje učestalosti kriminalnih aktivnosti i moguća pojava novih vrsta kriminalnih aktivnosti predstavljaju izazove za pravne sustave, kao i za provedbu zakona.

Vijeće Europe bilo je među prvim međunarodnim tijelima koja su reagirala kada je 1996. godine ovlastilo skupinu stručnjaka da sastave nacrt međunarodnog ugovora za rješavanje tog pitanja. Stručnjaci Vijeća Europe primijetili su da brzi razvoj u području informacijske tehnologije ima izravan utjecaj na sve dijelove modernog društva. Integracija telekomunikacijskih i informacijskih sustava, omogućavajući pohranu i prijenos, bez obzira na udaljenost, svih vrsta komunikacija otvara cijeli niz novih mogućnosti. Spajanjem na informacijsko komunikacijske usluge korisnici stvaraju svojevrsni zajednički prostor, nazvan „*cyber space*“, koji se koristi u legitimne svrhe, ali može biti i predmet zlouporabe. Takvi prijestupi u kibernetičkom prostoru ili su počinjeni protiv integriteta, dostupnosti i povjerljivosti računalnih sustava i telekomunikacijskih mreža ili se sastoje od upotrebe takvih mreža i njihovih usluga za počinjenje tradicionalnih kaznenih djela. Prekogranični karakter takvih kaznenih djela, koje je počinjeno putem interneta, u suprotnosti je s teritorijalnošću nacionalnih tijela za provođenje zakona.

Europska unija aktivna je na području kibernetičkog kriminala od početka novog tisućljeća, posebice od usvajanja Komunikacije o stvaranju sigurnijeg informacijskog društva 2001. godine poboljšanjem sigurnosti informacijskih infrastruktura i borbom protiv računalnog kriminala[5]. Komunikacija iz 2001. godine predložila je radnje u nizu područja, uključujući odgovarajuće materijalne i proceduralne zakonske odredbe za rješavanje domaćeg i transnacionalnog računalnog kriminala.

Nakon Komunikacije usvojeno je nekoliko važnih prijedloga. To uključuje Direktivu 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža, *OJ L 105*, koja više nije na snazi.[6], a bila je važan korak prema uspostavi

[5] EUR- Lex (COM (2000) 890 final), [Izvor: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF, Pristupljeno: Svibanj 2023.]

[6] Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža, OJ L 105, ista nije na snazi[Izvor: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32006L0024&from=EN , Pristupljeno: Svibanj 2023.]

usklađenog sustava za prikupljanje i pohranu podatke o prometu u EU, te Okvirnu odluku o napadima na informacijske sustave[7]. Okvirna odluka bila je pokušaj Europske unije da postigne minimalnu razinu približavanja u pogledu tri kaznena djela povezana s računalima (nezakonit pristup informacijskim sustavima, nezakonito ometanje sustava, nezakonito ometanje podataka), čije se definicije u velikoj mjeri temelje na onoj ili na onima iz Konvencije Vijeća Europe o kibernetičkom kriminalu. Međutim, Okvirna odluka nije dosegla višu razinu usklađivanja od Vijeća Europe, očekivano u pogledu primjenjivih sankcija.

Uz pitanja kaznenog prava, Europska unija također se pozabavila povezanim područjem opće kibernetičke sigurnosti s drugim priopćenjem iz 2001. godine, priopćenjem o mrežnoj i informacijskoj sigurnosti.[8] Politika kibernetičke sigurnosti od tada je razvijena kroz niz aktivnosti, kao npr. u Komunikacijama o strategiji za sigurno informacijsko društvo[9] i o borbi protiv neželjene pošte, špijunskog i zlonamjernog softvera[10], te u stvaranju ENISA-e (eng. *European Union Agency For Cybersecurity)*[11] 2004. godine. Glavni cilj ENISA-e je razviti stručnost za poticanje suradnje između javnog i privatnog sektora i pružanje pomoći Komisiji i državama članicama.

Na temelju ove linije politike, daljnji razvoj politike EU-a odavno je prepoznat kao prioritet od strane država članica i Komisije. Akcijski plan Vijeća i Komisije za provedbu Haaškog programa utvrdio je potrebu za hitnim djelovanjem za poboljšanje europske koordinacije i suradnje između jedinica za visokotehnološki kriminal u državama članicama i s privatnim sektorom. U tom kontekstu predviđeno je donošenje nove Komisije o kibernetičkom kriminalu i politici kibernetičke sigurnosti. Ovo priopćenje usvojeno je 22. svibnja 2007. godine.

Komisija je planirala provesti opću strategiju za borbu protiv kibernetičkog kriminala. Najvažnije aktivnosti predviđene za razdoblje od 2007. do 2009.godine uključivale su da će Komisija pomno pratiti rad mreže za 24-satne kontakte za međunarodni visokotehnološki kriminal,

[7] EUR- Lex (2005/222/JHA) , [Izvor: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32005F0222, Pristupljeno: Svibanj 2023.]
[8] EUR- Lex (COM(2001)298 final), [Izvor: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF, Pristupljeno: Svibanj 2023.]
[9] EUR- Lex (COM(2006)251 final), [Izvor: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF, Pristupljeno: Svibanj 2023.]
[10] EUR- Lex (COM(2006)688 Final), [Izvor: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:EN:PDF, Pristupljeno: Svibanj 2023.]
[11] ENISA(EUR-Lex, 2019/881), [Izvor: https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX%3A32019R0881, Pristupljeno: Svibanj 2023.]

a kojoj je značajan broj država širom svijeta, uključujući većinu država članica EU. Mreža G8 predstavlja mehanizam za ubrzavanje kontakata između država sudionica, s 24-satnim točkama kontakta za slučajeve koji uključuju elektroničke dokaze i one koji zahtijevaju hitnu pomoć stranih tijela za provođenje zakona. Plan komisije nastojao je međusobno povezati svaku novu ili postojeću mrežu diljem EU s mrežom G8 i drugim međunarodnim strukturama. Slično tome, Komisija će kao dio svojih međunarodnih obveza, poticati sve države članice da ratificiraju Konvenciju Vijeća Europe o kibernetičkom kriminalu i da se pridruže gore navedenoj mreži koja radi 24 sata dnevno, 7 dana u tjednu, s obzirom na dogovorenu važnost Konvencije i relevantnost njezinih odredbi u kojoj prilaže veliku pozornost prilikom definiranja svoje politike kibernetičkog kriminala[3].

2.2 Što obuhvaća područje kibernetičkog prava?

Glavna područja kibernetičkog prava uključuju [2]:

- Prijevaru - potrošači se oslanjaju na kibernetičke zakone koji ih štite od online prijevara. Postoje zakoni za sprječavanje krađe identiteta, krađe kreditnih kartica i drugih financijskih zločina koji se događaju na internetu. Osoba koja počini krađu identiteta može se suočiti s federalnom ili državnom kaznenom prijavom. Također bi se mogli suočiti s građanskom tužbom koju je pokrenula žrtva. Kibernetički odvjetnici rade na procesuiranju i obrani od optužbi za prijevaru korištenjem interneta.
- Autorska prava - internet je olakšao kršenje autorskih prava. Rani dani internet komunikacije učinili su kršenje autorskih prava lakim. Pojedinci i tvrtke trebaju odvjetnike za pokretanje postupaka za provođenje zaštite autorskih prava. Kršenje autorskih prava područje je kibernetičkog prava koje brani prava pojedinaca i tvrtki na zaradu od svojih kreativnih djela.
- Klevetu - mnogi ljudi koriste internet kako bi izrazili svoje mišljenje. Kada ljudi koriste internet kako bi rekli stvari koje nisu istinite, to može prijeći granicu klevete. Zakoni o kleveti su građanski zakoni koji štite pojedince od neistinitih javnih izjava koje mogu naštetiti poslovnom ili nečijem osobnom ugledu.
- Uznemiravanje i uhođenje - ponekad izjave na internetu mogu kršiti kaznene zakone koji zabranjuju uznemiravanje i uhođenje. Kada osoba daje ponavljajuće ili prijeteće izjave o nekom drugom na internetu, može prekršiti građanske i kaznene zakone. Odvjetnici

procesuiraju i brane ljude kada se uhođenje dogodi putem interneta i drugih oblika elektroničke komunikacije.

- Slobodu govora[12]- važno područje kibernetičkog zakona je sloboda govora. Iako zakoni zabranjuju određena ponašanja na internetu, zakoni o slobodi govora također dopuštaju ljudima da izraze svoje mišljenje. Odvjetnici moraju savjetovati svoje klijente o granicama slobode govora, uključujući zakone koji zabranjuju opscenost. Osim toga, odvjetnici mogu braniti svoje klijente kada se vodi rasprava o tome predstavljaju li njihovi postupci dopuštenu slobodu govora.
- Poslovne tajne - tvrtke koje posluju na internetu često se oslanjaju na kiber netički zakon kako bi zaštitile svoje poslovne tajne. Na primjer, *Google* i druge tražilice na internetu provode puno vremena razvijajući algoritme koji proizvode rezultate pretraživanja. Oni također provode mnogo vremena razvijajući druge značajke kao što su karte, inteligentna pomoć i usluge traženja letova. Odvjetnici pomažu svojim klijentima u poduzimanju pravnih radnji prema potrebi kako bi zaštitili svoje poslovne tajne.
- Ugovorna i radna prava - svaki put kada korisnik klikne gumb koji kaže da se slaže s odredbama i uvjetima korištenja web stranice, upotrijebio je kibernetički zakon. Ugovori štite pojedince i korporacije dok koriste tehnologiju i posluju putem interneta. Na primjer, klauzule o zabrani natjecanja u ugovorima o radu utjecale su samo na malo lokalno geografsko područje. Kako se sve više poslovanja seli na internet, način na koji odvjetnici sastavljaju te ugovore i način na koji ih sudovi provode mogu se promijeniti. Odvjetnici moraju raditi na zastupanju najboljih interesa svojih klijenata u područjima prava koja još uvijek mogu biti neriješena.
- Sporove oko domena[13]- kada se strane ne slažu oko toga tko je vlasnik ili tko bi trebao biti vlasnik web stranice, odvjetnici mogu uskočiti. Građanski spor može uključivati traženje novčane odštete ili sudsku zabranu kako bi se spriječilo ponašanje druge strane

[12] Sloboda govora- Internet nastoji potaknuti slobodan, suradnički stav prema dijeljenju informacija. Wikipedija je dobar primjer za to. U Wikipediji ljudi besplatno pišu, uređuju i provjeravaju ima li pogrešaka ili vandalizma za milijune tekstova na nekoliko jezika. Čineći to, oni omogućuju slobodan pristup golemoj količini znanja i informacija[6].

[13] Primjer spora oko domene je Micros0ft.com. Tvrtka Zero Micro Software dobila je registraciju za micros0ft.com (s nulom umjesto drugog 'o'), ali je registracija suspendirana nakon što je Microsoft uložio protest. Kada je naziv domene ukinut zbog neplaćanja naknada, naziv domene preuzeo Vision Enterprises iz Roanokea, Texas. [7]

- Širenje dezinformacija i netočnosti- jedna od najznačajnijih stvari u kibernetičkom pravu današnjice. Širenje lažnih informacija može nanijeti niz štetnih posljedica koje mogu rezultirati ugrožavanjem identiteta okrivljene osobe, zdravlja, sigurnosti itd. [8] Jedan od primjera su takozvani „*Clickbait*“ portali koji navode ljude da otvaraju članke radi svojih profita. Primjer *clickbait-a* je objava optužbe poznatog sportaša Cristiana Ronalda za utaju poreza i presudu od dvije godine zatvorske kazne [9].

Konvencija Vijeća Europe o kibernetičkom kriminalu[14], ETS. br. 185, kolektivni je odgovor članica Vijeća Europe i nekih država nečlanica izazovu kibernetičkog kriminala. Rezultat je to četiri godine intenzivnog rada stručnog povjerenstva kojem je Odbor ministara povjerio pripremu pravno obvezujućeg instrumenta temeljenog na prethodnim preporukama Vijeća Europe o problemima računalnog kriminala i kaznenog postupka povezanih s informacijskom tehnologijom. Glavni ciljevi Konvencije bili su utvrditi zajedničke definicije određenih kaznenih djela kako bi se zakonodavstvo moglo uskladiti na nacionalnoj razini, definirati zajednička pravila za istražne ovlasti koje su prilagođene okruženju informacijske tehnologije, odrediti tradicionalne i nove vrste međunarodne suradnje kako bi zemlje mogle surađivati, te brzo djelovati u svojim istragama i kaznenim progonima [3].

Prvi dio konvencije odnosi se na kaznena djela. Očekivano je da će, ako ih države ugovornice pravilno provedu, eliminirati probleme dvojne kažnjivosti. Kaznena djela, od kojih su mnoga već definirana u Preporuci o kriminalu povezanom s računalima[15] iz 1989. godine, a spadaju u četiri kategorije su:

- kaznena djela protiv povjerljivosti, integriteta i dostupnosti podataka ili računalnih sustava,
- kaznena djela povezana s računalom,
- kaznena djela povezana sa sadržajem,
- kaznena djela koja uključuju povredu intelektualnog vlasništva i srodnih prava.

[14] Konvencija Vijeća Europe o kibernetičkom kriminalu, ETS. br. 185, [Izvor: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf, Pristupljeno: Svibanj 2023.]
[15] Odbor ministra Vijeća Europe [Preporuka, br. 9 R(89)], [Izvor: https://rm.coe.int/09000016804f1094, Pristupljeno: Svibanj 2023.]

U prvoj kategoriji postoji šest kaznenih djela. Svi se tiču kaznenih djela čija su primarna meta računalni sustav ili podaci, stoga je usko povezana s računalnim okruženjem u kojem se događaju. Iako neka od tih kaznenih djela mogu imati ekvivalent u običnom svijetu, njihovo proglašenje vlastitim kaznenim djelima temeljilo se na jasnoj kaznenoj politici zaštite računalne mreže i podatke koje one sadrže. Stvarnu ili potencijalnu štetu uzrokovanu takvim računalnim prijestupima ne treba podcjenjivati. Upad u računalni sustav i unošenje virusa može lako dovesti do uništenja podataka ili cijelih sustava diljem svijeta zbog međusobne povezanosti mreža.

1) Kaznena djela u prvoj kategoriji nazivaju se "kaznena djela protiv povjerljivosti, cjelovitosti i dostupnosti podataka ili informacijskih sustava". Oni uključuju ilegalni pristup ili hakiranje koje Konvencija smatra osnovnim prekršajem jer može dovesti do drugih prekršaja, kao što je nezakonit pristup povjerljivim podacima, korištenje sustava bez plaćanja i drugi oblici računalne prijevare ili krivotvorenja. Mnoga nacionalna zakonodavstva već sadrže odredbe o kaznenim djelima hakiranja, ali se njihov opseg i sastavni elementi znatno razlikuju. Određene zemlje primjenjuju usku definiciju ili zahtijevaju dodatne kvalificirajuće okolnosti.
2) Drugo kazneno djelo u ovoj kategoriji je protuzakonito presretanje, koje je modelirano na povredu privatnosti, poput prisluškivanja i snimanja usmenih telefonskih razgovora, a primjenjuje se na sve oblike elektroničkog prijenosa podataka, bilo telefonom, faksom, elektroničkom poštom. ili prijenos datoteke. Prekršaj se odnosi na nejavne prijenose računalnih podataka. Priopćeni podaci mogu biti javno dostupni podaci, ali bitno je da strane žele komunicirati povjerljivo ili se podaci mogu čuvati u tajnosti u komercijalne svrhe dok se usluga ne plati. Međutim, u nekim zemljama presretanje može biti usko povezano s kaznenim djelom neovlaštenog pristupa računalnom sustavu. Kako bi se osigurala dosljednost zabrane i primjene zakona, zemlje koje zahtijevaju nečasnu namjeru ili da se kazneno djelo počini u odnosu na računalni sustav koji je povezan s drugim računalnim sustavom u skladu s odredbom o nezakonitom pristupu, mogu također zahtijevati slične kvalificirajuće elemente za pripisivanje kaznene odgovornosti za ovo djelo.

Odredba o ometanju sustava inkriminira djela računalne sabotaže. Kazneno djelo se sastoji u namjernom ometanju zakonite uporabe računalnih sustava, uključujući i telekomunikacijska sredstva, korištenjem ili utjecajem na računalne podatke. Za razliku od ometanja podataka, ometanje računalnih sustava mora biti ozbiljno da bi se smatralo kaznenim djelom. Svaka će

država ugovornica morati odrediti koji kriteriji moraju biti ispunjeni da bi se ometanje smatralo ozbiljnim. Na primjer, država može zahtijevati da se prouzroči minimalni iznos štete kako bi se ometanje smatralo ozbiljnim. Stručnjaci Vijeća Europe smatrali su ozbiljnim slanje podataka određenom sustavu u takvom obliku, veličini ili učestalosti da ima značajan štetan učinak na sposobnost vlasnika ili operatera da koristi sustav ili da komunicira s drugim sustavima, npr. putem programa koji generiraju napade uskraćivanja usluge, zlonamjernih kodova poput virusa koji sprječavaju ili značajno usporavaju rad sustava ili programa koji šalju ogromne količine elektroničke pošte primatelju kako bi blokirali komunikacijske funkcije sustava.

Kaznena djela u drugoj kategoriji pokrivaju računalne verzije dva kaznena djela, prijevare i krivotvorenja, koja se obično čine na tradicionalan način, u fizičkom svijetu. Ipak, prijevara ili krivotvorenje može se izvršiti i na računalnim mrežama, koje posljedično postaju sredstvo kojim se kazneno djelo počinje, umjesto da budu njegova meta. Oba su u osnovi ponašanja temeljena na manipulaciji. Takvo je ponašanje potrebno razdvojiti kao kaznena djela jer definicija tradicionalnih oblika , s obzirom na većinu nacionalnih zakona, implicira da se oni ne mogu primijeniti na radnje počinjene putem računalnih mreža. Štoviše, kada je prijevara ili krivotvorenje počinjeno putem računalnih mreža, veća je vjerojatnost da će veći broj ljudi pretrpjeti štetu. Njihovo uključivanje potvrđuje činjenicu da u mnogim zemljama određeni tradicionalni pravni interesi nisu dovoljno zaštićeni od novih oblika uplitanja i napada. Doista, s dolaskom tehnološke revolucije mogućnosti za počinjenje gospodarskih zločina kao što su prijevare, uključujući prijevare s kreditnim karticama, višestruko su se povećale. Imovina predstavljena ili administrirana u računalnim sustavima postala je meta manipulacija poput tradicionalnih oblika vlasništva. Ta se kaznena djela uglavnom sastoje od manipulacija unosom, pri čemu se u računalo unose netočni podaci ili programskih manipulacija i drugih smetnji u tijek obrade podataka.

Cilj odredbe o računalnim prijevarama je kriminalizirati svaku nedopuštenu manipulaciju, uključujući unos, izmjenu, brisanje, potiskivanje podataka kao i ometanje funkcioniranja računalnog programa ili sustava, tijekom obrade podataka s namjerom dobivanja nezakonitog prijenosa imovine. Cilj je odredbe o krivotvorenju putem računala stvoriti paralelno kazneno djelo s krivotvorenjem materijalnih isprava. Također, potrebno je popuniti praznine u kaznenom pravu koje se odnose na tradicionalno krivotvorenje, koje zahtijeva vizualnu čitljivost izjava ili izjava sadržanih u dokumentu i koje se tradicionalno ne primjenjuje na elektronički pohranjene podatke.

Manipulacije takvim podacima s dokaznom vrijednošću mogu imati iste ozbiljne posljedice kao i tradicionalne radnje krivotvorenja ako se treća strana time dovede u zabludu. Računalno krivotvorenje podrazumijeva neovlašteno stvaranje ili izmjenu pohranjenih podataka kako bi oni dobili drugu dokaznu vrijednost, a tijek pravnog prometa koji se oslanja na vjerodostojnost informacija sadržanih u podacima podložan je obmani.

3.) Treća kategorija kaznenih djela odnosi se na nezakonite sadržaje i uključuje niz radnji povezanih s dječjom pornografijom. Vijeće Europe je pri izradi Konvencije identificiralo ovu kategoriju nezakonitog sadržaja kao najopasniju u kontekstu računalnih mreža, koju je trebalo obraditi kaznenopravnim odredbama. Konvencija je u skladu s time razna djela od namjernog posjedovanja do proizvodnje i distribucije dječje pornografije učinila kaznenim djelima, čime su obuhvaćene sve moguće karike u lancu. Unatoč intenzivnim naporima, druge vrste nezakonitog sadržaja, posebice rasistička propaganda, nisu bile uključene među kaznena djela povezana sa sadržajem u samoj konvenciji, već su dodane kasnije u dopunskom protokolu.[16]

Odredba o dječjoj pornografiji nastoji ojačati mjere zaštite djece, uključujući zaštitu od seksualnog iskorištavanja, modernizacijom kaznenopravnih odredbi koje ograničavaju korištenje računalnih sustava u počinjenju seksualnih delikata protiv djece. Većina država već kriminalizira tradicionalnu proizvodnju i fizičku distribuciju dječje pornografije, ali uz sve veću upotrebu interneta kao primarnog instrumenta za trgovanje takvim materijalom, smatralo se da su posebne odredbe u međunarodnom pravnom instrumentu ključne za borbu protiv ovog novog oblika seksualnog iskorištavanja i ugrožavanja djece. Uvriježeno je mišljenje da takav materijal i online praksa igraju ulogu u podržavanju, poticanju ili olakšavanju seksualnih prijestupa protiv djece.

4.) Četvrta kategorija kaznenih djela uključuje povredu autorskog i srodnih prava putem računalnih mreža. Ova je kategorija također povezana sa sadržajem, ali sadržajem koji je legalan i zaštićen. Povrede prava intelektualnog vlasništva, posebice autorskog prava, među najčešćim su prekršajima na internetu, koji mogu prouzročiti znatnu štetu. Umnožavanje i širenje na Internetu zaštićenih djela, bez odobrenja nositelja autorskog prava, iznimno su česti. Takva zaštićena djela uključuju književna, fotografska, glazbena, audiovizualna i druga djela [3]. CC(eng. *Creative Commons)* je međunarodna neprofitna organizacija koja osnažuje ljude

[16] Dopunski protokol, ETS No. 189, [Izvor: https://rm.coe.int/168008160f , Pristupljeno: 24. kolovoza 2023.]

da rastu i održe uspješno zajedničko znanje i kulturu koja nam je potrebna za rješavanje najhitnijih svjetskih izazova i stvaranje svjetlije budućnosti za sve. Zajedno s globalnom zajednicom i brojnim partnerima, gradi kapacitete i infrastrukturu, razvija praktična rješenja i zalaže se za bolje dijeljenje koje je kontekstualno, uključivo, pravedno, pravedno, recipročno i održivo. [10] Lakoća s kojom se mogu napraviti neovlaštene kopije zahvaljujući digitalnoj tehnologiji i razmjeri reprodukcije i širenja u kontekstu elektroničkih mreža učinili su nužnim uključiti odredbe o kaznenopravnim sankcijama i poboljšati međunarodnu suradnju u ovom području. Konvencija predviđa da stranke moraju kriminalizirati namjerna kršenja autorskog prava i srodnih prava, koja se ponekad nazivaju i srodna prava, koja proizlaze iz sporazuma navedenih u članku, kada su takva kršenja počinjena putem računalnih sustava u komercijalnoj mjeri [3].

3. KIBERNETIČKA SIGURNOST

Kibernetička sigurnost je zaštita internetski povezanih sustava kao što su hardver, softver i podaci od kibernetičkih prijetnji. Koriste ju pojedinci i poduzeća za zaštitu od neovlaštenog pristupa podatkovnim centrima i drugim računalnim sustavima[11].

Snažna strategija kibernetičke sigurnosti može pružiti dobru sigurnosnu poziciju protiv zlonamjernih napada osmišljenih za pristup, izmjenu, brisanje, uništavanje ili iznuđivanje sustava i osjetljivih podataka organizacije ili korisnika. Također, kibernetička sigurnost je ključna u sprječavanju napada koji imaju za cilj onemogućiti ili poremetiti rad sustava ili uređaja [11].

Slika 2. Kibernetička sigurnost[17]

Prednosti implementacije i održavanja kibernetičke sigurnosti uključuju [11]:

- Zaštita poslovanja od kibernetičkih napada i povreda podataka,
- Zaštita podataka i mreža,
- Sprječavanje neovlaštenog pristupa korisnika,
- Poboljšano vrijeme oporavka nakon povrede,
- Zaštita za krajnje korisnike i krajnje uređaje,

[17] Izvor: Forage. What is Cybersecurity? Preuzeto sa: https://www.theforage.com/blog/careers/cybersecurity [Pristupljeno: lipanj 2023.]

- Usklađenost s propisima,
- Kontinuitet poslovanja,
- Poboljšano povjerenje u ugled tvrtke i povjerenje programera, partnera, kupaca, dionika i zaposlenika.

Snažna strategija kibernetičke sigurnosti ima slojeve zaštite za obranu od kibernetičkog kriminala, uključujući kibernetičke napade koji pokušavaju pristupiti, promijeniti ili uništiti podatke, iznuđivati novac od korisnika ili organizacije ili imaju za cilj ometanje normalnog poslovanja. Protumjere bi se trebale odnositi na [12]:

- Sigurnost kritične infrastrukture - nacionalni institut za standarde i tehnologiju stvorio je okvir za kibernetičku sigurnost kako bi pomogao organizacijama u ovom području.
- Mrežna sigurnost - sigurnosne mjere za zaštitu računalne mreže od uljeza, uključujući žičane i bežične veze.
- Sigurnost aplikacije - procesi koji pomažu u zaštiti aplikacija koje rade lokalno i u oblaku. Sigurnost bi trebala biti ugrađena u aplikacije u fazi projektiranja, uzimajući u obzir način na koji se postupa s podacima, provjeru autentičnosti korisnika itd.
- Sigurnost u oblaku – konkretno i povjerljivo računalstvo koje šifrira podatke u oblaku dok miruju i dok su u upotrebi za podršku privatnosti korisnika, poslovnim zahtjevima i usklađenosti s propisima.
- Informacijska sigurnost - mjere zaštite podataka, kao što je opća uredba o zaštiti podataka, koje štite korisnikove najosjetljivije podatke od neovlaštenog pristupa, izlaganja ili krađe
- Edukacija krajnjih korisnika - izgradnja svijesti o sigurnosti u cijeloj organizaciji kako bi se ojačala sigurnost krajnjih točaka.
- Planiranje oporavka od katastrofe - alati i procedure za odgovor na neplanirane događaje, kao što su prirodne katastrofe, nestanci struje ili sigurnosni incidenti, s minimalnim prekidima ključnih operacija.
- Sigurnost pohrane - čvrsta otpornost podataka s brojnim zaštitnim mjerama. To uključuje enkripciju i nepromjenjive i izolirane kopije podataka. Oni ostaju u istom skupu tako da se mogu brzo vratiti u radni odnos za podršku oporavku, minimizirajući utjecaj kibernetičkog napada.

- Mobilna sigurnost - omogućuje upravljanje i zaštitu mobilne radne snage sa sigurnošću aplikacija.

3.1. Vrste prijetnji i poznati kibernetički napadi

Stručnjaci za kibernetičku sigurnost naporno rade na uklanjanju sigurnosnih rupa. Napadači konstantno traže nove načine da izbjegnu obrambene mjere i iskoriste slabosti. Vrste kibernetičkih prijetnji uključuju:

- *Malware* - zlonamjerni softver koji se odnosi na varijante zlonamjernog softvera kao što su crvi, virusi, trojanci i špijunski softver koji omogućuju neovlašteni pristup ili uzrokuju štetu računalu. Napadi zlonamjernim softverom osmišljeni su da zaobiđu poznate metode otkrivanja, kao što su antivirusni alati koji traže privitke zlonamjernih datoteka [12]. Emotet Trojan, kralj zlonamjernog softvera, jedan je od najpoznatijih softvera. U 2021. godini, tijela za provođenje zakona i pravosudna tijela prekinuli su ono što se reklamira kao najopasniji zlonamjerni softver na svijetu, Emotet. Riječ je o računalnom zlonamjernom softveru, prvi put otkrivenom 2014. godine, a prvenstveno cilja na bankarske i zdravstvene institucije. Emotet je postao poznat 2018. godine nakon što je zarazio bolnicu Fürstenfeldbruck u Njemačkoj prisilivši ih da ugase 450 računala. Iste godine američko ministarstvo domovinske sigurnosti identificiralo ga je kao jedan od najrazornijih malwarea. Širi se prikupljanjem Outlooka, gdje trojanac čita e-poštu sa žrtvina računala i šalje phishing e-poštu koja sadrži word dokument žrtvinim kontaktima, čineći da se čini kao da je sadržaj iz pouzdanog izvora[13].
- *Ransomware* - vrsta zlonamjernog softvera koji zaključava datoteke, podatke ili sustave i prijeti da će obrisati ili uništiti podatke. Također, može prijetiti da će datoteke učiniti privatnim ili osjetljive podatke javnim, osim ako se ne plati otkupnina kibernetičkim kriminalcima koji su pokrenuli napad. Nedavni napadi ciljali su državne i lokalne vlasti koje je lakše probiti nego organizacije i pod pritiskom su plaćanja otkupnine kako bi se vratile aplikacije i web stranice na koje se građani oslanjaju [12]. WannaCry se u svibnju 2017. godine proširio poput digitalne epidemije i kao taoce držao datoteke 250 tisuća korisnika; Microsoft Windows korisnika u 150 zemalja. Hakerska skupina pod nazivom Shadow Brokers koristila je hack koji je navodno razvila američka Agencija za nacionalnu sigurnost pod nazivom EternalBlue kako bi iskoristila ranjivost u Microsoft Windows

računalima. Hakeri su šifrirali datoteke na računalu i tražili otkupninu u vrijednosti od 300 do 600 dolara u kriptovaluti Bitcoin. Britanski istraživač sigurnosti Marcus Hutchins zaustavio je WannaCry registracijom web domene u kodu zlonamjernog softvera [14].

- *Phishing* - oblik društvenog inženjeringa koji vara korisnike da daju vlastite podatke koji otkrivaju identitet ili osjetljive podatke. U *phishing* prijevarama, e-poruke ili tekstualne poruke izgledaju kao da dolaze od legitimne tvrtke koja traži osjetljive podatke, kao što su podaci o kreditnoj kartici ili podaci za prijavu [12]. Litvanac po imenu Evaldas Rimasauskas ukrao je preko 100 milijuna dolara od Facebooka i Googlea. Rimasauskas i njegovi suvjerenici stvorili su prilično uvjerljive krivotvorene račune e-pošte Quanta Computera sa sjedištem u Tajvanu, koji zapravo posluje s Facebookom i Googleom. Poslali su pažljivo izrađene phishing e-poruke s lažnim fakturama, ugovorima i pismima zaposlenicima oba tehnološka diva, lažno im naplaćujući milijune dolara u razdoblju od dvije godine između 2013. i 2015. Zaposlenici Facebooka i Googlea platili su više od 100 milijuna dolara. Bankovni računi Rimasauskasove lažne tvrtke, koje je navodno oprao preko banaka u Latviji, Cipru, Slovačkoj, Litvi, Mađarskoj i Hong Kongu [15].
- Insajderske prijetnje - Sadašnji ili bivši zaposlenici, poslovni partneri, izvođači ili osoba koja je u prošlosti imala pristup sustavima ili mrežama može se smatrati prijetnjom iznutra ako zlorabi svoje dozvole za pristup. Insajderske prijetnje mogu biti nevidljive tradicionalnim sigurnosnim rješenjima poput vatrozida i sustava za otkrivanje upada koji su usmjereni na vanjske prijetnje [9]. U srpnju 2020. Twitter je postao vijest o vjerojatnom insajderskom napadu. Računi visokog profila na Twitteru hakirani su i korišteni za nezakonite transakcije bitcoinom. Prikupljeni gubici procjenjuju se na 250 milijuna dolara. Uzrok je identificiran kao preuzimanje računa visokoprofiliranih korisnika Twittera, uključujući Baracka Obamu i Elona Muska. Prevaranti su koristili račune za promicanje bitcoin prijevare. Istraga napada na Twitteru otkrila je da su napadi potekli putem društvenog inženjeringa i telefonskog lažiranja. Napadi spearphishing bili su usredotočeni na Twitterov administratorski tim, koji je imao privilegirani pristup alatima za administratore računa. Istraga se još uvijek nastavlja, no vjeruje se da su hakeri uspjeli ući u Slack kanal Twitter administratora. Odatle je nedostatak brige o higijeni vjerodajnica doveo hakere do pristupa alatima za administraciju, omogućujući pristup korisničkim računima na Twitteru[16].

- Distribuirani napadi uskraćivanja usluge – napad koji pokušava srušiti poslužitelja, web stranicu ili mrežu preopterećujući ih prometom, obično iz više koordiniranih sustava. Napadi preplavljuju poslovne mreže putem jednostavnog protokola za upravljanje mrežom koji se koristi za modeme, pisače, preklopnike, usmjerivače i poslužitelje [12]. Najveći DDoS napad ikada desio se u rujnu 2017. godine. U ovom napadu hakeri su poslali pakete informacija na 180 tisuća web poslužitelja koji su Googleu poslali ukupno 2,54 Tbps informacija. Napad je identificiran u rujnu 2017. godine, no kasnije je otkriveno da su hakeri šest mjeseci usmjeravali više DDoS napada na Google. Google Cloud je tek više od tri godine kasnije, u listopadu 2020., javno objavio informacije o napadu [17].
- Napredne trajne prijetnje- uljez ili grupa uljeza infiltriraju se u sustav i ostaju neotkriveni dulje vrijeme. Uljez ostavlja mreže i sustave netaknutima tako da može špijunirati poslovne aktivnosti i ukrasti osjetljive podatke, izbjegavajući aktivaciju obrambenih protumjera [12]. *GhostNet* je naziv koji su istraživači dali operaciji kibernetičke špijunaže velikih razmjera koja je prvi put otkrivena 2009. godine. Izvedeni u Kini, napadi su bili uspješni u kompromitiranju računala u više od 100 različitih zemalja s fokusom na infiltraciju mrežnih uređaja povezanih s veleposlanstvima i vladinim ministarstvima . Na operacije se uglavnom gledalo kao na pokušaje Kine da se pozicionira kao predvodnica nadolazećeg „informacijskog rata". Ove napade karakterizirala je njihova zastrašujuća sposobnost da kontroliraju kompromitirane uređaje, pretvarajući ih u uređaje za slušanje daljinskim uključivanjem njihove kamere i funkcija snimanja zvuka [18].
- *Man in the middle* napadi - napad prisluškivanjem gdje kibernetički kriminalac presreće i prosljeđuje poruke između dvije strane kako bi ukrao podatke. Na primjer, na nesigurnoj mreži, napadač može presresti podatke koji se prenose između uređaja gosta i mreže [9]. Prvi zabilježeni napad takvog tipa u povijesti dogodio se puno prije nego što je internet uopće izumljen, a uključuje Guglielma Marconija, dobitnika Nobelove nagrade koji se smatra izumiteljem radija. Kada je pravni savjetnik Marconija, profesor Fleming, izvodio demonstraciju bežičnog prijenosa s jedne lokacije na drugu, gospodin Maskelyne, britanski mađioničar i izumitelj, svojim je prijemnikom presreo poruku koja je trebala biti poslana iz Cornwalla na Kraljevski institut i zatim prenio vlastitu poruku te time dokazao da Macroni nije bio u pravu i da poruke mogu biti presretnute i ometane.[19].

Ostali uobičajeni napadi uključuju botnete, napade po preuzimanju, setove za iskorištavanje, zlonamjerno oglašavanje, napade nabacivanjem vjerodajnica, napade skriptiranjem na više stranica, napade ubacivanjem SQL-a[18] (eng. *Structured Query Language*), kompromitaciju poslovne e-pošte itd.

Kibernetički napadi događaju se svaki dan i to čak svakih 39 sekundi. Bez obzira na motivaciju hakera, financijsku ili političku, ova učestalost kibernetičkog kriminala ima opsežne implikacije. U modernom digitalnom dobu napadi mogu zatvoriti nuklearnu elektranu, zaustaviti zaradu tvrtke ili ukrasti milijune korisničkih podataka, a sve to putem *phishing* e-pošte [20].

Kibernetički napadi motivirani su uglavnom novcem, pri čemu kibernetički kriminalci traže podatke koje mogu upotrijebiti u prijevari identiteta ili priliku da zadrže IT (eng. *Information Technologies*) sustave svojih meta za otkupninu. Predviđa se da će globalni trošak kibernetičkog kriminala do 2025.godine dosegnuti 10,5 milijardi dolara. Bilo je mnogo kibernetičkih napada kroz povijest, no neki su ostavili veći trag u tome [21].

Jedan od najstarijih i najpoznatijih kibernetičkih napada koji je utjecao na dvije istaknute vladine organizacije u Sjedinjenim Državama poznate kao DoD (eng. *Department of Defense*[19]) i NASA (eng. *National Aeronautics and Space*[20] *Administration*) desio se 1999. godine kada je haker tinejdžer provalio u mreže Ministarstva obrane i NASA-e. Napad je izvršio tako što je instalirao *backdoor* pristup poslužiteljima Ministarstva obrane i nastavio preuzimati softver od NASA-e vrijedan oko 1,7 milijuna dolara. Iako je napad imao minimalan učinak i nisu procurili nikakvi osobni podaci, doveo je do prekida rada NASA-ine mreže na tri tjedna. Nadalje, tinejdžer je optužen za napad i suočen je sa 6 mjeseci pritvora [20].

CardersMarket[21], zloglasni napad, dogodio se 2007. godine kroz višestruke napade i žrtve na crnom webu. Točnije, dogodilo se na konkurentskim tržištima preprodavača kreditnih kartica koje je napadač iskoristio za izgradnju vlastite baze podataka sa dva milijuna kartica te štetom od

[18] *Structured Query Language* je standardizirani programski jezik koji se koristi za upravljanje relacijskim bazama podataka i izvođenje različitih operacija nad podacima u njima. U početku stvoren 1970-ih, SQL redovito koriste ne samo administratori baza podataka, već i programeri koji pišu skripte za integraciju podataka i analitičari podataka koji žele postaviti i pokrenuti analitičke upite.
[19] engl. *Department of Defense, DoD* - Odjel obrane; izvor: [22].
[20] engl. *National Aeronautics and Space Administration, NASA* – Nacionalna zrakoplovna i svemirska agencija: izvor: [23].
[21] CardersMarket napad; izvor: [20].

87 milijuna dolara u lažnim kupnjama. To je osakatilo konkurente i dovelo do jednog od najvećih kibernetičkih napada ikada. Napad je izvršio pojedinac poznat na internetu kao The Iceman, ili njegovo pravo ime: Max Butler. Na kraju je priznao krivnju za dvije točke optužnice za prijevaru putem interneta s kaznom od 14 godina, što je u to vrijeme bila najveća kazna bilo kojeg hakera u Americi. Također mu je naređeno da plati gotovo 40 milijuna dolara odštete [20].

Početkom 2009. godine Heartland Payment Systems objavio je da su njegovi sustavi probijeni u prethodnoj godini. Budući da je Heartland jedan od 5 najvećih kartičnih procesora podataka na svijetu, stručnjaci za sigurnost procjenjuju da je povreda utjecala na čak 100 milijuna kartica i više od 650 tvrtki za financijske usluge. Optuženo je više napadača, uključujući Alberta Gonzaleza i dvojicu Ruskih državljana. Kao odgovor na napad, Visa je uklonila Heartland iz svojih sustava na kratko vrijeme dok tvrtka ne potvrdi svoju usklađenost s PCI DSS (eng. *The Payment Card Industry Data Security Standard*). Nadalje, Heartland je šifrirao cijeli svoj informacijski sustav računa kako bi omogućio end-to-end enkripciju, što je označilo novi trend povećane sigurnosti za industriju obrade kartica [20].

Nadalje, napad na Playstation network 2011. godine pamte stručnjaci za sigurnost i igrači jer je označio jednu od najvećih povreda podataka ikada, u to vrijeme, sa 77 milijuna pogođenih računa i gotovo mjesec dana gašenja mreže. Zbog napada Sony je morao zatvoriti PlayStation Network na 23 dana, što je tvrtku koštalo procijenjenih 171 milijun dolara. Iako točan napadač nikada nije identificiran, tvrtka je nadoknadila pogođenim korisnicima s besplatnim mjesecom njihove usluge premium pretplate. Nadalje, tvrtka je pokrenula novu policu osiguranja od krađe identiteta od milijun dolara za sve korisnike. Ured britanskog povjerenika za informiranje kaznio je Sony s 250.000 funti zbog kršenja britanskog Zakona o zaštiti podataka. Nakon toga, 27. travnja 2011. Kristopher Johns iz Alabame objavio je tužbu u ime svih korisnika PlayStationa, tvrdeći da Sony „nije uspio šifrirati podatke i uspostaviti odgovarajuće vatrozide za rješavanje nepredviđenih slučajeva upada na poslužitelj." Druga tužba iz Kanade protiv Sony USA, Sony Canada i Sony Japan traži odštetu do milijardu kanadskih dolara [21].

Napad na Saudi Aramco 2012. godine srušio je najveće svjetske proizvođače nafte i odgodio proizvodnju. Hakiranje se dogodilo s virusom poznatim kao *Shamoon*, koji je bio modularan i

višestruk poput Stuxneta[22], ali je imao samo jednu svrhu, a to je pronaći i uništiti podatke. Napadom su kibernetički kriminalci uspjeli uništiti podatke na trideset tisuća računala, što je dovelo do gubitka ogromne količine informacija i zaustavljanja poslovanja u tvrtki. Iako je ovaj napad imao ograničen utjecaj na Aramcoov novčani tok, vrijedan je pažnje jer je bio snažan primjer kibernetičkih napada koji utječu na fizički svijet. Sumnja se da je krivac za napad Iran. Naime, američke obavještajne agencije identificirale su Iran kao napadača, no Iran je to opovrgnuo, optužujući Jemen [20].

Kroz dva napada, Yahoo je 2013. i 2014. godine pretrpio najveće povrede podataka ikad. Iako nije prijavljeno do 2016. godine, postalo je poznato kao najveća povreda podataka u povijesti interneta. Proboj su izvršile četiri osobe optužene za slučaj, koji su proveli ruski agenti kroz shemu unajmljivanja hakera. Samo se jedan od četiri muškarca ikada suočio s optužbama, g. Baratov, a završio je s pozamašnim novčanim kaznama i petogodišnjom zatvorskom kaznom. Iako je teško izmjeriti utjecaj ovog napada na milijarde krajnjih korisnika, sigurnosni istraživači primijetili su da je otvorio vrata zabrinjavajućim slučajevima kibernetičke špijunaže za ciljane napade na visokorangirane dužnosnike američke obavještajne službe koji su bili pogođeni provalom.

Godine 2021. napadnut je sustav naftovoda, što je dovelo do najvećeg napada na naftnu infrastrukturu u Sjedinjenim Državama. Naftovod, kojim upravlja Colonial Pipeline, prenosio je benzin kroz cijeli jugoistočni dio Sjedinjenih Država. Tvrtka je bila prisiljena zatvoriti naftovod nakon što je *malware* zarazio sustav koji kontrolira protok nafte kroz njihove cjevovode. Iako je tvrtka radila s FBI-em i platila otkupninu od 4,4 milijuna dolara putem Bitcoina, to je ipak dovelo do višednevnog gašenja sustava. To je bilo zbog dugog vremena obrade da bi ponovno postao operativan. Učinak ovog napada imao je posljedice u stvarnom svijetu, pri čemu su države koje su bile najteže pogođene, poput Virginije, vidjele da je 71% njihovih benzinskih postaja u Charlotte-u ostalo bez goriva. Unatoč ogromnom negativnom utjecaju, nitko nije službeno optužen za napad, a točan krivac do danas ostaje neutvrđen.

U prosincu 2015. sofisticirani kibernetički napad na elektroenergetsku mrežu Ukrajine ostavio je više od 200 000 ljudi bez struje na nekoliko sati, označavajući prvi uspješan kibernetički napad na nacionalnu infrastrukturu. Napad, koji se pripisuje grupi hakera poznatoj kao SandWorm

[22] Napad na Saudi Aramco; izvor: [20].

povezanoj s Rusijom, uključivao je korištenje zlonamjernog softvera BlackEnergy, kao i KillDisk i okvir napada VPNFilter. Ovi su alati hakerima omogućili daljinski pristup sustavima upravljanja elektroenergetskom mrežom i potom poremetili njezin rad. Incident je poslužio kao poziv na uzbunu vladama i organizacijama diljem svijeta, naglašavajući potrebu za povećanim oprezom, poboljšanim sigurnosnim mjerama i međunarodnom suradnjom u rješavanju kibernetičkih prijetnji. Ovaj slučaj pokazuje važnost ulaganja u kibernetičku sigurnost kako bi se zaštitila ne samo digitalna imovina, već i fizička dobrobit građana koji se oslanjaju na osnovne usluge [20].

Kibernetičku sigurnost neprestano ugrožavaju hakeri, gubitak podataka, privatnost, upravljanje rizicima i promjene strategija kibernetičke sigurnosti. Ne očekuje se da će se broj kibernetičkih napada smanjiti u bliskoj budućnosti. Štoviše, povećanje ulaznih točaka za napade, kao što je dolazak IoT-a (eng. *Internet of Things*), povećava potrebu za sigurnošću mreža i uređaja [11].

„Jedan od najproblematičnijih elemenata kibernetičke sigurnosti je razvojna priroda sigurnosnih rizika. Kako se pojavljuju nove tehnologije i kako se tehnologija koristi na nove ili drugačije načine, razvijaju se novi načini napada. Pratiti te česte promjene i napredak u napadima, kao i ažurirati zaštitu od njih, može biti izazov. Problemi uključuju osiguravanje stalnog ažuriranja svih elemenata kibernetičke sigurnosti radi zaštite od potencijalnih ranjivosti.To može biti posebno teško za manje organizacije bez osoblja ili vlastitih resursa.

Osim toga, organizacije mogu prikupiti mnogo potencijalnih podataka o pojedincima koji koriste jednu ili više njihovih usluga. Uz sve više podataka koji se prikupljaju, vjerojatnost da kibernetički kriminalac želi ukrasti podatke koji otkrivaju identitet te čak i posebne vrste osobnih podataka bez privole fizičke osobe (pojedinca) je još jedna briga. Na primjer, organizacija koja pohranjuje podatke koji otkrivaju identitet u oblaku može biti izložena napadu ransomwarea[23]*. Organizacije bi trebale učiniti sve što mogu kako bi spriječile proboj oblaka“* [24].

Programi kibernetičke sigurnosti bi se trebali baviti obrazovanjem krajnjih korisnika, budući da zaposlenici mogu slučajno unijeti viruse na radno mjesto na svojim prijenosnim računalima ili

[23] engl. *ransomware* – ucjenjivački softver, vrsta ucjenjivačkog softvera koja može zaključati računalo i za uzvrat tražiti

mobilnim uređajima. Redovita obuka o svijesti o sigurnosti pomoći će zaposlenicima da učine svoj dio u zaštiti svoje tvrtke od kibernetičkih prijetnji.

Još jedan izazov za kibernetičku sigurnost uključuje nedostatak kvalificiranog osoblja za kibernetičku sigurnost. Kako raste količina podataka koje tvrtke prikupljaju i koriste, raste i potreba za osobljem za kibernetičku sigurnost koje analizira, upravlja i reagira na incidente [14].

3.2 Uredbe i direktive u EU

EU već dulje vrijeme aktivno radi na jačanju kibernetičke sigurnosti i zaštiti komunikacije i podataka u više područja, uključujući politiku, energetiku, gospodarstvo, zdravstvo i financijski sektor. Ti su sektori sve više ovisni o digitalnim tehnologijama. Međutim, složeni zakonodavni sustavi koji se preklapaju u tim sektorima još uvijek bi se mogli pokazati neučinkovitima za rastuću zabrinutost moderne kibernetičke sigurnosti u budućnosti. To je, zajedno s krizom izazvanom COVID-19 i tekućim sukobom između Rusije i Ukrajine, potaknulo potrebu za još sveobuhvatnijim regulativnim okvirom kibernetičke sigurnosti [25].

U Europskoj uniji postoje uredbe i direktive koje se odnose na kibernetičku sigurnost te koje moraju poštivati članice Europske Unije. [26]:

- *The European Union Agency for Cybersecurity*[24] (ENISA), (EUR-Lex 2019/881)
- *The Directive on security of network and information systems*[25] (NIS)
- Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, OJL 333, koja je na snazi u EU[26]
- Zakon o kibernetičkoj sigurnosti Europske unije (eng. *Cybersecurity Act*)[27]
- European Union General Dana Protection[28] (EU GDPR)

[24]ENISA(EUR-Lex, 2019/881), [Izvor: https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX%3A32019R0881, Pristupljeno: 13.02.2023.]
[25] NIS(EUR- Lex, 2019/1148), [Izvor: https://eur-lex.europa.eu/legal-content/HR/LSU/?uri=CELEX:32016L1148, Pristupljeno: 13.02.2023.]
[26] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća, [Izvor: http://eurlex.europa.eu/legalcontent/HR/TXT/?uri=CELEX:32022L2555&qid=169141775514, Pristupljeno: 20. kolovoz 2023.)
[27]*European Union Cyber Security Act* (EUR- Lex, 2019/881), [Izvor: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881, Pristupljeno: 13.02.2023.]]
[28]EU GDPR(EUR-LEX, 2016/679), [Izvor: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, Pristupljeno: 13.02.2023.]

3.2.1 ENISA

Agencija Europske unije za kibernetičku sigurnost, ENISA, agencija je Unije posvećena postizanju visoke zajedničke razine kibernetičke sigurnosti diljem Europe. Osnovana 2004. godine i ojačana Zakonom o kibernetičkoj sigurnosti EU-a, Agencija Europske unije za kibernetičku sigurnost doprinosi kibernetičkoj politici EU-a, unapređuje pouzdanost ICT proizvoda, usluga i procesa pomoću shema certificiranja kibernetičke sigurnosti, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi za cyber izazove sutrašnjice. Dijeljenjem znanja, izgradnjom kapaciteta i podizanjem svijesti, Agencija radi zajedno sa svojim ključnim dionicima na jačanju povjerenja u povezano gospodarstvo, povećanju otpornosti infrastrukture Unije i, u konačnici, održavanju digitalne sigurnosti europskog društva i građana [27].

Vrijednosti koje ima ENISA su način razmišljanja zajednice. ENISA radi sa zajednicama, poštujući njihove kompetencije i stručnost, te potiče sinergije i povjerenje da najbolje postigne svoju misiju. Također, ENISA teži vrhunskoj stručnosti u svom radu, održava najviše standarde kvalitete poslovanja i ocjenjuje njihovu izvedbu i teži kontinuiranom poboljšanju kroz inovacije i predviđanje. Nadalje, ENISA podržava etička načela i relevantna pravila EU-a, te obveze u svojim uslugama i radnom okruženju. ENISA poštuje temeljna europska prava i vrijednosti, pokriva sve svoje usluge i radno okruženje, kao i očekivanja njegovih dionika. Preuzima odgovornost i time osigurava integraciju društvene i ekološke dimenzije prakse i procedure, te usvaja procedure, strukture i procese koji su otvoreni, činjenični i neovisni čime ograničavaju pristranost, dvosmislenost, prijevare i nejasnoće [28].

3.2.2 NIS

Direktiva NIS (EU 2016/1148) bila je prvi dio zakonodavstva o kibernetičkoj sigurnosti na razini cijele EU. Njezin je cilj poboljšati kibernetičku sigurnost diljem EU-a. Direktiva NIS usvojena je 2016. godine, a nakon toga, budući da se radi o direktivi EU, svaka država članica EU počela je usvajati nacionalno zakonodavstvo koje slijedi direktivu [29].

Široko je prihvaćena u zakonodavstvu država članica. Omogućuje određenu razinu fleksibilnosti u njezinom usvajanju u zakonodavnim tijelima država članica uzimajući u obzir nacionalne okolnosti. NIS direktive sastoje se od nacionalne sposobnosti, prekogranične suradnje i nacionalnog nadzora kritičnih sektora. Kod nacionalnih sposobnosti, države članice EU-a moraju imati određene nacionalne kibernetičke sigurnosne sposobnosti pojedinačnih zemalja EU-a, npr.

moraju imati nacionalni CSIRT, izvoditi kibernetičke vježbe itd. Prekograničnoj suradnja predstavlja suradnju između zemalja EU, npr. operativna EU CSIRT mreža[29], strateška NIS skupina za suradnju itd. U nacionalnom nadzoru kritičnih sektora države članice EU-a moraju nadzirati kibernetičku sigurnost kritičnih tržišnih operatera u svojoj zemlji, tj. nadzor u kritičnim sektorima (energija, transport, voda, zdravstvo, digitalna infrastruktura i sektor financija) te nadzor za pružatelje kritičnih digitalnih usluga (mrežna tržišta, oblak i online tražilice) [30].

NIS je zakonodavstvo o kibernetičkoj sigurnosti na razini cijele EU. Pruža pravne mjere za jačanje ukupne razine kibernetičke sigurnosti u EU-u. Pravila EU-a o kibernetičkoj sigurnosti uvedena 2016. ažurirana su Direktivom NIS2[30] koja je stupila na snagu 2023. Njome je moderniziran postojeći pravni okvir kako bi se držalo korak s povećanom digitalizacijom i razvojem kibernetičkih sigurnosnih prijetnji. Proširujući opseg pravila kibernetičkih sigurnosti na nove sektore i subjekte, dodatno se poboljšava otpornost i kapaciteti odgovora na incidente javnih i privatnih subjekata, nadležnih tijela i EU-a u cjelini [31].

3.2.3 Cybersecurity Act

Uveden u lipnju 2019., Zakon o kibernetičkoj sigurnosti jača ulogu ENISA-e dajući agenciji stalni mandat te više financijskih i ljudskih resursa. Zakon o kibernetičkoj sigurnosti objedinjuje kibernetičku sigurnost EU-a u jedinstveni okvir, s ENISA-om kao glavnom jezgrom. To znači da ENISA sada može doprinijeti operativnoj suradnji i upravljanju krizama diljem EU-a sa shemom certificiranja za cijelu EU koja će izgraditi povjerenje, povećati rast tržišta kibernetičke sigurnosti, olakšati trgovinu diljem EU-a [25].

ENISA ima mandat za povećanje operativne suradnje na razini EU-a, pomažući državama članicama EU-a koje to žele zatražiti u rješavanju njihovih kibernetičkih incidenata i podržavajući koordinaciju EU-a u slučaju velikih prekograničnih kibernetičkih napada i kriza. Ovaj zadatak temelji se na ulozi ENISA-e kao tajništva nacionalne mreže timova za odgovor na računalne sigurnosne incidente, uspostavljene Direktivom o sigurnosti mrežnih i informacijskih sustava.

[29] CSIRT - Mreža CSIRT pruža forum na kojem članovi mogu surađivati, razmjenjivati informacije i graditi povjerenje. Članovi će moći poboljšati postupanje s prekograničnim incidentima, pa čak i raspravljati o tome kako koordinirano odgovoriti na specifične incidente [Izvor: https://csirtsnetwork.eu/] Pristupljeno: Lipanj 2023.
[30] Direktiva NIS2; [Izvor: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, Pristupljeno: Lipanj 2023.]

Zakon o kibernetičkoj sigurnosti EU uvodi certifikacijski okvir kibernetičke sigurnosti[31] za ICT proizvode, usluge i procese na razini cijele EU. Tvrtke koje posluju u EU-u imat će koristi od toga što će svoje ICT proizvode, procese i usluge morati certificirati samo jednom i vidjeti svoje certifikate priznate u cijeloj Europskoj uniji. 18. travnja 2023. godine Komisija je predložila ciljanu izmjenu Zakona o kibernetičkoj sigurnosti EU-a. Predloženi amandman omogućit će buduće usvajanje europskih shema certificiranja za upravljane sigurnosne usluge koje pokrivaju područja kao što su odgovor na incidente, testiranje prodora, sigurnosne revizije i savjetovanje. Certifikacija je ključna za osiguranje visoke razine kvalitete i pouzdanosti ovih vrlo kritičnih i osjetljivih kibernetičkih sigurnosnih usluga koje pomažu tvrtkama i organizacijama da spriječe, otkriju, odgovore na incidente ili se oporave od njih [32].

3.2.4 EU GDPR

Opća uredba o zaštiti podataka, poznatija kao GDPR, najstroži je pravni akt o privatnosti i sigurnosti na svijetu. Iako ga je predložila Europska Komisija i donio EU parlament i Vijeće, nameće obveze organizacijama bilo gdje, sve dok ciljaju ili prikupljaju podatke koji se odnose na građane Europske Unije. Uredba je stupila na snagu 25. svibnja 2018. godine i nameće oštre novčane kazne protiv onih koji krše njezine standarde privatnosti i sigurnosti, a kazne sežu u desetke milijuna eura.

S GDPR-om, Europa signalizira svoj čvrsti stav o privatnosti i sigurnosti podataka u vrijeme kada sve više ljudi povjerava svoje osobne podatke uslugama u oblaku, a povrede su svakodnevna pojava. Sama uredba je opsežna, dalekosežna i prilično lagana u detaljima, što usklađivanje s GDPR-om čini zastrašujućom perspektivom, posebno za mala i srednja poduzeća [33].

GDPR postavlja sedam osnovnih načela na kojima temelji svoje propise i pravila usklađenosti u vezi s osobnim podacima, a to su zakonitost, poštenje i transparentnost, ograničenje namjene, minimizacija podataka, organizacije koje prikupljaju podatke, ograničenje pohrane, integritet i povjerljivost te sakupljanje podataka. Zakonitost, poštenje i transparentnost su načelo gdje ispitanik mora biti jasno obaviješten o tome kako će se njegovi podaci koristiti, ograničenje namjene jer se podaci mogu prikupljati samo za posebne svrhe. Također, minimizacija podataka iz

[31] Misija ENISA-e u području certifikacijskog okvira EU-a za kibernetičku sigurnost opisana je kao proaktivni doprinos nastajanju okvira EU-a za ICT certifikaciju proizvoda i usluga i provedba izrade shema certificiranja kandidata u skladu s Zakon o kibernetičkoj sigurnosti, te dodatne usluge i zadaće. [https://www.enisa.europa.eu/topics/certification]

razloga što je količina prikupljenih podataka ograničena na ono što je potrebno za konkretnu obradu. Organizacije koje prikupljaju podatke moraju osigurati njihovu točnost i po potrebi ih ažurirati. Podaci se moraju izbrisati ili promijeniti kada nositelj podataka podnese takav zahtjev. Načelo ograničenja pohrane prikupljeni podatke neće čuvati dulje nego što je potrebno. Integritet i povjerljivost znači da se na osobne podatke moraju primijeniti odgovarajuće mjere zaštite kako bi se osigurala njihova sigurnost i zaštita od krađe ili neovlaštene upotrebe. Sakupljači podataka odgovorni su za osiguranje usklađenosti s GDPR-om. [34]. Od 25. svibnja 2018. godine Uredba nije ažurirana te je istu potrebno dopuniti sukladno modernim tehnologijama poput interneta stvari, umjetne inteligencije itd. Ove godine navršila se peta godina primjene GDPR-au Hrvatskoj. Kršenje GDPR-a može dovesti tvrtke do ogromnih novčanih kazni. U Hrvatskoj, prvu novčanu kaznu , u iznosu od 146 tisuća eura, AZOP je izrekao jednoj od kreditnih institucija, tj. Banci, zbog povrede uredbe GDPR-a jer su odbijali dostaviti osobne podatke građanima, klijentima ili ispitanicima te banke. 2022. godine, kaznu od 285 tisuća eura dobila je jedna od vodećih telekomunikacijskih usluga u RH radi nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka [35].

4. RAČUNALSTVO U OBLAKU

Jednostavno rečeno, računalstvo u oblaku znači pružanje procesorske snage elektroničkim uređajima (osobnim računalima, tabletima, pametnim telefonima) putem udaljene infrastrukture. Računarstvo u oblaku nema međunarodno prihvaćenu definiciju, ali neke su institucije pokušale definirati ovaj fenomen. Na primjer, Nacionalni institut za standarde i tehnologiju Sjedinjenih Država (engl. *National Institute of Standards and Technology*, NIST) definirao je računalstvo u oblaku kao „model za omogućavanje sveprisutnog, odgovarajućeg, mrežnog pristupa na zahtjev za dijeljenje konfigurabilnih računalnih resursa (npr. mreže, poslužitelja, spremišta podataka, aplikacija i servisa/usluga) koji se mogu brzo omogućiti i dodijeliti uz minimalan napor i interakciju sa davateljem usluge". Sa druge strane, Europska komisija je rekla da se računalstvo u oblaku može shvatiti kao:„pohrana, obrada i uporaba podataka koji se nalaze na udaljenim računalima i kojima se pristupa putem Interneta", što predstavlja daljnju industrijalizaciju (standardizacija, povećanje, široko rasprostranjena dostupnost) pružanja računalne snage („komunalno računanje") na isti način na koji su elektrane industrijalizirale opskrbu električnom energijom" [36].

Nisu svi oblaci isti i nijedna vrsta računalstva u oblaku ne odgovara svima. Razvilo se nekoliko različitih modela, tipova i usluga kako bi se ponudilo pravo rješenje za potrebe korisnika. Prvo se mora odrediti vrsta implementacije oblaka ili arhitektura računalstva u oblaku na koju će se implementirati usluga oblaka [37].

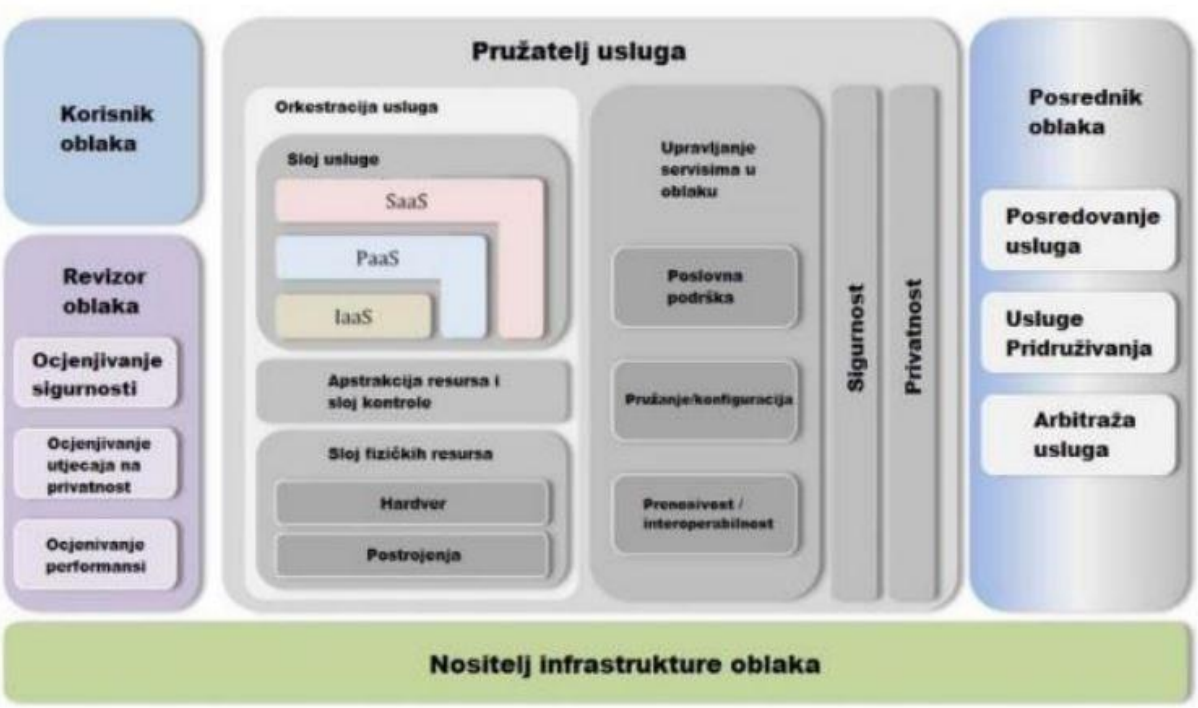
Postoje tri različita načina za implementaciju usluga u oblaku [37]:

- Javni oblak - njima upravljaju pružatelji usluga u oblaku trećih strana koji isporučuju svoje računalne resurse poput poslužitelja i pohrane te putem interneta. *Microsoft Azure* je primjer javnog oblaka. S javnim oblakom, sav hardver, softver i druga prateća infrastruktura u vlasništvu je i upravlja pružatelj usluga oblaka. Ovim uslugama korisnik pristupa i upravlja svojim računom pomoću *web* preglednika.
- Privatni oblak - odnosi se na računalne resurse u oblaku koje koristi isključivo jedna tvrtka ili organizacija. Privatni oblak može se fizički nalaziti u podatkovnom centru tvrtke na licu mjesta. Neke tvrtke također plaćaju pružateljima usluga trećih strana da ugoste njihov

privatni oblak. Privatni oblak je onaj u kojem se usluge i infrastruktura održavaju na privatnoj mreži.

- Hibridni oblak - kombiniraju javne i privatne oblake, povezane tehnologijom koja omogućuje dijeljenje podataka i aplikacija između njih. Dopuštajući podacima i aplikacijama da se kreću između privatnih i javnih oblaka, hibridni oblak korisnikovom poslovanju daje veću fleksibilnost, više mogućnosti implementacije i pomaže optimizirati postojeću infrastrukturu korisnika, sigurnost i usklađenost.

Referentna arhitektura računalstva u oblaku definira pet glavnih uloga, a to su korisnik oblaka, pružatelj usluga u oblaku, posrednik u oblaku, revizor oblaka te nositelj infrastrukture oblaka kao što je prikazano na slici 1. Također identificirane su njihove aktivnosti i funkcije [23].



Slika 3. Referentna arhitektura računalstva u oblaku
Izvor: [36]

Postoje tri glavna modela pružatelja usluga u oblaku [38]:

- Softver kao usluga (SaaS, eng. *Softver as a Service*)
- Infrastruktura kao usluga (IaaS, eng. *Infrastructure as a Service*)
- Platforma kao usluga (PaaS, eng. *Platform as a Service*)

Iako ih sve pokreće računalstvo u oblaku, svaki model radi drugačije i tvrtkama pruža vrlo različite usluge.

SaaS je najpoznatiji od tri modela isporuke usluga u oblaku. To je zato što većina ljudi koristi SaaS aplikacije svaki dan, bili oni toga svjesni ili ne. Kada ljudi govore o „oblaku", često govore o SaaS aplikacijama kao što su *Google Drive*, *Dropbox* ili čak *Netflix*.

SaaS model isporuke omogućuje korisnicima pristup potpuno funkcionalnom softveru kojim se upravlja i radi u oblaku. Korisnici obično pristupaju SaaS aplikacijama putem web preglednika. Prednost ovoga je što korisnik ne mora brinuti o preuzimanju i instaliranju programa jer se dobavljač brine za to. Prednost SaaS-a je što je lagan za korištenje, nema potrebe za ažuriranjem softvera i nema licenciranja softvera.

Kako je tehnologija rasla, tvrtke su se okrenule pružateljima usluga u oblaku za pomoć u upravljanju svojom IT infrastrukturom. Tako je rođen IaaS i tvrtke su počele prelaziti s lokalne na infrastrukturu u oblaku. IaaS omogućuje tvrtkama pristup virtualiziranim računalnim resursima s poslužitelja u oblaku. Prednosti IaaS-a je veća fleksibilnost, pouzdanost i ušteda troškova.

PaaS organizacijama omogućuje stvaranje, pokretanje i upravljanje softverom temeljenim na oblaku bez potrebe za infrastrukturom na licu mjesta. Platforme osigurava i održava dobavljač treće strane. To znači da tvrtke ne moraju brinuti o aktivnostima kao što su sigurnosne kopije i pružanje poslužitelja, odnosno sve se radi za njih. Prednosti PaaS-a su poboljšana učinkovitost, jednostavnost i bolja suradnja.

Neke od platformi za pružanje usluga računalstva u oblaku su *Microsoft Azure*, *Amazon Web Services*, *Google Cloud*, *IBM Cloud*, *Oracle Cloud Infrastructure* te *Cloud Linux* [38].

4.1 Prednosti i nedostaci

Računalstvo u oblaku ima niz značajnih prednosti:

• Sklopovska podrška (računala, uređaji za pohranu) u vlasništvu je pružatelja usluga računalstva u oblaku, a ne korisnika koji s njim komunicira putem interneta;

• Upotreba sklopovske podrške dinamički je optimizirana u čitavoj mreži računala, tako da točna lokacija podataka ili procesa, kao i informacije, koji dio sklopovske podrške zapravo opslužuje određenog korisnika u danom trenutku, u načelu ne moraju zabrinuti korisnika, iako to može imati značajan utjecaj na primjenjivo pravno okruženje;

• Davatelji usluga oblaka često premještaju radna opterećenja svojih korisnika (npr. sa jednog računala na drugo ili iz jednog podatkovnog centra u drugo) kako bi optimizirali korištenje dostupne sklopovske podrške;

• Udaljena sklopovska podrška pohranjuje i obrađuje podatke te ih čini dostupnima, npr. putem aplikacija (kako bi tvrtka mogla koristiti svoje računalstvo zasnovano na oblaku na isti način na koji potrošači već danas koriste svoje račune web pošte);

• Organizacije i pojedinci mogu pristupiti njihovom sadržaju, te koristiti njihovu programsku podršku kad i gdje im zatrebaju, npr. na stolnim računalima, prijenosnim računalima, tabletima i pametnim telefonima;

• Postavljanje oblaka sastoji se od slojeva: sklopovske podrške, međuopreme ili platforme i aplikacijske programske podrške. Standardizacija je važna osobito na srednjem sloju jer omogućuje programerima da se obrate širokom rasponu potencijalnih kupaca i daje korisnicima izbor;

• Korisnici obično plaćaju korištenjem, izbjegavajući velike unaprijed i fiksne troškove potrebne za postavljanje i rad sa sofisticiranom računalnom opremom;

• U isto vrijeme, korisnici mogu vrlo lako promijeniti količinu sklopovske podrške koju koriste (npr. s nekoliko klikova mišem donijeti novi kapacitet pohrane na mreži u nekoliko sekundi).

Osim čiste uštede, računarstvo u oblaku može pomoći u prelasku na javne usluge 21. stoljeća koje su interoperabilne, prilagodljive i u skladu s potrebama mobilnog stanovništva i tvrtki koje žele imati koristi od jedinstvenog europskog digitalnog tržišta. Prvi inkrementalni koraci bili bi poboljšana izvedba usluga, poput poboljšane sigurnosti, usluga prilagođenijih

korisnicima, mogućnost uvođenja novih usluga jeftino, brzo i fleksibilno, relativna jednostavnost korištenja računalstva u oblaku za stvaranje platformi za društveni angažman ili za određene kampanje i mogućnost boljeg praćenja ishoda. Računarstvo u oblaku moglo bi pomoći u smanjenju javnih troškova i povećanju javnih koristi te dati širu osnovu za gospodarske aktivnosti koje uključuju cijelo stanovništvo [36].

Svaki novčić ima dva lica. To naravno ne znači da računalstvo u oblaku nema nedostataka. Neki od nedostataka tijekom korištenja oblaka mogu se sažeti kao [36]:

• Potrebna je brza mreža i stalno povezivanje;

• Privatnost i sigurnost potencijalno nisu dobri ukoliko pružatelj usluga nije odgovarajuće zaštitio prijenos podataka. Podatci i aplikacija u javnom oblaku možda nisu jako sigurni;

• Katastrofalne situacije su neizbježne i oporavak nije uvijek moguć. Ako oblak izgubi nečije podatke, korisnik i davatelj usluga nailaze na ozbiljne probleme;

• Korisnici imaju vanjsku ovisnost o kritičnim aplikacijama;

• Zahtijeva stalno praćenje i provedbu ugovora o razini usluge.

4.2 Prijetnje računalstva u oblaku

Velika količina podataka koja teče između organizacija i pružatelja usluga u oblaku stvara prilike za slučajno i zlonamjerno curenje osjetljivih podataka nepouzdanim trećim stranama. Ljudska pogreška, prijetnje iznutra, zlonamjerni softver, slabe vjerodajnice i kriminalne aktivnosti pridonose većini povreda podataka usluge oblaka. Zlonamjerni akteri, uključujući hakere koje sponzorira država, nastoje iskoristiti sigurnosne propuste usluge oblaka kako bi izvukli podatke iz mreže organizacije žrtve za profit ili druge nedopuštene svrhe. Općenito, značajke koje usluge u oblaku čine lako dostupnima zaposlenicima i IT sustavima također otežavaju organizacijama sprječavanje neovlaštenog pristupa. Međutim, sigurnosni izazovi koje uvode usluge u oblaku nisu usporili usvajanje računalstva u oblaku i pad lokalnih podatkovnih centara. Kao rezultat toga, organizacije svih veličina moraju ponovno razmisliti o svojim mrežnim sigurnosnim protokolima kako bi ublažile rizik od neovlaštenog prijenosa podataka, prekida usluge i štete po ugled. Usluge u oblaku izlažu organizacije novim sigurnosnim prijetnjama povezanim s autentifikacijom i javnim API-jima. Sofisticirani hakeri koriste svoju stručnost za ciljanje sustava u oblaku i dobivanje

pristupa. Hakeri koriste društveni inženjering, preuzimanje računa, taktike izbjegavanja otkrivanja i slično, kako bi održali dugoročnu prisutnost na mreži organizacije žrtve, često koristeći ugrađene alate iz usluga u oblaku. Njihov cilj je prijenos osjetljivih informacija u sustave pod njihovom kontrolom [39].

Gotovo svaka organizacija usvojila je računalstvo u oblaku u različitim stupnjevima unutar svog poslovanja. Međutim, s ovim usvajanjem oblaka dolazi potreba da se osigura da je sigurnosna strategija oblaka organizacije sposobna zaštititi od najvećih prijetnji sigurnosti oblaka [40].

Pogrešne konfiguracije sigurnosnih postavki u oblaku vodeći su uzrok povrede podataka u oblaku. Strategije upravljanja sigurnosnim položajem u oblaku mnogih organizacija neadekvatne su za zaštitu njihove infrastrukture temeljene na oblaku. Tome pridonosi nekoliko čimbenika. Infrastruktura oblaka dizajnirana je da bude lako upotrebljiva i da omogući jednostavno dijeljenje podataka, što otežava organizacijama da osiguraju da podaci budu dostupni samo ovlaštenim stranama. Također, organizacije koje koriste infrastrukturu temeljenu na oblaku također nemaju potpunu vidljivost i kontrolu nad svojom infrastrukturom, što znači da se moraju osloniti na sigurnosne kontrole koje pruža njihov pružatelj usluga u oblaku kako bi konfigurirali i osigurali svoje implementacije u oblaku. Budući da mnoge organizacije nisu upoznate s osiguravanjem infrastrukture u oblaku i često imaju implementacije u više oblaka, svaki s drugačijim nizom sigurnosnih kontrola koje pruža dobavljač, lako je zbog pogrešne konfiguracije ili sigurnosnog nadzora resurse organizacije temeljene na oblaku ostaviti izloženima napadačima.

Za razliku od lokalne infrastrukture organizacije, njihove implementacije temeljene na oblaku izvan su mrežnog perimetra i izravno su dostupne s javnog interneta. Iako je ovo prednost za dostupnost ove infrastrukture zaposlenicima i klijentima, također olakšava napadaču neovlašteni pristup resursima organizacije u oblaku. Neispravno konfigurirana sigurnost ili ugrožene vjerodajnice mogu omogućiti napadaču izravan pristup, potencijalno bez znanja organizacije [40].

U nastavku su opisane neke od glavnih kibernetičkih prijetnji računalstva u oblaku.

Kibernetički kriminal je posao, a kibernetički kriminalci odabiru svoje mete na temelju očekivane isplativosti svojih napada. Infrastruktura temeljena na oblaku izravno je dostupna s javnog interneta, često je nepropisno osigurana i sadrži mnogo osjetljivih i vrijednih podataka. Osim toga, oblak koriste mnoge različite tvrtke, što znači da se uspješan napad vjerojatno može

ponoviti mnogo puta s velikom vjerojatnošću uspjeha. Kao rezultat toga, organizacije u oblaku su česta meta kibernetičkih napada [40].

Insajderske prijetnje glavni su sigurnosni problem za svaku organizaciju. Zlonamjerni insajder već ima ovlašteni pristup mreži organizacije i nekim od osjetljivih resursa koje ona sadrži. Pokušaji da se dobije ova razina pristupa su ono što otkriva većinu napadača njihovoj meti, što otežava nepripremljenoj organizaciji otkrivanje zlonamjernog insajdera. U oblaku je otkrivanje zlonamjernog insajdera još teže. S implementacijama u oblaku, tvrtkama nedostaje kontrola nad njihovom temeljnom infrastrukturom, što mnoga tradicionalna sigurnosna rješenja čini manje učinkovitima. To, zajedno s činjenicom da je infrastruktura temeljena na oblaku izravno dostupna s javnog interneta i često pati od sigurnosnih pogrešnih konfiguracija, dodatno otežava otkrivanje zlonamjernih insajdera [40].

Jedna od prijetnji računalstvu u oblaku su nesigurna sučelja. CSP-ovi (eng. *Content Security Policy*[32]) često pružaju niz sučelja za programiranje aplikacija i sučelja za svoje klijente. Općenito, ta su sučelja dobro dokumentirana u pokušaju da budu lako upotrebljiva za klijente CSP-a. Međutim, to stvara potencijalne probleme ako korisnik nije ispravno osigurao sučelja za svoju infrastrukturu temeljenu na oblaku. Dokumentaciju dizajniranu za kupca također može koristiti kibernetički kriminalac za prepoznavanje i iskorištavanje potencijalnih metoda za pristup osjetljivim podacima i njihovo izvlačenje iz okruženja oblaka organizacije [40].

Nadalje, mnogi ljudi imaju izuzetno slabu sigurnost lozinki, uključujući ponovnu upotrebu lozinki i korištenje slabih lozinki. Ovaj problem pogoršava utjecaj phishing napada i povrede podataka budući da omogućuje korištenje jedne ukradene lozinke na više različitih računa. Otmica računa jedno je od ozbiljnijih sigurnosnih problema u oblaku jer se organizacije sve više oslanjaju na infrastrukturu i aplikacije temeljene na oblaku za osnovne poslovne funkcije. Napadač s vjerodajnicama zaposlenika može pristupiti osjetljivim podacima ili funkcijama, a kompromitirane vjerodajnice korisnika daju potpunu kontrolu nad njihovim online računom. Osim toga, u oblaku organizacijama često nedostaje sposobnost identificiranja i odgovora na te prijetnje jednako učinkovito kao i za lokalnu infrastrukturu [40].

[32] Politika sigurnosti sadržaja (CSP) dodatni je sloj sigurnosti koji pomaže u otkrivanju i ublažavanju određenih vrsta napada, uključujući *Cross-Site Scripting* (XSS) i napade ubacivanjem podataka. Ovi se napadi koriste za sve, od krađe podataka, do narušavanja web mjesta i distribucije zlonamjernog softvera [41].

Isto tako, resursi organizacije temeljeni na oblaku nalaze se izvan korporativne mreže i rade na infrastrukturi koju tvrtka ne posjeduje. Kao rezultat toga, mnogi tradicionalni alati za postizanje mrežne vidljivosti nisu učinkoviti za okruženja oblaka, a nekim organizacijama nedostaju sigurnosni alati usmjereni na oblak. To može ograničiti sposobnost organizacije da nadzire svoje resurse temeljene na oblaku i zaštiti ih od napada [40].

Cloud je dizajniran da olakša dijeljenje podataka. Mnogi oblaci pružaju opciju da izričito pozovete suradnika putem e-pošte ili da podijelite vezu koja svakome s URL-om omogućuje pristup dijeljenom resursu. Iako je ovo jednostavno dijeljenje podataka prednost, ono može biti i veliki sigurnosni problem u oblaku. Korištenje dijeljenja temeljenog na poveznici, popularna opcija jer je jednostavnija od izričitog pozivanja svakog namjeravanog suradnika, otežava kontrolu pristupa dijeljenom resursu. Dijeljena poveznica može biti proslijeđena nekom drugom, ukradena kao dio kibernetičkog napada ili pogođena od strane kibernetičkog kriminalca, omogućavajući neovlašteni pristup dijeljenom resursu. Osim toga, dijeljenje na temelju veze onemogućuje opoziv pristupa samo jednom primatelju dijeljene veze [40]

Također, napadi uskraćivanjem usluge su jedni od prijetnji računalstva u oblaku. Oblak je ključan za sposobnost poslovanja mnogih organizacija. One koriste oblak za pohranjivanje podataka kritičnih za poslovanje i pokretanje važnih internih aplikacija i aplikacija usmjerenih na korisnike. To znači da će uspješan napad uskraćivanja usluge na infrastrukturu oblaka vjerojatno imati veliki utjecaj na brojne različite tvrtke. Kao rezultat toga, DoS napadi u kojima napadač zahtijeva otkupninu za zaustavljanje napada predstavljaju značajnu prijetnju resursima organizacije u oblaku [40].

4.3 Sigurnost i zaštita računalstva u oblaku

Sigurnosne prijetnje postale su naprednije kako se digitalno okruženje nastavlja razvijati. Ove prijetnje izričito ciljaju na pružatelje usluga računalstva u oblaku zbog sveukupnog nedostatka vidljivosti organizacije u pristupu i kretanju podataka. Bez poduzimanja aktivnih koraka za poboljšanje sigurnosti u oblaku, organizacije se mogu suočiti sa značajnim rizicima upravljanja i usklađenosti pri upravljanju informacijama o klijentima, bez obzira na to gdje su pohranjene. Sigurnost u oblaku trebala bi biti važna tema za raspravu bez obzira na veličinu poduzeća. Infrastruktura oblaka podržava gotovo sve aspekte modernog računarstva u svim industrijama. Međutim, uspješno prihvaćanje oblaka ovisi o postavljanju odgovarajućih protumjera za obranu

od modernih kibernetičkih napada. Bez obzira na to djeluje li organizacija u javnom, privatnom ili hibridnom okruženju oblaka, sigurnosna rješenja u oblaku su nužna kada se osigurava kontinuitet poslovanja [42].

Sigurnost u oblaku je disciplina kibernetičke sigurnosti posvećena osiguravanju računalnih sustava u oblaku. To uključuje privatnost i sigurnost podataka u infrastrukturi, aplikacijama i platformama temeljenim na mreži. Osiguranje ovih sustava uključuje napore pružatelja usluga oblaka i klijenata koji ih koriste, bilo da ih koriste pojedinci, mala, srednja ili velika poduzeća. Pružatelji usluga u oblaku drže usluge na svojim poslužiteljima putem stalno uključenih internetskih veza. Budući da se njihovo poslovanje oslanja na povjerenje kupaca, koriste se sigurnosne metode u oblaku kako bi podaci klijenata bili privatni i sigurno pohranjeni. Međutim, sigurnost u oblaku dijelom također leži u rukama klijenta. Razumijevanje oba aspekta ključno je za zdravo sigurnosno rješenje u oblaku [43].

Sigurnost u oblaku cijeli je skup tehnologije, protokola i najboljih praksi koji štite okruženja računalstva u oblaku, aplikacije koje se izvode u oblaku i podatke koji se nalaze u oblaku. Osiguranje usluga u oblaku počinje razumijevanjem što se točno osigurava, kao i aspekata sustava kojima se mora upravljati. Potpuni opseg sigurnosti u oblaku osmišljen je za zaštitu [43]:

- Fizičke mreže — usmjerivači, električna energija, kablovi, kontrole klime itd.
- Pohrane podataka — tvrdi diskovi, itd.
- Podatkovnih poslužitelja — računalni hardver i softver jezgrene mreže
- Okvira računalne virtualizacije — softver virtualnog stroja, host strojevi i gostujući strojevi
- Operativnih sustava — softver koji sadrži
- *Middleware* — upravljanje aplikacijskim programskim sučeljem (API),
- Izvršnih okruženja — izvođenje i održavanje pokrenutog programa
- Podataka — sve informacije koje se pohranjuju, mijenjaju i kojima se pristupa
- Aplikacije — tradicionalne softverske usluge (e-pošta, porezni softver, paketi za produktivnost itd.)
- Hardvera krajnjeg korisnika — računala, mobilni uređaji, uređaji Interneta stvari itd.

Vrste sigurnosnih rješenja u oblaku su [42]:

- Upravljanje identitetom i pristupom-Alati i usluge za upravljanje identitetom i pristupom (IAM) omogućuju tvrtkama da implementiraju protokole za provedbu na temelju pravila za sve korisnike koji pokušavaju pristupiti i lokalnim uslugama i uslugama temeljenim na oblaku. Temeljna funkcija IAM-a je stvaranje digitalnih identiteta za sve korisnike kako bi se mogli aktivno nadzirati i ograničavati kada je to potrebno tijekom svih interakcija podataka
- Sprječavanje gubitka podataka - usluge sprječavanja gubitka podataka (DLP) nude skup alata i usluga dizajniranih za osiguranje sigurnosti reguliranih podataka u oblaku. DLP rješenja koriste kombinaciju upozorenja o popravci, enkripcije podataka i drugih preventivnih mjera za zaštitu svih pohranjenih podataka, bilo da miruju ili se kreću.
- Sigurnosne informacije i upravljanje događajima- Upravljanje sigurnosnim informacijama i događajima pruža sveobuhvatno rješenje za sigurnosnu orkestraciju koje automatizira nadzor prijetnji, otkrivanje i odgovor u okruženjima temeljenim na oblaku. Korištenjem tehnologija koje se pokreću umjetnom inteligencijom za korelaciju podataka dnevnika na više platformi i digitalnih sredstava, SIEM[33] (eng. *Security information and event management*) tehnologija daje IT timovima mogućnost da uspješno primjenjuju svoje mrežne sigurnosne protokole, a istovremeno mogu brzo reagirati na sve potencijalne prijetnje.
- Kontinuitet poslovanja i oporavak od katastrofe- bez obzira na preventivne mjere koje su organizacije poduzele za svoje lokalne infrastrukture i infrastrukture temeljene na oblaku, i dalje može doći do upada podataka i prekida rada. Poduzeća moraju biti sposobna brzo reagirati na novootkrivene ranjivosti ili značajne ispade sustava što je prije moguće. Rješenja za oporavak od katastrofe glavna su komponenta sigurnosti u oblaku i organizacijama pružaju alate, usluge i protokole potrebne za ubrzavanje oporavka izgubljenih podataka i nastavak normalnog poslovanja.

Nacionalni institut za standarde i tehnologiju (NIST) napravio je popis najboljih praksi koje se mogu slijediti kako bi se uspostavio siguran i održiv okvir računalstva u oblaku. NIST je

[33] Upravljanje sigurnosnim informacijama i događajima ili SIEM je sigurnosno rješenje koje pomaže organizacijama da prepoznaju i riješe potencijalne sigurnosne prijetnje i ranjivosti prije nego što imaju priliku poremetiti poslovne operacije. SIEM sustavi pomažu sigurnosnim timovima poduzeća da otkriju anomalije u ponašanju korisnika i koriste umjetnu inteligenciju za automatizaciju mnogih ručnih procesa povezanih s otkrivanjem prijetnji i odgovorom na incidente.

stvorio potrebne korake za svaku organizaciju da sama procijeni svoju sigurnosnu spremnost i primijeni odgovarajuće preventivne i sigurnosne mjere za oporavak na svojim sustavima. Ova su načela izgrađena na NIST-ovih pet stupova kibernetičke sigurnosti: Identificiraj, Zaštiti, Otkrij, Odgovori i Oporavi. Još jedna nova tehnologija u sigurnosti oblaka koja podržava izvođenje NIST-ovog okvira kibernetičke sigurnosti je upravljanje sigurnosnim položajem oblaka. CSPM (eng. *Cloud security posture management*) rješenja dizajnirana su za rješavanje uobičajene greške u mnogim okruženjima oblaka - pogrešne konfiguracije. Infrastrukture oblaka koje poduzeća ili čak pružatelji usluga oblaka ostaju pogrešno konfigurirane mogu dovesti do nekoliko ranjivosti koje značajno povećavaju površinu napada organizacije. CSPM rješava ove probleme pomažući organizirati i implementirati ključne komponente sigurnosti u oblaku. To uključuje upravljanje identitetom i pristupom, upravljanje usklađenošću s propisima, praćenje prometa, odgovor na prijetnje, ublažavanje rizika i upravljanje digitalnom imovinom [42].

Enkripcija je jedan od najboljih načina za zaštitu vaših računalnih sustava u oblaku. Postoji nekoliko različitih načina korištenja enkripcije, a može ih ponuditi pružatelj usluga oblaka ili zasebni pružatelj sigurnosnih rješenja u oblaku. To su enkripcija komunikacije s oblakom u cijelosti, posebno osjetljiva enkripcija podataka, kao što su vjerodajnice računa i end-to-end enkripcija svih podataka koji se učitavaju u oblak [42].

Postoje brojni algoritmi za šifriranje podataka koji se mogu izabrati, ovisno o slučaju uporabe, no oni koji se najčešće koriste su [44]:

- 3DES ili TDES (eng. the Triple Data Encryption Algorithm)—pokreće DES algoritam, zastarjeli standard, tri puta, šifriranje, dešifriranje i ponovno šifriranje kako bi se stvorio duži ključ. Može se pokrenuti s jednim ključem, dva ključa ili tri različita ključa uz povećanu sigurnost. 3DES koristi metodu blok šifriranja, što ga čini ranjivim na napade kao što je sudar blokova.
- RSA (eng. Rivest-Shamir-Adleman) —jedan od prvih algoritama s javnim ključem, koristi jednosmjernu asimetričnu enkripciju. RSA je popularan zbog svoje duge duljine ključa i naširoko se koristi na Internetu. Dio je mnogih sigurnosnih protokola, poput SSH, OpenPGP, S/MIME i SSL/TLS, a preglednici ga koriste za stvaranje sigurnih veza preko nesigurnih mreža.

- *Twofish*—jedan od najbržih algoritama, dostupan je u veličinama od 128, 196 i 256 bita sa složenom strukturom ključa za povećanu sigurnost. Besplatan je za korištenje i pojavljuje se u nekim od najboljih besplatnih softvera: VeraCrypt, PeaZip i KeePass te standardu OpenPGP..

Unutar oblaka, podaci su u većoj opasnosti od presretanja kada su u pokretu. Ranjiv je kada se premješta s jedne lokacije za pohranu na drugu ili se prenosi korisnikovoj aplikaciji na licu mjesta. Stoga je end-to-end enkripcija najbolje sigurnosno rješenje u oblaku za kritične podatke. S end-to-end enkripcijom ni u jednom trenutku komunikacija nije dostupna vanjskim osobama bez vašeg ključa za šifriranje. Međutim, ako koristi oblak samo za pohranjivanje neosjetljivih podataka kao što su korporativne grafike ili videozapisi, end-to-end enkripcija bi mogla biti pretjerana. S druge strane, za financijske, povjerljive ili komercijalno osjetljive informacije to je od vitalnog značaja.

Konfiguracija je također dobra u sigurnosti oblaka. Mnoge povrede podataka u oblaku dolaze iz osnovnih ranjivosti kao što su pogreške u pogrešnoj konfiguraciji. Njihovim sprječavanjem se uvelike smanjuje sigurnosni rizik u oblaku.

Osnovni savjeti o kibernetičkoj sigurnosti također bi trebali biti ugrađeni u svaku implementaciju oblaka. Ne smije se zanemariti standardne prakse kibernetičke sigurnosti. Osnovni savjeti tiču se korištenja jake lozinke, zaštite uređaja koji se koriste za pristup podacima u oblaku, redovite sigurnosne kopije podataka u slučaju, prekida rada u oblaku ili gubitka podataka, zaštite antivirusima, izbjegavanje pristupa podacima na javnoj mreži itd.

Doneseni su zakoni, odnosno pravni akti koji pomažu u zaštiti krajnjih korisnika od prodaje i dijeljenja njihovih osjetljivih podataka. Opća uredba o zaštiti podataka (GDPR) i Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja[34] (HIPAA) obavljaju svaki svoju dužnost zaštite privatnosti, ograničavajući način na koji se podaci mogu pohraniti i kako im se može pristupiti.

Metode upravljanja identitetom poput maskiranja podataka korištene su za odvajanje prepoznatljivih značajki od korisničkih podataka radi usklađenosti s GDPR-om. Za usklađenost sa

[34] HIPAA [Izvor: https://www.cdc.gov/phlp/publications/topic/hipaa.html, Pristupljeno: 20. kolovoza 2023.]

HIPAA, organizacije poput zdravstvenih ustanova moraju se pobrinuti da njihov pružatelj također izvrši svoj dio u ograničavanju pristupa podacima.

Zakon o cloud-u pružateljima usluga oblaka daje vlastita pravna ograničenja kojih se moraju pridržavati, potencijalno po cijenu privatnosti korisnika. Savezni zakon SAD-a sada dopušta tijelima za provedbu zakona na saveznoj razini da traže tražene podatke od poslužitelja pružatelja usluga oblaka. Iako to može omogućiti učinkoviti nastavak istrage, to može zaobići neka prava na privatnost i uzrokovati potencijalnu zlouporabu ovlasti [43].

5 SIGURNOST OSOBNIH PODATAKA

Sigurnost podataka ključna je za organizacije javnog i privatnog sektora iz raznih razloga. Postoji zakonska i moralna obveza tvrtki da zaštite svoje korisnike i korisničke podatke od pada u pogrešne ruke. Na primjer, financijske tvrtke mogu podlijegati standardu sigurnosti podataka industrije platnih kartica koji prisiljava tvrtke da poduzmu sve razumne mjere za zaštitu podataka o klijentima [45].

Slika 4. Sigurnost osobnih podataka[35]

Postoji i reputacijski rizik od povrede podataka ili hakiranja. Ako se sigurnost podataka ne shvaća ozbiljno, ugled može biti trajno oštećen u slučaju provale ili hakiranja visokog profila. Također, financijske i logističke posljedice povrede podataka mogu biti ogromne. Trebat će potrošiti vrijeme i novac kako bi se procijenila i popravila šteta, kao i utvrdilo koji poslovni procesi nisu uspjeli, a koje je potrebno poboljšati.

Tri su ključna elementa sigurnosti podataka kojih bi se sve organizacije trebale pridržavati, a to su povjerljivost, integritet i dostupnost. Povjerljivost osigurava da podacima pristupaju samo ovlašteni korisnici s odgovarajućim vjerodajnicama. Integritet osigurava da su svi pohranjeni

[35] Izvor: PC Kings. Personal dana safety are You social media savvy?. Preuzeto sa: https://pckings.uk/personal-data-safety/ [Pristupljeno: lipanj 2023]

podaci pouzdani, točni i da ne podliježu neopravdanim promjenama. Dostupnost osigurava da su podaci lako i sigurno dostupni za poslovne potrebe.

Korištenje pravih tehnologija za sigurnost podataka može pomoći organizaciji spriječiti provale, smanjiti rizik i održati zaštitne sigurnosne mjere. Narušavanje sigurnosti često je neizbježno, pa se mora uspostaviti postupak koji otkriva glavni uzrok. Softverska rješenja za reviziju podataka bilježe i izvješćuju o stvarima kao što su kontrolne promjene podataka, zapisi o tome tko je pristupio osjetljivim informacijama i korišteni put datoteke. Svi ovi revizijski postupci ključni su za proces istrage kršenja. Odgovarajuća rješenja za reviziju podataka IT administratorima također pružaju vidljivost u sprječavanju neovlaštenih promjena i mogućih povreda.

Obično je tvrtkama potrebno nekoliko mjeseci prije nego što otkriju da je došlo do povrede podataka. Prečesto tvrtke otkrivaju kršenja preko svojih kupaca ili dobavljača i izvođača trećih strana, a ne vlastitih IT odjela. Korištenjem sustava u stvarnom vremenu i tehnologije nadzora podataka moći će brže otkriti kršenja. To pomaže ublažiti uništavanje podataka, gubitak, promjenu ili neovlašteni pristup osobnim podacima. Procjena rizika podataka pomoći će organizaciji identificirati svoje najizloženije, osjetljive podatke. Potpuna procjena rizika također će ponuditi pouzdane i ponovljive korake prema određivanju prioriteta i sanaciji ozbiljnih sigurnosnih rizika. Proces počinje identificiranjem osjetljivih podataka kojima se pristupa putem globalnih grupa, podataka koji su zastarjeli ili podataka s nedosljednim dopuštenjima. Točna procjena rizika sažet će važne podatke, razotkriti ranjivosti i uključiti prioritetne preporuke za sanaciju.

Tradicionalno, organizacije su gledale na što više podataka kao na korist. Uvijek je postojala mogućnost da bi to moglo dobro doći u budućnosti. Danas se velike količine podataka sa sigurnosnog stajališta smatraju problemom. Što više podataka ima, veći je broj meta za hakere. Zato je smanjivanje podataka sada ključna sigurnosna taktika. Ako podaci ne postoje unutar mreže, ne mogu biti ugroženi. Zato treba obrisati stare ili nepotrebne podatke i koristiti sustave koji mogu pratiti pristup datotekama i automatski arhivirati neiskorištene datoteke. U modernom dobu godišnjih akvizicija i reorganizacija, vrlo je vjerojatno da mreže bilo koje značajne veličine imaju više zaboravljenih poslužitelja koji se drže bez valjanog razloga [45].

5.1 Vrste sigurnosti osobnih podataka

Vrste sigurnosti podataka su [45]:

- Kontrole pristupa - vrsta mjera sigurnosti podataka koja uključuje ograničavanje fizičkog i digitalnog pristupa kritičnim sustavima i podacima. To uključuje osiguranje da su sva računala i uređaji zaštićeni obaveznim unosom prijave te da u fizičke prostore može ući samo ovlašteno osoblje
- Ovjera - autentifikacija se posebno odnosi na točnu identifikaciju korisnika prije nego što ima pristup podacima. To obično uključuje stvari poput lozinki, PIN brojeva, sigurnosnih tokena, proklizavajućih kartica ili biometrije.
- Sigurnosne kopije i oporavak - dobra sigurnost podataka znači da korisnik ima plan za siguran pristup podacima u slučaju kvara sustava, katastrofe, oštećenja podataka ili povrede. Korisniku će trebati sigurnosna kopija podataka pohranjena na zasebnom formatu kao što je fizički disk, lokalna mreža ili oblak za oporavak ako je potrebno.
- Brisanje podataka - brisanje podataka koristi softver za potpuno brisanje podataka na bilo kojem uređaju za pohranu i sigurnije je od standardnog brisanja podataka. Brisanje podataka potvrđuje da se podaci ne mogu oporaviti i stoga neće pasti u pogrešne ruke.
- Maskiranje podataka - korištenjem softvera za maskiranje podataka, informacije se skrivaju zaklanjanjem slova i brojeva proxy znakovima. To učinkovito maskira ključne informacije čak i ako im neovlaštena strana pristupi. Podaci se vraćaju u izvorni oblik tek kada ih primi ovlašteni korisnik.
- Otpornost podataka - sveobuhvatna sigurnost podataka znači da sustavi mogu izdržati ili se oporaviti od kvarova. Ugradnja otpornosti u hardver i softver znači da događaji poput nestanka struje ili prirodnih katastrofa neće ugroziti sigurnost.
- Šifriranje - računalni algoritam pretvara tekstualne znakove u nečitljiv format putem ključeva za šifriranje. Samo ovlašteni korisnici s ispravnim odgovarajućim ključevima mogu otključati i pristupiti informacijama. Sve, od datoteka i baze podataka do komunikacije e-poštom treba biti šifrirano do neke mjere.

5.2 Zakoni o sigurnosti u RH i sukladnost s GDPR-om

Jedno od temeljnih prava svakog čovjeka je pravo na zaštitu osobnih podataka. Zaštita osobnih podataka je zaštita privatnog života, ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Pravo zaštite legitimnih interesa pojedinca koje se odnosi na sprječavanje i rješavanje zlouporaba osobnih podataka je pravo na zaštitu osobnih podataka, a

garantirano je međunarodnim i nacionalnim propisima. U Republici Hrvatskoj, zaštita osobnih podataka je ustavna kategorija u kojem je svakom građaninu zajamčena zaštita ljudskih prava i temeljnih sloboda neovisno o državljanstvu, prebivalištu, rasi, spolu, jeziku, političkom uvjerenju, podrijetlu, imovini, rođenju, položaju u društvu i drugim osobinama.

GDPR-om, odnosno, Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/18 koja se izravno primjenjuje u Republici Hrvatskoj i svim članicama Europske unije od 2018. godine, moderniziran je regulatorni okvir kako bi u današnje digitalno doba išao u korak s rapidnim razvojem tehnologije i bio učinkovit, a ujedno i osnažio povjerenje pojedinca u elektroničke usluge i jedinstveno digitalno tržište. Tim Zakonom GDPR-a, koji je stupio na snagu 25. svibnja 2018. godine, osigurava se provedba Opće uredbe o zaštiti podataka[36] [46].

Početkom primjene Opće uredbe o zaštiti podataka i stupanjem na snagu Zakona o provedbi Opće uredbe o zaštiti podataka, prestaje važiti prijašnji Zakon o zaštiti osobnih podataka (NN, broj 103/03., 118/06., 41/08., 130/11. i 106/12- pročišćeni tekst). Za nadzor provedbe uredbe Europskog parlamenta i Vijeća o zaštiti pojedinca u vezi s obradom osobnih podataka te Zakona o provedbi Opće uredbe o zaštiti podataka (NN, broj 42/18[37]) kojim se osigurava provedba uredbe zaslužna je Agencija za zaštitu osobnih podataka. Agencija za zaštitu osobnih podataka nadležna je za obavljanje zadaća koje su joj povjerene i izvršavanje ovlasti koje su joj dodijeljene u skladu s Općom uredbom o zaštiti podataka na području Republike Hrvatske. Misija Agencije za zaštitu osobnih podataka je uspješno izvršavanje nadzora nad provođenjem propisa o zaštiti osobnih podataka, te omogućavanje ostvarivanja tog prava svakom pojedincu u Republici Hrvatskoj, praćenje razvoja na tom području, te predlaganje mjera za unaprjeđenje zaštite osobnih podataka [47].

Općom uredbom o zaštiti podataka zajamčena su prava za sve građane Republike Hrvatske kao i za građane Europske unije. Prilikom obrade podataka korisnika organizacije, društva ili državnog tijela trebaju na jasan i sažet način informirati korisnika o upotrebi njegovih podataka što obuhvaća informacije [46]:

[36] *General Data Protection Regulation*(EUR- Lex, broj 2016/679), [Izvor: https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A32016R0679, Pristupljeno: 13.02.2023.]
[37] Narodne novine, broj 42/2018., [Izvor: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, Pristupljeno: 13.02.2023.]

- za koju će se svrhu podaci koristiti,
- koji je pravni temelj za obradu podataka,
- koliko će dugo podaci biti pohranjeni,
- s kime će dijeliti podatke,
- osnovnih prava u pogledu zaštite podataka.
- hoće li se podaci prenositi izvan EU-a,
- prava na podnošenje pritužbe,
- kako povući privolu,
- kontakt podataka organizacije/društva odgovorne za obradu podataka.

5.3 Krajnji korisnici i zaštita njihovih osobnih podataka

Sigurnost bi uvijek trebala biti na umu kada je korisnik na mreži. Bilo na većoj organizacijskoj razini ili na individualnoj razini, uvijek bi trebalo imati barem neki način da se zaštite podaci. Što se više podataka mora zaštititi, to važniji postaje čin zaštite podataka.

Osobni podaci obično se odnose na podatke koji mogu identificirati osobu, kao što su podaci o kreditnoj kartici, podaci o bankovnom računu, broj socijalnog osiguranja ili drugi osjetljivi podaci. Čin zaštite podataka uključuje radnje poput zaštite važnih informacija od oštećenja, ugrožavanja ili gubitka. Velik dio zaštite podataka osigurava da se podaci mogu brzo vratiti nakon situacije kao što je gubitak ili oštećenje podataka. Ostale ključne komponente zaštite podataka prvenstveno uključuju radnje kao što su zaštita i zaštita podataka od ugrožavanja. Da bi se to postiglo, uvijek treba znati s kime se dijele informacije, održavati odgovarajuću sigurnost na uređajima i znati kako pravilno raspolagati podacima kada više ne budu potrebni [48] .

Ljudi iz cijelog svijeta provode više od 7 sati na internetu svaki dan. Iako internet i digitalne tehnologije pomažu i olakšavaju život, nose i određene opasnosti. Broj povreda podataka raste svake godine, a internetska sigurnost postaje veliki problem. I pojedinci i tvrtke moraju zaštititi svoje podatke na internetu. Nekoliko načina kojima se učinkovito mogu zaštiti podaci su [49]:

- Šifriranje podataka pomoću VPN-a - Jedan od najučinkovitijih načina da korisnik zaštititi svoje podatke je da počne koristiti VPN uslugu. VPN je kratica za virtualnu privatnu mrežu, uslugu koja omogućuje odabir poslužitelja i lokacije koju korisnik želi koristiti za spajanje na internet. Tehnologija je u uporabi od 2005. godine, dobro

je ispitana i sigurna za korištenje. Pruža nekoliko prednosti vrijednih pažnje. Pružatelji VPN usluga koriste industrijske protokole enkripcije kao što su OpenVPN, IPSec/IKEv2 i L2TP/IPSec kako bi pružili *end-to-end* enkripciju. To znači da će prilikom korištenja VPN-a podaci biti kodirani. Čak i ako netko uspije ući u korisnikovu vezu i ukrasti podatke, neće ih moći dešifrirati i upotrijebiti. Osim što kriptira podatke i čini ih neupotrebljivima za sve osim korisnika, VPN također maskira korisnikovu IP adresu i dodjeljuje novu, čime štiti njegovu privatnost i anonimnost.

- Ne spremanje lozinke na pregledniku - Mnogi preglednici i aplikacije imaju praktičnu opciju za pohranjivanje zaporki, ali ako se izgubi uređaj, bude ukraden ili netko drugi koristi radnu stanicu, imat će puni pristup svim računima za koje je korisnik pohranio zaporke. Da bi se to izbjeglo, treba se onemogućiti automatsko pohranjivanje lozinki. Ako korisnik smatra da je automatsko popunjavanje obavezna pogodnost, treba koristiti odgovarajući upravitelj zaporki za sigurno pohranjivanje zaporki. Upravitelji zaporki omogućuju da korisnik zadrži svoje zaporke na jednom mjestu i zaključa ih glavnom zaporkom. Najbolji upravitelji zaporki kompatibilni su s više uređaja, što omogućuje praktičnu pohranu zaporki na mobilnim i stolnim uređajima.
- Izbjegavanje upotrebe javne mreže - Javni Wi-Fi praktičan je kao i automatsko popunjavanje. Korisnik može uštedjeti dodatne podatke na svom planu ili izbjeći značajne troškove tijekom putovanja. Međutim, javni i besplatni Wi-Fi u zračnoj luci ili restoranu ne dolazi bez rizika. Većina javnih Wi-Fi mreža nije osigurana. Haker može lako preuzeti kontrolu nad mrežom i ući u korisnikovu vezu. Oni mogu vidjeti koje web stranice posjećuje, račune i lozinke ili instalirati zlonamjerni softver na uređaj kako bi pratili aktivnost i ukrali podatke, čak i kada se više ne koristi javni Wi-Fi.
- Ažuriranje alata, aplikacija i operativnog sustava- Svaka aplikacija i alat koji se koristi, uključujući operativni sustav, dio je softvera koji zahtijeva redovita ažuriranja. Ova ažuriranja ne uključuju samo nove i poboljšane značajke, već i zakrpe ranjivosti i sigurnosna ažuriranja. Na primjer, jedno od najnovijih sigurnosnih ažuriranja sustava Microsoft Windows zakrpa ranjivost koja je

hakerima omogućila anonimno povezivanje i pristup uređajima s operativnim sustavom Windows. Najvažnije je ažurirati operativni sustav i alate za aplikacije kako bi se spriječilo iskorištavanje ranjivosti i zaštitilo podatke.

- Ne otvarati nepoznate veze - Provjeravanje i odgovaranje na e-poštu postala je svakodnevna rutina za mnoge ljude. Budući da je to jedan od najpopularnijih komunikacijskih kanala, kibernetički kriminalci će ga često koristiti kako bi se dočepali podataka. Da bi to učinili, koriste takozvane *phishing* veze. Nakon što korisnik klikne a poveznicu, velike su šanse da će se uređaj zaraziti zlonamjernim softverom. Iako je najsigurnija praksa izbjegavanje klikanja na nepoznate privitke i poveznice, najbolje bi bilo naučiti uočiti *phishing* e-poštu.
- Ne dijeliti osobne podatke s drugima- Mnogi ljudi internetsku sigurnost shvaćaju olako. Svoje privatne podatke dijele rado i bez ikakve brige. Dijele svoju lokaciju na društvenim mrežama, odvajaju vrijeme za ispunjavanje anketa kako bi dobili besplatne stvari i pretplaćuju se na popise e-pošte kako bi dobili pristup bonus pogodnostima na web stranicama. Prva linija obrane osobnih podataka je sam korisnik. Ako dijeli svoje osobne podatke na internetu, riskira da procure nakon što tvrtka s kojom ih je podijelio bude hakirana. Značajno poboljšanje sigurnosti podataka je ako ih se drži privatnima i podalje od stranica kao što su društveni mediji. Ako ih korisnik želi dijeliti na mreži, treba pročitati pravila o privatnosti stranice koju koristite kako bi bio siguran da stranice ne pohranjuju i ne dijele podatke s trećim stranama.
- Korištenje proizvoda za kibersigurnost - Vrhunski kibersigurnosni proizvodi nisu rezervirani samo za tvrtke. Svaki popularni proizvod za kibernetičku sigurnost ima verziju za osobnu upotrebu. Ovi su proizvodi razvijeni za praćenje uređaja i veze u stvarnom vremenu i rano otkrivanje zlonamjernog softvera, a mogu pomoći u čišćenju uređaja od zlonamjernog softvera i virusa. Oni automatski skeniraju USB flash pogone kako bi spriječili zlonamjerni softver uređajima korisnika.
- Ne koristiti osobne uređaje na poslu-Mnoge organizacije zahtijevaju od zaposlenika da budu online putem šifrirane privatne mreže tvrtke. Također mogu imati drugačija rješenja za kontrolu pristupa i demokratizaciju podataka. To jednostavno znači da će svi osobni podaci proći kroz mrežu kojom upravlja i upravlja tvrtka. Drugim

riječima, tvrtka može pregledati podatke i oni se čak mogu pohraniti, izlažući korisnika rizicima od curenja podataka ako tvrtka postane žrtva kibersigurnosnog napada.

- Praćenje aktivnosti na uređajima i alatima- Praćenje aktivnosti preko računa, izvješća, aktivnosti i alata je ključno. Kibernetički napad poput iznenadnog masovnog prijenosa podataka ne izgleda kao svakodnevna aktivnost. Praćenje može pomoći u otkrivanju odstupanja, zaštititi podatke i spriječiti povrede kibernetičke sigurnosti. Najbolji način je korištenje alata razvijenih izričito za praćenje aktivnosti korisnika, uređaja i mreže. Postoji mnogo alata u ovoj kategoriji, uključujući Nagios Core za praćenje mrežne aktivnosti, Apps Tracker za praćenje korištenja aplikacije ili Kiwi Application Monitor za primanje obavijesti kada aplikacije pokreću vanjske programe.

ZAKLJUČAK

Kibernetičko pravo je skup zakona ili posebnih zakona koji se odnose na internetske i računalne prijestupe te se navedenim pokušava regulirati računala i internet. Dotiče gotovo sve aspekte transakcija i aktivnosti te uključuje internet i cyberspace. Kibernetički zakoni daju pravno priznanje elektroničkim dokumentima i strukturu za podršku transakcijama e-podnošenja i e-trgovine te također pružaju pravnu strukturu za smanjenje i kontrolu kibernetičkog kriminala. Pokriva sve transakcije putem interneta i prati sve aktivnosti na internetu. Kibernetički zakoni su važni za kažnjavanje kriminalaca koji čine ozbiljne zločine povezane s računalom kao što su hakiranje, internetsko uznemiravanje, krađa podataka, ometanje mrežnog tijeka rada bilo kojeg poduzeća i napad na drugu osobu ili web stranicu. Kibernetički zakoni određuju različite oblike kažnjavanja ovisno o vrsti zakona koji je prekršen, koga je isti uvrijedilo i gdje je počinjen.

Važno je dovesti kriminalce iza rešetaka jer većina kibernetičkih zločina ne ulazi u kategoriju običnog kriminala i može dovesti do uskraćivanja pravde. Zločini mogu ugroziti povjerljivost i financijsku sigurnost nacije, stoga se ti problemi trebaju rješavati na zakonit način. Ljudska bića postaju kibernetička bića koja odlučuju provesti značajnu količinu vremena u kibernetičkom svijetu. Kako se kibernetički svijet širi, kriminal raste s njim. Kibernetički kriminal je složen, s obzirom na to da u kibernetičkom svijetu ne postoje geografske granice. Radnje na internetu imaju brze i dalekosežne posljedice. Anonimnost koju dodjeljuje kibernetički prostor dodatno komplicira stvari, stoga se takve aktivnosti ne mogu na zadovoljavajući način riješiti konvencionalnim zakonima. Kibernetički zakon/i su zakoni koji uređuju cyber prostor i važni su za sve koji koriste internet, bilo da se radi o pravnim ili fizičkim osobama, odnosno organizacijama ili pojedincima.

Protiv kriminalaca na internetu potrebno se dobro zaštiti. U današnjem digitalnom svijetu ne može se zanemariti kibernetička sigurnost. Jedan jedini sigurnosni proboj može dovesti do otkrivanja osobnih podataka milijuna ljudi. Ta kršenja imaju snažan financijski učinak na tvrtke, a također i gubitak povjerenja kupaca. Samim time može se zaključiti da je kibernetička sigurnost vrlo bitna za zaštitu tvrtki i pojedinaca od pošiljatelja neželjene pošte i kibernetičkih kriminalaca. Kibernetička sigurnost je važna jer štiti uređaje, podatke i povjerljive informacije od kibernetičkih napada. Također pomaže da se izbjegnu online prijevare, ostane u skladu s propisima i zaštititi

ugled. Osim toga, kibernetička sigurnost smanjuje rizik od kibernetičkih napada i pomaže pri oporavku od istog.

Zaštita podataka je važna jer štiti organizacije od mogućih napada hakiranja, krađe informacija i identiteta. Svaka organizacija koja želi učinkovito raditi mora osigurati sigurnost svojih informacija provedbom plana zaštite podataka. Kako se povećava količina pohranjenih i stvorenih podataka, tako raste i važnost zaštite podataka. Povrede podataka i kibernetički napadi mogu prouzročiti razornu štetu. Organizacije moraju proaktivno štititi svoje podatke i redovito ažurirati svoje zaštitne mjere. U konačnici, ključno načelo i važnost zaštite podataka je čuvanje i zaštita podataka od različitih prijetnji i pod različitim okolnostima.

LITERATURA

[1] Upcounsel. CyberLaw: Everything You Need To Know., Listopad 2022. Preuzeto: https://www.upcounsel.com/cyber-law [Pristupljeno: Svibanj 2023.]

[2] Java T point. What is Cyber Law?. Preuzeto: https://www.javatpoint.com/what-is-cyber-law [Pristupljeno: Svibanj 2023.]

[3] Csonka Peter. Revue internationale de droit penal, The council of europe's convention on cyber-crime and other European initiatives. 2006/3-4(vol. 77), 473-501. Preuzeto: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm#no21 [Pristupljeno: Svibanj 2023.]

[4] Kokot, I.: Kaznenopravna računalnih sustava, programa i podataka, Pregledni znanstveni rad, Sveučilište u Zagrebu, Pravni Fakultet, 2014. Preuzeto: https://hrcak.srce.hr/file/209347 [Pristupljeno: Svibanj 2023.]

[5] IUS-INFO. Sankcioniranje cyber nasilja prema novom Kaznenom zakonu., Bagović K, Lipanj 2012. Preuzeto: https://www.iusinfo.hr/aktualno/u-sredistu/13063 [Pristupljeno: Svibanj 2023.] Kate Bagović, mr. sc., Zagreb

[6] Future Learn. How has the Internet affected freedom of speech?. Preuzeto: https://www.futurelearn.com/info/courses/global-citizenship/0/steps/121650 [Pristupljeno: Lipanj 2023.]

[7] BITLAW. Domain name disputes. Preuzeto: https://www.bitlaw.com/internet/domain.html [Pristupljeno: Lipanj 2023.]

[8] European Commision. Preuzeto: https://digital-strategy.ec.europa.eu/hr/policies/online-disinformation [Pristupljeno: Kolovoz 2023.]

[9] Medijska pismenost. Preuzeto: https://medijskapismenost.raskrinkavanje.ba/oblici-manipulacija-i-kome-se-obratiti-ako-ih-uocite/koji-sve-oblici-medijskih-manipulacija-postoje/dezinformacija/ [Pristupljeno: Kolovoz 2023.]

[10] Creative Commons. Preuzeto: https://creativecommons.org/ [Pristupljeno: Kolovoz 2023.]

[11] TechTarget. What is Cybersecurity?. Shea S., Rujan 2022. Preuzeto: https://www.techtarget.com/searchsecurity/definition/cybersecurity [Pristupljeno: Prosinac 2022.]

[12] IBM. What is cybersecurity?. Preuzeto: https://www.ibm.com/topics/cybersecurity [Pristupljeno: Svibanj 2023.]

[13] CROWDSTRIKE. The 12 most common types of malware, Baker K., Veljača 2023. Preuzeto: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/ [Pristupljeno: Lipanj 2023.]

[14] Astra. 10 of the biggest ransomware attacks in history. Preuzeto: https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/ [Pristupljeno: Lipanj 2023.]

[15] Graphus. The worst phishing attacks in history. Preuzeto: https://www.graphus.ai/blog/worst-phishing-attacks-in-history/ [Pristupljeno: Lipanj 2023.]

[16] Infosec. 8 of the world's biggest insider threat security incidents., Morrow S., Rujan 2020. Preuzeto: https://resources.infosecinstitute.com/topic/8-of-the-worlds-biggest-insider-threat-security-incidents/ [Pristupljeno: Lipanj 2023.]

[17] Microsoft. Top 5 most famous DDoS attacks. Preuzeto: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/top-5-most-famous-ddos-attacks#:~:text=The%20effects%20of%20Mafiaboy's%20attacks,Tbps%20of%20information%20to%20Google [Pristupljeno: Lipanj 2023.]

[18] Get safe online. Five notable examples of advanced persistent threat attacks. Preuzeto: https://www.getsafeonline.org/business/blog-item/five-notable-examples-of-advanced-persistent-threat-apt-attacks/ [Pristupljeno: Lipanj 2023.]

[19] Heimdal. Famous man-in-the-middle examples., Georgescu E., Kolovoz 2021. Preuzeto: https://heimdalsecurity.com/blog/man-in-the-middle-mitm-attack/#:~:text=The%20Marconi%20Case,the%20inventor%20of%20the%20radio [Pristupljeno: Lipanj 2023.]

[20] Cobalt. 8 biggest cybersecurity attacks in history, Fox J., Listopad 2022. Preuzeto: https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history [Pristupljeno: Svibanj 2023.]

[21] Tech Monitor. The six biggest cyberattacks in history, Silvia Pellegrino, Srpanj 2022. Preuzeto: https://techmonitor.ai/technology/biggest-cyberattacks-in-history [Pristupljeno: Svibanj 2023.]

[22] U.S Deparment of Defense. Preuzeto: https://www.defense.gov/ [Pristupljeno: Lipanj 2023.]

[23] NASA. Preuzeto: https://www.nasa.gov/ [Pristupljeno: Lipanj 2023.]

[24] Mataić I. Cyber security-zaštita kritičnih infrastruktura. Završni rad. Sveučilište Sjever u Zagrebu, 2022. Preuzeto: https://dabar.srce.hr/islandora/object/unin:5406, Pristupljeno: Kolovoz 2023.]

[25] UpGuard. List of Cybersecurity Regulations in the European Union, Kaushik Sen, Ožujak 2023. Preuzeto: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union [Pristupljeno: Svibanj 2023.]

[26] Knowledgehut. Cyber Security Laws and Regulations of 2023, Narasimman Preethiga, Lipanj 2023. Preuzeto: https://www.knowledgehut.com/blog/security/cyber-security-laws [Pristupljeno: Lipanj 2023.]

[27] ENISA. About ENISA- The European Union Agency for Cybersecurity. Preuzeto: https://www.enisa.europa.eu/about-enisa [Pristupljeno: Siječanj 2023.]

[28] ENISA. A trusted and cyber secure Europe. Preuzeto: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy [Pristupljeno: Siječanj 2023.]

[29] ENISA. Supporting the implementation of Union policy and law regarding cybersecurity. Preuzeto: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[30] Ipleaders. What is ENISA and how ha sit hečšed enforce cyber laws in the EU, Rishabh Mishr, Listopad 2021. Preuzeto: https://blog.ipleaders.in/what-is-enisa-and-how-has-it-helped-enforce-cyber-laws-in-the-eu/ [Pristupljeno: Siječanj 2023.]

[31] European Commission. Directive on measures for high common level of cybersecurity across the Union. Preuzeto: https://digital-strategy.ec.europa.eu/en/policies/nis2-

directive#:~:text=The%20Directive%20on%20security%20of,them%20to%20be%20appropriately%20equipped. [Pristupljeno: Siječanj 2023.]

[32] UpGuard. List of Cybersecurity Regulations in the European Union, , Kaushik Sen, Ožujak 2023. Preuzeto: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union [Pristupljeno: Svibanj 2023.]

[33] European Commission. The EU Cybersecurity Act. Preuzeto: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act [Pristupljeno: Svibanj 2023.]

[34] GDPR-eu. What is GDPR, the EU's new data protection law?, Ben Wolford, 2020. Preuzeto: https://gdpr.eu/what-is-gdpr/ [Pristupljeno: Siječanj 2023.]

[35] Poslovni.hr. Za kršenje GDPR-a izdane 32 kazne, pogledajte tko je najčešće kažnjavan, Poslovni.hr/Hina, svibanj 2023. Preuzeto: https://www.poslovni.hr/hrvatska/za-krsenje-gdpr-a-izdane-32-kazne-pogledajte-tko-je-najcesce-kaznjavan-4388828 [Pristupljeno: Lipanj 2023.]

[36] Tipurić M., *Pregled usluga računalstva u oblaku za obradu prometnih podataka.* Završni rad. Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2021. Preuzeto sa: https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A2415/datastream/PDF/view [Pristupljeno: Svibanj 2023.]

[37] Techtarget. General Dana Protection Regulation, Castagna Rich, Siječanj 2021. Preuzeto: https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR [Pristupljeno: Siječanj 2023.]

[38] Microsoft Azure, *What is cloud computing?;* Preuzeto sa: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/ [Pristupljeno: Svibanj 2023.]

[39] Fortra, *What are the most common cloud computing service delivery models?*, Torres Corral, Lipanj 2021. Preuzeto sa: https://www.alertlogic.com/blog/what-are-the-most-common-cloud-computing-service-delivery-models/ [Pristupljeno: Svibanj 2023.]

[40] VECTRA. What are Cloud Security Threats?. Preuzeto: https://www.vectra.ai/learning/cloud-security-threats [Pristupljeno: Svibanj 2023.]

[41] Mdn web docs. Content Security Policy. Preuzeto: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP [Pristupljeno: Lipanj 2023.]

[42] Check Point. Top 15. Cloud Security Issues, Threats and Concerns. Preuzeto: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ [Pristupljeno: Svibanj 2023.]

[43] IBM. What is cloud security?. Preuzeto: https://www.ibm.com/topics/cloud-security [Pristupljeno: Svibanj 2023.]

[44] Kaspersky. What is cloud security? Preuzeto: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security [Pristupljeno: Svibanj 2023.]

[45] Varonis. Data: Definition, Explanation and Guide. Harrington D., 6. srpnja 2021. Preuzeto: https://www.varonis.com/blog/data-security [Pristupljeno: Svibanj 2023.]

[46] Azop. Prava ispitanika. Preuzeto: https://azop.hr/prava-ispitanika/ [Pristupljeno: Svibanj 2023.]

[47] Azop. Djelokrug. Preuzeto: https://azop.hr/djelokrug/ [Pristupljeno: Svibanj 2023.]

[48] TechTarget. 10 tips to keep your personal dana safe and secure, Alexander S. Gillis, 2020. Preuzeto: https://www.techtarget.com/whatis/10-Tips-to-Keep-Personal-Data-Safe-and-Secure [Pristupljeno: Svibanj 2023.]

[49] National Cybersecurity Alliance. 10 must know tips for keeping your personal dana safe. Preuzeto: https://staysafeonline.org/resources/10-must-know-tips-for-keeping-your-personal-data-safe/ [Pristupljeno: Svibanj 2023.]

POPIS SLIKA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je Diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada 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.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Kibernetičko pravo, sigurnost i zaštita osobnih podataka , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 29. Kolovoza 2023.

Mateo Tipurić, TIPURIĆ MATEO
(ime i prezime, *potpis*)