# Informacijski kriminalitet

**Jakolić, Kristina**




**VELEUČILIŠTE**

**s pravom javnosti**

**BALTAZAR ZAPREŠIĆ**

**Zaprešić**

**Preddiplomski stručni studij**

**Informacijske tehnologije**

**KRISTINA JAKOLIĆ**

# INFORMACIJSKI KRIMINALITET

**STRUČNI ZAVRŠNI RAD**

**Zaprešić, 2020. godine**

**VELEUČILIŠTE**

**s pravom javnosti**

**BALTAZAR ZAPREŠIĆ**

**Zaprešić**

**Preddiplomski stručni studij**

**Informacijske tehnologije**

**STRUČNI ZAVRŠNI RAD**

# INFORMACIJSKI KRIMINALITET

**Mentorica:**
**Dr. sc. Alisa Bilal Zorić**

**Studentica:**
**Kristina Jakolić**

**Naziv kolegija:**
**INFORMACIJSKE TEHNOLOGIJE**

**JMBAG studenta:**
**0135241749**

# Sadržaj

# SAŽETAK

Cilj ovog rada je upoznati čitatelja/e sa problemom informacijske sigurnosti s naglaskom na *cyber* kriminalitet unutar informacijskih sustava i njegov utjecaj na iste. U virtualnom svijetu, to se odnosi na bilo kakvo neovlašteno korištenje, dostupnost ili tajnost digitalnih podataka te njihova zloupotreba koja je po svojim posljedicama sve opasnija po društvo, ali i pojedinca. Budući da je informacijski, odnosno računalni kriminalitet raširen u različitim segmentima poslovanja, ali i samog života, potrebno je osvijestiti društvo i pojedince o posljedicama te kako da na vrijeme uoče nepravilnosti u radu i spriječe negativne posljedice koje računalni kriminalitet donosi.

**Ključne riječi**: informacijski sustavi, računalni kriminalitet, zlouporaba

# ABSTRACT

The aim of this paper is to familiarize the reader with the problem od information security with an emphasis on *cybercrime* within Information systems and its impact on them. In the virtual world, *cybercrime* refers to any unauthorized use, availability or secrecy of digital data and their misuse, which in its consequences is increasingly dangerous to society as well as to individuals. Since information or *cybercrime* is widespread in various segments of business, but also in life itself, it is necessary to make society and individuals aware of the consequences and how to detect irregularities and prevent the negative impact of computer crime.

**Key words**: Information systems, *cybercrime*, misuse

# 1. UVOD

Uz kontinuirano uvođenje tehnologije dolazi do povećane izloženosti i rizika, posebno za kibernetički kriminal i *cyber*-terorizam. Kako bi mogli definirati što je zapravo kibernetički kriminal, u poglavlju Informacijski sustavi ćemo se osvrnuti na sustav koji *cybercrime* zapravo napada.

Sami pojam *cyber* kriminala ne razlikuje se radikalno od koncepta konvencionalnog kriminala. Oba uzrokuju kršenje zakona i povredu prava pojedinca. Najčešće se napadi u *cyber*-prostoru izvode zbog financijske dobiti ili onemogućavanja rada neke organizacije, ali nerijetko se pretvore u kibernetičke ratove oštećujući tako i cijelu ekonomiju društva što će biti spomenuto u poglavlju Hakiranje.

Tehnologija je danas neizostavna u različitim segmentima poslovanja, ali i samog života te svi koji imaju mogućnost pristupa Internetu, mogu upoznavati nove ljude, razvijati svoje vještine, kupovati ili prodavati dobra putem raznih web-stranica te biti povezani u privatnom, ali i poslovnom svijetu. Što više mogućnosti tehnologija otvara, to više rizika i izloženosti postoji jer kibernetički kriminal nije ograničen. Može se dogoditi bilo kada, bilo gdje i bilo kome, jeftino ga je počiniti i teško otkriti, a kako se preventivno zaštititi od samih napada će biti pobliže opisano u poglavlju Mjere zaštite od *cyber* kriminaliteta.

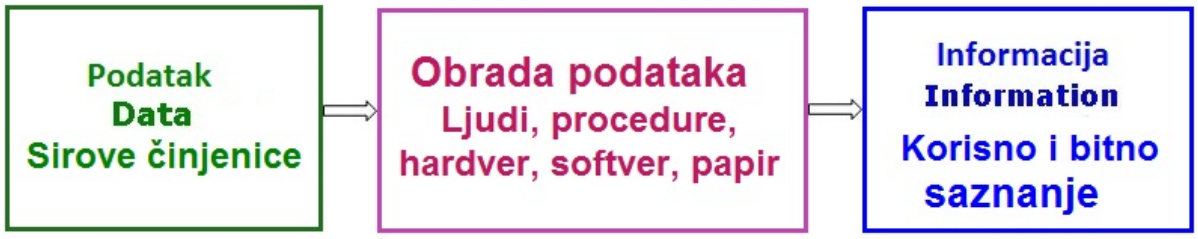
# 2. INFORMACIJSKI SUSTAVI

Da bi mogli definirati informacijski sustav, potrebno je objasniti par pojmova koji ga se tiču, a to su podatak, informacija, znanje i sami sustav.

**Podatak** je skup prepoznatljivih znakova, odnosno simbola zapisanih na nekom mediju čime zapisujemo činjenice, pritom ne razmatrajući njihov kontekst (Varga, 2014.).

Interpretacijom podataka i stavljanjem istih u kontekst, nastaje **informacija**. Informacija je , dakle, činjenica s određenim značenjem koja donosi novost, obavještava o nečemu, otklanja neizvjesnost te općenito služi kao podloga za odlučivanje. Da bi ona bila kvalitetna treba imati sljedeće karakteristike: točnost, potpunost, relevantnost i pravovremenost (Varga, 2014.).

Kada bi spojili kombinaciju podataka i informacija te im pridodali ekspertno mišljenje, vještinu i iskustvo (Varga, 2014.), dobili bi **znanje** pomoću kojeg možemo kreirati nove podatke i značenja.




*Slika 1 - Odnos podatka i informacije*

*Izvor: znanje.org*

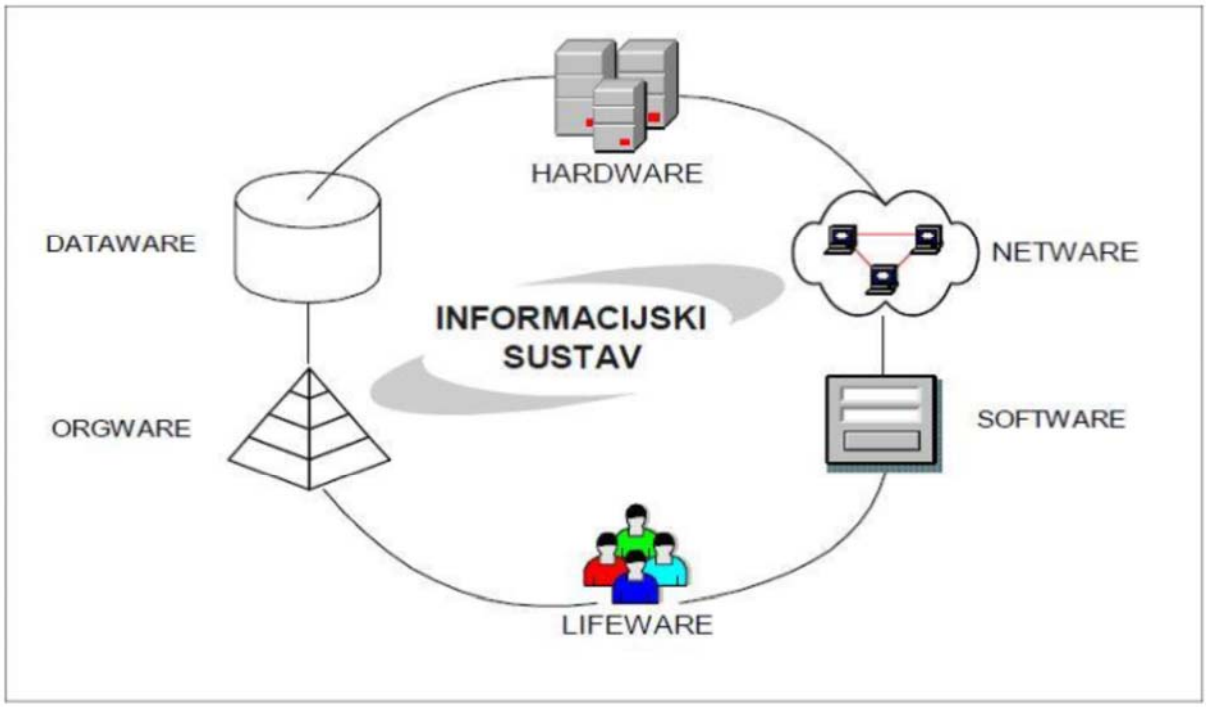
**Sustav** se može definirati kao grupa međuovisnih komponenti koja funkcionira zajedno kako bi se postigao željeni učinak, odnosno rezultat.( L. Whitten, J.; D. Bentley, 2007.)

Kako navodi Varga**, informacijski sustav** je „sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju i društvo, tako da budu dostupne i upotrebljive za svakog tko ih želi koristiti, uključujući poslovodstvo, klijente, osoblje i ostale“.

Prema Spremiću i Srići, svaki informacijski sustav sastoji se od šest komponenti:

1. **Hardware** (materijalna osnova) – ulazno-izlazni uređaji, sama računala, zajedno s bilo kojim perifernim uređajima, uključujući poslužitelje, monitore, pisače i uređaje za pohranu
2. **Software** (nematerijalni elementi) – prikupljanje, organiziranje i manipuliranje podacima i izvršavanje uputa,
3. **Netware** – skup protokola za komunikaciju između računala,
4. **Lifeware** – ljudska komponenta,
5. **Orgware** – usklađivanje svih komponenti u cjelinu raznim metodama i organizacijskim postupcima

6. **Dataware** – velika zbirka podataka i informacija koja koristi za donošenje odluka.




*Slika 2 - Komponente informacijskog sustava*

*Izvor: Srića, V.; Spremić, M.: Informacijskom tehnologijom do poslovnog uspjeha, Sinergija, Zagreb, 2000.*

# 3. POJAM I DEFINIRANJE *CYBER* KRIMINALITETA

U hrvatskom jeziku ne postoji inačica koja bi vjerodostojno prevela englesku riječ *cyber*. *Convention on Cybercrime/Konvencija o kibernetičkom kriminalu* na hrvatskom nije prevedena potpuno točno jer *cyber* ne možemo poistovjetiti sa riječju kibernetika jer kibernetiku prema Hrvatskom jezičnom portalu definiramo kao „znanost o istraživanju i automatskim sustavima kontrole u strojeva i živih bića, istraživanje procesa upravljanja raznim sustavima (biološkim, tehničkim, ekonomskim i dr.)“, dok Oxford dictionary opisuje *cyber* kao „pridjev koji se odnosi na ili je karakterističan za kulturu računala, elektroničke komunikacijske mreže, informacijske tehnologije i virtualnu stvarnost“. Zbog toga će se u ostatku rada koristiti upravo *cyber*.

Prvi zabilježeni *cyber* zločin dogodio se 1820. kada je Joseph – Marie Jacquard, francuski proizvođač tekstila, proizveo razboj/tkalački stan koji je radio na principu bušenih kartica. Razboj je omogućio ponavljanje niza koraka u tkanju posebnih tkanina te je to rezultiralo strahom među zaposlenicima da im prijeti gubitak posla pa su počeli činiti sabotaže kako bi Jacquarda odvratili od daljnje upotrebe nove tehnologije.[1] Od tada su računala prešla dug put, a *cyber* kriminalitet je napredovao.

Postoji mnoštvo definicija za *cyber* kriminalitet, no nijedna nije u potpunosti adekvatna za tako širok pojam, ali u suštini se sve svode na to da je *cybercrime* zločin koji uključuje računalo i mrežu. (Moore, 2005) Računalo u ovom smislu može biti korišteno za počinjenje napada, ali također može biti i meta počinitelja. Zašto je teško definirati *cybercrime*? „Jer da bi se neko djelo smatralo krivičnim mora se odvijati unutar specifičnih vremenskih i prostornih granica u kojima je ono prepoznato kao zabranjeno“ (Moise, 2014). *Cybercrime* u sebi uključuje sve, od preuzimanja ilegalnih glazbenih datoteka do krađe milijuna sa bankovnih računa. Uključuje i nemonetarna kaznena djela kao što su virusi, krivotvorenje, internetsko vrebanje ili pak objava povjerljivih podataka.

Kibernetički zločini od konvencionalnih se razlikuju na četiri načina (Chawki 2005):

1) Lako je naučiti kako se počine,
2) Zahtijevaju malo resursa u odnosu na potencijalnu štetu,
3) Mogu se počiniti u bilo kojoj nadležnosti, a da u njoj počinitelj nije fizički prisutan i
4) Često nisu očito ilegalni.

Većina objavljenih *cyber* kriminala uključuje (Schell, Martin 2004):

- „Cracking“ - stjecanje neovlaštenog pristupa računalnim sustavima radi počinjenja kaznenog djela
- Piratstvo – kopiranje zaštićenog softvera bez autorizacije

[1] https://www.academia.edu/1869461/Cyber_Crime

- *Cyber* vrebanje – uznemiravanje i teroriziranje pojedinca ili institucije korištenjem računala, uzrokujući strah ili štetu
- *Cyber* pornografija – izrada i/ili distribucija pornografije koristeći računalo
- *Cyber* terorizam – nezakoniti napadi i prijetnje napada terorista protiv računala, mreža i informacija pohranjenih u njima u svrhu zastrašivanja ili prisiljavanja vlade ili ljudi da unaprijede političke ili društvene ciljeve počinitelja

U tablici 1 prikazana su najzastupljenija kaznena djela cyber kriminaliteta u Republici Hrvatskoj 2017. i 2018. godine.

*Tablica 1 – Kaznena djela cyber kriminaliteta*

*Izvor: https://www.sabor.hr/sites/default/files/uploads/sabor/2019-12-18/122002/IZVJESCE_MUP_2018.pdf*

| **Kaznena djela** | **Prijavljena** | | |
|---|---|---|---|
| | **Broj djela** | | **+/-%** |
| | **2017.** | **2018.** | |
| **Iskorištavanje djece za pornografiju** | 140 | 55 | -60,7 |
| **Neovlašteni pristup** | 7 | 16 | +128,60 |
| **Ometanje rada računalnog sustava** | 11 | 1 | -90,9 |
| **Računalno krivotvorenje** | 37 | 32 | -13,5 |
| **Računalna prijevara** | 1.114 | 1.310 | +17,6 |
| **Povreda žiga** | 80 | 130 | +62,5 |

Po podacima iz tablice vidimo da je najzastupljenija računalna prijevara, a po podacima iz Ministarstva unutarnjih poslova o obavljanju policijskih poslova u 2018. godini (Slika 2) možemo vidjeti da je ona drugo po redu najučestalije kazneno djelo gospodarskog kriminaliteta u Republici Hrvatskoj.

| Redni broj | Najučestalija kaznena djela gospodarskog kriminaliteta od 2014. - 2018.*** | Kaznena djela | | | | | Prijavljene osobe za kaznena djela | | | | | Prosječan broj kaznenih djela po počinitelju | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2014. | 2015. | 2016. | 2017. | 2018. | 2014. | 2015. | 2016. | 2017. | 2018. | 2014. | 2015. | 2016. | 2017. | 2018. |
| 1. | Krivotvorenje službene ili poslovne isprave | 1.653 | 1.781 | 1.759 | 2.323 | 1.564 | 88 | 107 | 88 | 65 | 63 | 18,8 | 16,6 | 20,0 | 35,7 | 24,8 |
| 2. | Računalna prijevara | 960 | 1.361 | 1.365 | 1.114 | | 70 | 78 | 81 | 102 | | 13,7 | 17,4 | 16,9 | 10,9 | |
| 3. | Zlouporaba položaja i ovlasti | 758 | 674 | 656 | 552 | 470 | 219 | 251 | 152 | 110 | 71 | 3,5 | 2,7 | 4,3 | 5,0 | |
| 4. | Nedozvoljena trgovina | 453 | 401 | 399 | 357 | | 321 | 291 | 234 | 206 | | 1,4 | 1,4 | 1,7 | 1,7 | |
| 5. | Zlouporaba povjerenja u gospodarskom poslovanju | 374 | 393 | 355 | 418 | 480 | 192 | 178 | 201 | 268 | 183 | 1,9 | 2,2 | 1,8 | 1,6 | 2,6 |
| 6. | Prijevara u gospodarskom poslovanju | 338 | 239 | 262 | 170 | 263 | 210 | 212 | 219 | 147 | 116 | 1,6 | 1,1 | 1,2 | 1,2 | 2,3 |
| 7. | Pronevjera | 282 | 359 | 370 | 542 | 444 | 166 | 171 | 195 | 167 | 158 | 1,7 | 2,1 | 1,9 | 3,2 | 2,8 |
| 8. | Izbjegavanje carinskog nadzora | 101 | 147 | 89 | 50 | 5 | 102 | 111 | 60 | 48 | 5 | 1,0 | 1,3 | 1,5 | 1,0 | 1,0 |
| 9. | Računalno krivotvorenje | 169 | 80 | 52 | 37 | | 10 | 1 | 12 | 2 | | 16,9 | 80,0 | 4,3 | 18,5 | |
| 10. | Utaja poreza ili carine | 165 | 141 | 404 | 148 | 292 | 73 | 73 | 175 | 73 | 196 | 2,3 | 1,9 | 2,3 | 2,0 | |
| 11. | Zlouporaba osobne isprave | 67 | 116 | 82 | 56 | 82 | 31 | 24 | 19 | 23 | 35 | 2,2 | 4,8 | 4,3 | 2,4 | 2 |
| 12. | Nedozvoljena igra na sreću | 159 | | | | | 182 | | | | | 0,9 | | | | |
| 13. | Protupravna eksploatacija rudnog blaga | 134 | 1 | 3 | 116 | 2 | 12 | 1 | 3 | 6 | 3 | 11,2 | 1,0 | 1,0 | 19,3 | 1 |
| 14. | Zlouporaba naprava | 19 | 69 | 160 | 9 | | 70 | 0 | 1 | 10 | | 0,3 | | 160,0 | 0,9 | |
| 15. | Primanje mita | 61 | 28 | 124 | 95 | 19 | 26 | 15 | 3 | 23 | 3 | 2,3 | 1,9 | 41,3 | 4,1 | 6 |
| 16. | Davanje mita | 55 | 34 | 98 | 98 | 26 | 23 | 19 | 21 | 38 | 25 | 2,4 | 1,8 | 4,7 | 2,6 | 1,0 |
| 17. | Neovlašteni pristup | 16 | 29 | 115 | 7 | | 7 | 8 | 9 | 3 | | 2,3 | 4 | 13 | 2 | |
| 18. | Pogodovanje vjerovnika | 35 | 19 | 92 | 167 | 81 | 14 | 8 | 6 | 4 | 3 | 2,5 | 2 | 15 | 41,8 | 27,0 |
| 19. | Povreda obveze vođenja trgovačkih i poslovnih knjiga | 84 | 67 | 85 | 82 | 107 | 55 | 42 | 48 | 42 | 66 | 1,5 | 2 | 2 | 2,0 | 1,6 |
| 20. | Zlouporaba čeka i platne kartice | 16 | 16 | 13 | 9 | 81 | 10 | 8 | 9 | 8 | 13 | 1,6 | 2 | 1 | 1,1 | 6,2 |
| 21. | Neisplata plaće | 113 | 78 | 148 | 356 | 109 | 59 | 57 | 83 | 59 | 63 | 1,9 | 1 | 2 | 6,0 | 1,7 |
| | **UKUPNO** | **6.012** | **6.033** | **6.631** | **6.706** | **4.025** | **1.940** | **1.655** | **1.619** | **1.404** | **1.003** | **3,1** | **3,6** | **4,1** | **4,8** | **4,0** |
| | **OSTALA KAZNENA DJELA** | 381 | 307 | 480 | 351 | 267 | 237 | 168 | 213 | 144 | 114 | 1,6 | 1,8 | 2,3 | 2,4 | 2,3 |
| | **SVEUKUPNO** | **6.393** | **6.340** | **7.111** | **7.057** | **4.292** | **2.177** | **1.823** | **1.832** | **1.548** | **1.117** | **2,9** | **3,5** | **3,9** | **4,6** | **3,8** |

*Slika 3 – Kaznena djela gospodarskog kriminaliteta*

*Izvor: https://www.sabor.hr/sites/default/files/uploads/sabor/2019-12-18/122002/IZVJESCE_MUP_2018.pdf*

S obzirom na navedeno, možemo potvrditi da „moderni lopov može ukrasti više koristeći računalo nego pištolj, a terorist bi mogao počiniti više štete tipkovnicom nego bombom“ (National Research Council, „Computers at Risk“, 1991).

# 4. KATEGORIJE *CYBER* KRIMINALITETA

*Cyber* kriminal je najnoviji i najsloženiji problem u *cyber* prostoru te se uloga računala u kibernetičkom kriminalu može klasificirati u užem ili širem smislu gdje se računalo može koristiti kao objekt, alat ili računalo kao okruženje ili kontekst. Kibernetski kriminal Schell i Martin (2004) široko su klasificirali na sljedeći način:

## 4.1. *Cyber*-kriminalitet koji rezultira imovinskom štetom

Kibernetski zločini počinjeni nad osobama su vrsta kaznenih djela koja utječu izravno na osobnost pojedinca. Neke od najpoznatijih vrsta kibernetičkih zločina koji predstavljaju prijetnju osobi su sljedeći:

- SMS podvale - Ovdje prijestupnik krade identitet druge osobe u obliku broja mobitela i slanjem SMS-a putem interneta i primatelj dobiva SMS s broja mobitela žrtve. To je vrlo ozbiljan *cyber* zločin protiv bilo kojeg pojedinca.
- "Cracking" / krekiranje
- „Carding" / kartiranje – lažne bankovne kartice, tj. debitne i kreditne kartice koje kriminalci koriste za svoje novčane koristi povlačenjem novca s žrtvinog bankovnog računa
- „Flooding" / poplavljivanje - oblik vandalizma u internetskom prostoru koji rezultira uskraćivanjem usluge (DoS – Denial-of-Service) ovlaštenim korisnicima web mjesta ili sustava
- „Phreaking" – vrsta prijevare kojom se koristeći tehnologiju pozivi ne naplaćuju počinitelju
- Proizvodnja i distribucija računalnih virusa i crva

## 4.2. *Cyber*-kriminalitet koji rezultira štetom za pojedinca

Ova kategorija se općenito dijeli u dvije podkategorije:

- *Cyberstalking* / *cyber*-uhođenje - korištenje internetskog prostora za kontrolu, uznemiravanje ili teroriziranje mete do te mjere da se on ili ona boji ozljede ili smrti, bilo sebe ili drugih koji su mu bliski
- *Cyberpornography* / *cyber*-pornografija - korištenje internetskog prostora za posjedovanje, stvaranje, uvoz, prikazivanje, objavljivanje ili distribuciju pornografije (pogotovo dječje) ili drugih sramotnih materijala

## 4.3. Tehnički neprijestupi

U tehničke neprijestupe spadaju:

- Haktivizam – povezanost hakiranja i aktivizma, način upadanja u računalne sustave temeljem kojih se vrši određena „agresija“ na informatičke programe i politička djelovanja
- *Cyber*-vigilantizam – „preuzimanje zakona u svoje ruke“, svjesno kršenje zakona u nastojanju da se zaštiti vlastiti ili život nekog bliskog.

# 5. HAKIRANJE

Haker je računalni stručnjak koji koristi svoje tehničko znanje kako bi prevladao problem. Iako se "haker" može odnositi na bilo kojeg vještog računalnog programera, taj se izraz u popularnoj kulturi pridružio "sigurnosnom hakeru", nekome tko sa svojim tehničkim znanjem koristi „bugove“ ili eksploatacije kako bi provalio u računalne sustave.[2] Hakerske aktivnosti su u najvećem broju slučajeva neka vrsta manipulacije kako bi se upalo u računalni sustav te su, kako navodi Yar (2006), zbog toga „ključni elementi hakiranja dobivanje pristupa i kontrola nad računalnim sustavom.“ No, ako je to učinjeno na zahtjev i prema ugovoru između etičkog hakera i organizacije, tada je hakiranje legalan čin. Ključna razlika je u tome što etički haker ima ovlaštenje istražiti „metu“. Međutim, većina ljudi hakera zapravo opisuje definicijom krekera. Krekeri su ljudi koji pokušavaju neovlašteno pristupiti računalima.[3] To se obično postiže korištenjem "backdoor" programa instaliranog na računalu. Mnogi krekeri također pokušavaju pristupiti resursima pomoću softvera za razbijanje lozinki, koji pokušava milijardama lozinki pronaći ispravnu za pristup računalu. U nastavku će biti detaljno opisana tri najčešća tipa hakiranja: zlouporaba računalnih tehnologija, kibernetičko ratovanje i kibernetički terorizam, te zašto je digitalna forenzika bitna za suzbijanje *cyber* kriminaliteta.

## 5.1. Malware

Virusi, crvi i drugi zlonamjerni softveri stalna su prijetnja i izvor mnogih problema i ogromnih frustracija za mnoge korisnike. Malware (kratica od *malicious software*; zlonamjerni softver) je općeniti pojam koji opisuje programski kod kreiran s namjerom da našteti računalnom sustavu (Conry-Murray, Weafer, 2005). Obuhvaća brojne zlonamjerne softvere koji će biti detaljno objašnjeni u nastavku.

„Virus je program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt, većina ih se samo razmnožava, ali mnogi mogu oštetiti naš računalni sustav ili korisničke podatke“ (Conry-Murray, Weafer, 2005). Gotovo svi virusi pridruženi su izvršnoj datoteci, što znači da virus možda postoji na računalu, ali ne može zaraziti računalo ako se ne pokrene ili ne otvori zlonamjerni program. Virus se ne može širiti bez ljudskog djelovanja (poput pokretanja zaraženog programa) kako bi se održao. Ljudi šire širenje računalnog virusa, uglavnom nesvjesno, dijeljenjem zaraženih datoteka ili slanjem e-pošte s virusima kao privitke u e-pošti.

Crvi su svojim dizajnom slični virusima te se smatraju njihovim podrazredom. To su programi koji omogućuju distribuciju vlastitih kopija, često bez interakcija čovjeka te za razliku od virusa ne inficiraju datoteke domaćina (Conry-Murray, Weafer, 2005). Najveća opasnost od crva je njegova sposobnost da se replicira na sustavu, pa umjesto da računalo pošalje jednog crva, moglo bi poslati stotine ili tisuće kopija samog sebe, stvarajući ogroman razarajući učinak. Zbog prirode kopiranja

[2] https://en.wikipedia.org/wiki/Hacker
[3] https://securitytrails.com/blog/hacker-vs-cracker

crva i njegove sposobnosti da putuje mrežama, krajnji rezultat je u većini slučajeva da crv troši previše memorije, zbog čega web poslužitelji, mrežni poslužitelji i pojedinačna računala prestaju reagirati.

U tablici 2 i 3 su prikazane detaljnije informacije o pojedinim vrstama virusa i crva.

*Tablica 2 - Virusi*

*Izvor: A.Conry-Murray,V.Weafer: Sigurni na Internetu, 2005.*

| **VIRUSI** | |
|---|---|
| **VRSTA** | **OPIS** |
| **Virus koji inficira datoteke** | Virusi koji inficiraju datoteke sami se kvače za programe, izvršne datoteke i skripte, a ako se na računalu izvodi zaražena datoteka, virus se može raširiti na druge programe. |
| **Makro virus** | Makronaredbe su mali programi koji postoje unutar većih aplikacija te ti virusi mogu sami sebe kopirati, brisati ili mijenjati dokumente i provoditi druge neželjene funkcije. |
| **Virus sektora za podizanje računala** | Virusi koji se izvršavaju svaki put kada se uključi računalo ili se pročita disk. |
| **Virus rezidentan u memoriji** | Virus koji ostaje u memoriji računala nakon aktiviranja koda virusa. |
| **Polimorfni virus** | Virus koji mijenja uzorak svojih bajtova kada se replicira čime sprječava otkrivanje. |
| **Retro virus** | Virus koji aktivno napada antivirusni program da bi spriječio otkrivanje. |

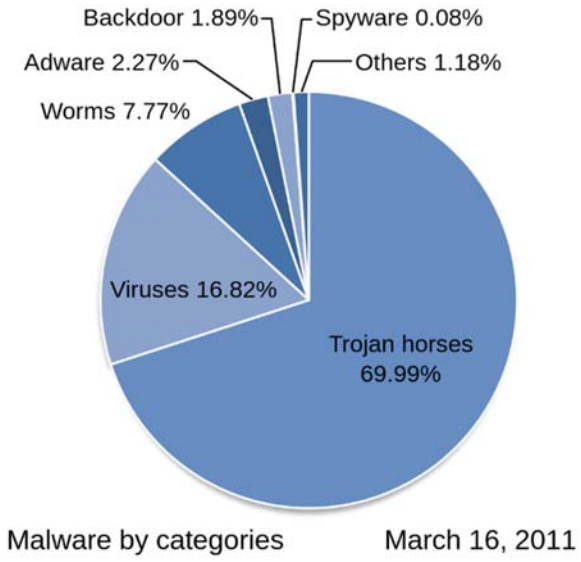
*Tablica 3 - Crvi*

*Izvor: A.Conry-Murray,V.Weafer: Sigurni na Internetu, 2005.*

| **CRVI** | |
|---|---|
| **VRSTA** | **OPIS** |
| **Crv** | Crv je program koji radi i omogućuje distribuciju vlastitih kopija s jednog na drugi disk ili kopira sebe koristeći se e-poštom ili drugim mehanizmima transporta. Može oštetiti i kompromitirati sigurnost računala. |
| **Mailer i mass-mailer crv** | Posebna klasa računalnih crva koji se sami šalju e-poštom. Mass-maileri šalju višestruke vlastite kopije dok maileri rjeđe šalju sami sebe. |
| **Miješane prijetnje** | Kombinacija karakteristika crva, virusa i trojanskih konja s ranjivosti softvera za pokretanje, prijenos i širenje napada. Imaju sposobnost nanošenja štete, razmnožavanja |

| | |
|---|---|
| | različitim metodama, napadanja višestrukih točaka… |

Conry-Murray, Weafer (2005) trojanske konje su definirali kao zlonamjerne programe koji se u sustav uvlače pod okriljem nekog bezopasnog softvera ili datoteke. Izgleda kao istinska aplikacija, ali za razliku od virusa, trojanski konji se ne repliciraju pa trebaju druge metode širenja, najčešće kao payload[4] crva i virusa upakiran u naizgled legitimnu aplikaciju. Do samog širenja dovode: preuzimanje nepoznatih besplatnih ili „cracked" programa, otvaranje privitaka sa neprovjerene e-mail adrese, posjećivanje sumnjivih web stranica…[5] Time otvaraju ulaz na računalu koji pruža zlonamjernim korisnicima / programima pristup računalnom sustavu, omogućavajući krađu povjerljivih i osobnih podataka.




*Slika 4 – Malware po kategorijama*

*Izvor: https://en.wikipedia.org/wiki/Malware#/media/File:Malware_statics_2011-03-16-en.svg*

Prema Conry-Murrayju i Weaferu spyware je pojam za neke tehnologije uhođenja koje se provode na računalu bez primjerenog upozorenja, suglasnosti ili kontrole koje otkrivaju antivirusni programi, a prate aktivnosti na računalu (špijuniranje korisnika). Također navode da je adware – podskup šire kategorije spyware-a – program koji prati online aktivnost i te podatke šalje oglasnoj ili marketinškoj agenciji. Za razliku od virusa, crva i trojanskih konja koji su uvijek nepoželjni, adware i spyware možemo podijeliti u dvije kategorije: visokorizični zlonamjerni programi i niskorizični programi koje svrstavamo tako da se odredi visina rizika, karakteristike instalacije, utjecaj na performanse te jednostavnost uklanjanja.

[4] Payload - opterećenje
[5] https://www.malwarebytes.com/trojan/

Važno je spomenuti DoS[6] napade jer su jako česti u poslovnom svijetu, a „žrtve“ su najčešće serveri organizacija visokog profila kao što su bankarstvo, trgovina i medijske tvrtke ili vladine organizacije. DoS je „vrsta napada na informacijski ili računalni sustav, čiji je cilj jednostavno uskratiti normalno funkcioniranje tog servera ili računala onim korisnicima kojima je taj server namijenjen.“[7] Iako DoS napadi obično ne rezultiraju krađom ili gubitkom značajnih podataka ili druge imovine, žrtvu mogu koštati puno vremena i novca.

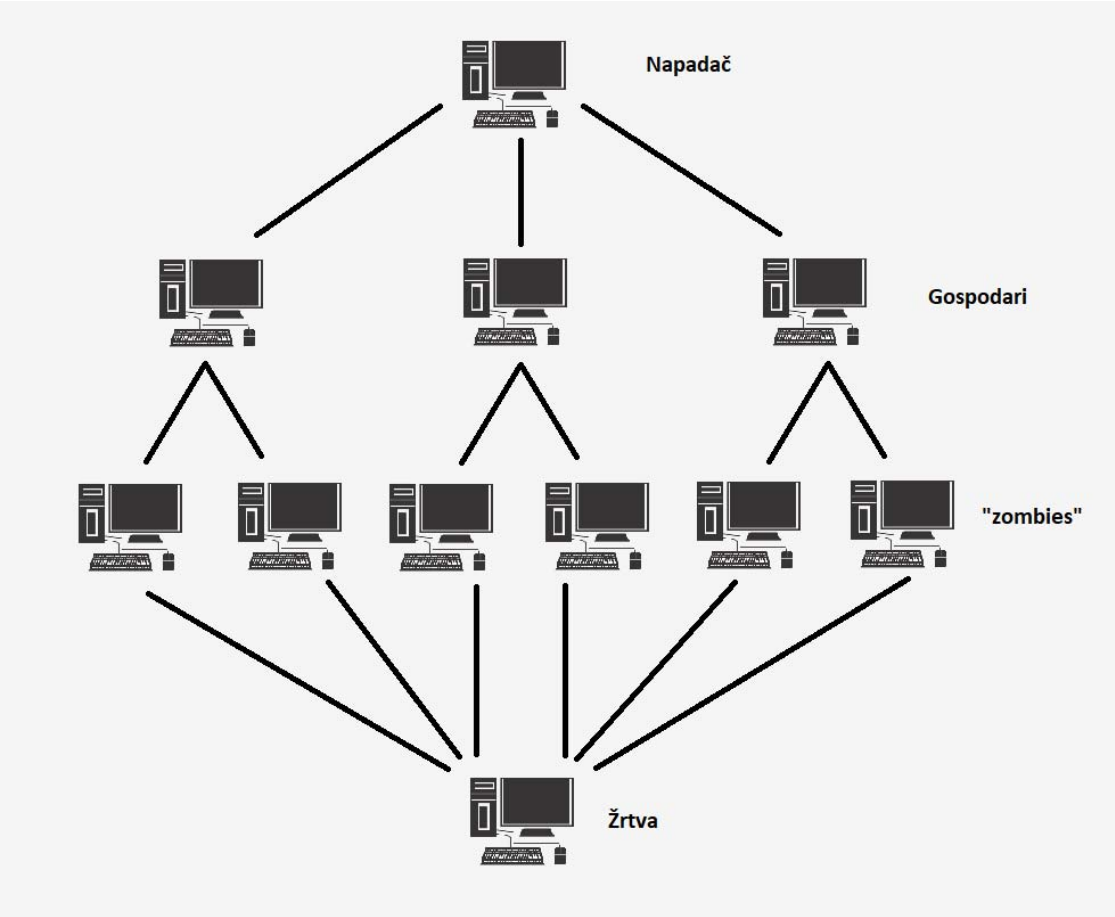
Budući da se temelje na velikoj količini podataka kojima se preplavljuje žrtva, DoS napadi se najčešće izvode kao DDoS[8] napadi. Za njihovo izvođenje potreban je velik broj računala koji sinkronizirano izvršavaju napad pod komandom napadača, a povećavanjem broja botneta[9], napadač povećava uspješnost napada. U nastavku je opisano izvođenje DDoS napada.[10]

DDoS napadi provode se s mrežama računala povezanih s Internetom. Te se mreže sastoje od računala i drugih uređaja koji su zaraženi zlonamjernim softverom, što omogućuje napadaču daljinsko upravljanje. Jednom kada je botnet uspostavljen, napadač može usmjeriti napad slanjem udaljenih uputa svakom botu, ali napadač najčešće komunicira samo sa bot masterima[11] koji kontroliraju napadačke sustave tzv. „zombije“. Kada napadač pošalje naredbu gospodarima, oni prosljeđuju adresu mete svojim botovima te napad s više strana može početi.

Slijedom navedenog, možemo primijetiti da razliku između DoS i DDoS napada čini količina napadača te je zbog veće uspješnosti u provedbi napada češći DDoS.

Suvremene sigurnosne tehnologije razvile su mehanizme za obranu od većinu oblika DoS napada, ali zbog jedinstvenih karakteristika, DDoS se i dalje smatra povišenom prijetnjom i više zabrinjava organizacije koje se boje da će biti meta takvog napada.

[6] DoS – Denial of Service/uskraćivanje usluge
[7] Napadi uskraćivanjem usluge. Nacionalni CERT
[8] DDoS – Distributed Denial of Service
[9] Botnet – broj uređaja povezanih s Internetom, od kojih svaki ima jednog ili više botova (Internet bot, web robot, robot ili jednostavno bot – softverska aplikacija koja pokreće automatizirane zadatke putem Interneta). Botneti se mogu koristiti za izvršavanje napada distribuiranog uskraćivanja usluge (DDoS), krađu podataka, slanje neželjene pošte i omogućuje napadaču pristup uređaju i njegovoj vezi. (Wikipedia)
[10] https://www.cis.hr/WikiIS/doku.php?id=dos_attacks
[11] Bot master/herder – gospodar; hakeri koji koriste automatizirane tehnike za skeniranje određenih dometa mreže i pronalazak ranjivih sustava, poput strojeva bez trenutnih sigurnosnih zakrpa, na koje mogu instalirati svoj bot program. Zaraženi stroj tada je postao jedan od mnogih zombija u botnetu i reagira na naredbe gospodara. (Wikipedia)




*Slika 5 - DDoS napad*

*Izvor: Rad autora prema https://www.cis.hr/WikiIS/doku.php?id=dos_attacks*

## 5.2. Kibernetičko ratovanje

Pojavom računala, a potom i mreža koje su ih povezivale, otvorile su se nove metode ratovanja. Računala ne samo da prate i navode konvencionalna vojna oružja, već su i sami računalni sustavi postali oružje. Kroz vrijeme su računala napredovala, a zajedno s tehnološkim napretkom, rastao je i obujam *cyber* kriminaliteta. Prva generacija zlonamjernog softvera u 1970-ima bila je uglavnom eksperimentalna i nije nanijela veliku štetu osim što je koristila RAM[12] i gnjavila svoje žrtve. S vremenom su računala postala manja i jeftinija (i dalje izuzetno skuplja nego danas) te su se počela koristiti u privatne svrhe odnosno za kućnu upotrebu te je 1980-ih *malware* evoluirao. Pojavili su se virusi, crvi i drugi zlonamjerni oblici softvera koji su šireći se Internetom uništavali

[12] RAM – Random Access Memory – memorija s nasumičnim pristupom; oblik primarne računalne memorije čijem se sadržaju može izravno pristupiti

podatke i preopterećivali sustave. Vrhunac napada u 80-ima uzrokovao je prvi *cyber* napad velikih razmjera – Crv Morris, koji je zaustavio deset posto Interneta[13], te prema svojem tvorcu nije bio napisan da prouzroči štetu, već da ukaže na mane i propuste zaštite u sustavu. Kritična pogreška koja je crva pretvorila iz bezazlene intelektualne vježbe u virtualni napad uskraćivanja usluge bila je u mehanizmu širenja. Crv je mogao utvrditi hoće li napasti novo računalo pitajući postoji li već pokrenuta kopija te je Morris uputio crva da se sam replicira i ako je jednom od sedam puta odgovor da već postoji kopija. Ta se razina kopiranja pokazala pretjeranom, a crv se brzo širio, više puta zarazivši neka računala. (Wikipedia, Morris Worm)

Od naglašavanja rizika za računalne sustave od strane Nacionalnog istraživačkog centra (*National Research Council*) prošlo je 20 godina. Od tada je paralelno s računalnim mrežama rastao i broj i složenost *cyber* napada. Cijela infrastruktura gospodarstva, financije, poslovi Vlade, a tako i vojna i nacionalna sigurnost počela je sa informatizacijom poslovnih procesa i spajanjem svojih sustava na mrežu, otvarajući tako vrata novom bojištu u modernom ratu. Iako su cyber napadi još uvijek u razvoju, mogućnosti napada su nebrojene.

Po definiciji iz Oxford dictionary-ja *cyberwar* ili kibernetičko ratovanje je korištenje računalne tehnologije za ometanje aktivnosti države ili organizacije, posebno za namjerno napadanje informacijskih sustava u strateške ili vojne svrhe, što jednostavnije možemo definirati kao vojni sukob između država u virtualnom prostoru koji se provodi pomoću informacijske tehnologije, no nakon čitanja raznih literatura, internetskih članaka i definicija, *cyberwar* po svrsi možemo podijeliti na:

- *cyber* napad – destruktivan učinak, oštećenje sustava
- *cyber* eksploataciju – nedestruktivna, pribavljanje povjerljivih podataka bez znanja korisnika

Evolucijom iz tradicionalnog u *cyber* oružje, počinitelji su se sve više udaljavali od pravnih posljedica. U tom pogledu sa *cyber* prostorom trebalo bi se postupati kao s bilo kojim drugim poprištem sukoba bez obzira na njegovo mjesto. Jedini međunarodni sporazum koji se približava definiranju kibernetičkih napada je Konvencija o kibernetičkom kriminalu[14] no ona nije široko prihvaćena pa nije ni obvezujuća kao međunarodno pravo. Cilj Konvencije je uskladiti domaće kaznene zakone država potpisnica, usvojiti odgovarajuće zakonodavstvo za kriminaliziranje unutar Konvencije pobrojanih cyber kaznenih djela. Odredbe o interferenciji podataka i interferenciji sustava najvažnije su za cyber napade. Konvencija zahtijeva da potpisnici usvoje zakone koji kriminaliziraju "oštećenje, brisanje, pogoršanje, izmjenu ili potiskivanje računalnih podataka bez prava“ kao i „ozbiljno bespravno ometanje funkcioniranja računalnog sustava unosom, prijenosom,

[13] The History Of Computer Viruses, http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml

[14] Convention on Cybercrime – multilateralni ugovor koji je povećao suradnju među potpisnicima u borbi protiv kibernetičkih kriminala poput prijevare, dječje pornografije i kršenja autorskih prava

oštećivanjem, brisanjem, pogoršanjem, mijenjanjem ili potiskivanjem računalnih podataka“ (Vijeće Europe, 2001).

S druge strane, *cyber* eksploatacija odnosi se „na upotrebu radnji i operacija - možda tijekom duljeg vremenskog razdoblja - za dobivanje podataka koji bi se inače držali povjerljivima i koji se nalaze na računalu ili protivničkom računalnom sustavu ili mreži“ (Lin, 2010). *Cyber* špijunažu je Wilson 2009. definirao kao „neovlašteno ispitivanje konfiguracije ciljnog računala za procjenu obrane sustava ili neovlašteno pregledavanje i kopiranje podatkovnih datoteka“. Špijunaža je jeftin i niskorizičan alat za državne vlade. Iste tehnike koje *cyber* kriminalci koriste za dobivanje povjerljivih podataka - zlonamjerni softver, krađa identiteta, virusi i drugi - državne vlade sposobne su koristiti i za obavještajnu i za komercijalnu špijunažu.

Kako bi postigli svoje ciljeve, cyber napadači kombiniraju i metode napada i metode eksploatacije. Na primjer, *cyber* napadač bi mogao otkriti koju vrstu sigurnosnog sustava koristi protivnička država putem *cyber* eksploatacije. Kada dobiju uvid u sigurnosni sustav, lako mogu osmisliti kibernetički napad koji će poremetiti taj sustav tako da se šteta može napraviti bez znanja žrtve.

Upravo zbog toga možemo reći da je *cyber* ratovanje budućnost ratovanja, a „informacijski rat je u svom najtemeljnijem smislu kazalište u nastajanju u kojem će se najvjerojatnije dogoditi budući sukob nacije protiv nacije na strateškoj razini“ (George J. Stein, Cyber War, 2020).

### 5.3. Kibernetički terorizam

Kako navodi Institut mira Sjedinjenih Država, *cyber* terorizam je „konvergencija internetskog prostora i terorizma, odnosi se na nezakonite napade i prijetnje napadima na računala, mreže i na njima pohranjene podatke zbog zastrašivanja vlade ili njezinog naroda, a u svrhu postizanja političkih ili društvenih ciljeva.“

Sjevernoatlantski ugovor (NATO) ponudio je vlastitu definiciju 2008. NATO je definirao cyber terorizam kao „cyber napad koji koristi ili koristi računalo ili komunikacijske mreže kako bi prouzročio dovoljno razaranja ili poremećaja kako bi stvorio strah ili zastrašio društvo u ideološkom cilju . "

Cyber terorizam kontroverzan je pojam. Neki autori odabiru vrlo usku definiciju, koja se odnosi na raspoređivanje, od strane poznatih terorističkih organizacija, napada ometanja informacijskih sustava s primarnom svrhom stvaranja alarma i panike. Prema ovoj uskoj definiciji teško je identificirati slučajeve cyber terorizma, no ukratko se na *cyber* terorizam vjerojatno najbolje gleda kao na operativnu taktiku usmjerenu na različit psihološki ishod, a ne kao na polje istraživanja koje cyber domenu u hipu povezuje s terorizmom u stvarnom prostoru. Važno je istaknuti, iako su istraživanja i politika *cyber* terorizma posljednjih godina donekle stali, iskorištavanje taktičkih pristupa za stvaranje terora u i kroz *cyber* prostor tek je na početku.

# 6. PRAVNA REGULACIJA U HRVATSKOJ

## *6.1. Nacionalna strategija kibernetičke sigurnosti*

*Nacionalna strategija kibernetičke sigurnosti* navodi „kako bi aktivnosti svih segmenata društva bile u sigurnom kibernetičkom prostoru, za osiguranje potrebne razine sigurnosti podataka pohranjenih u takvim registrima nužno je korištenje zajedničke osnovice za sigurnu razmjenu podataka unutar sustava državne informacijske infrastrukture, zajedničkog sustava identifikacije i autentifikacije.“[15] Zbog toga je uspostavljen *Nacionalni idenifikacijski i autentifikacijski sustav*.

*Nacionalni identifikacijski i autentifikacijski sustav* (u daljnjem tekstu: NIAS) „omogućuje sigurnu identifikaciju i autentifikaciju korisnika elektroničkih usluga“ čije su osnovne funkcije pružanje jedinstvenog elektroničkog identiteta prilikom pristupa i korištenja elektroničkih usluga, olakšavanje izdavanja vjerodajnica za e-identifikaciju te njihovu širu uporabu u uslugama povezanih sa NIAS sustavom.[16]

Usvojena strategija podiže svijest o sigurnosti svih korisnika internetskog prostora, te nastoji uspostaviti učinkovitiji mehanizam za razmjenu i pristup podacima u sigurnom okruženju.

## 6.2. E-identitet

Kako bi se osigurale potrebne razine sigurnosti podataka nužno je korištenje zajedničkog sustava autentifikacije i identifikacije da bi se spriječio računalni, odnosno kibernetički kriminalitet. Identifikacija (obavještavanje sustava tko smo) i provjera autentičnosti (dokaz identiteta) su osnova modernih sigurnosnih alata te „brane“ sigurnost kibernetičkog prostora. Zbog toga je uspostavljen središnji sustav autentifikacije i autorizacije – e-identitet – kako bi se jasno i pravno dodijelilo ovlaštenje djelovanja i korištenje resursa u *cyber* prostoru.

Ministarstvo uprave e-Hrvatska e-identitet definira kao jedinstveni skup podataka identifikacije o osobi ili računalnom sustavu u digitalnom obliku kroz koji je s potpunom sigurnošću moguće utvrditi identitet subjekta za koje subjekt tvrdi da mu pripada.

NIAS je podignut u računalno-komunikacijskoj mreži javnopravnih tijela HITRONet[17] - najvećoj državnoj računalnoj mreži koja povezuje sva ministarstva, Sabor, Ured predsjednika, Mirovinski zavod, HZZO, POA-u, pa čak i 144 suda te Agenciju za tržišno natjecanje i Hanfu.

[15] Nacionalna strategija kibernetičke sigurnosti, listopad 2015. (NN108/2015)
[16] Ministarstvo uprave e-Hrvatska: Program razvoja elektroničkih usluga, rujan 2013.
[17] HITRONet - računalno komunikacijska mreža tijela državne uprave u koju su spojene sve središnje lokacije središnjih tijela državne uprave (Nacionalna strategija kibernetičke sigurnosti, listopad 2015. (NN108/2015))

## 6.3. Kaznenopravna reforma

U Republici Hrvatskoj zakon o *cyber* kriminalitetu je teško provesti u djelo upravo zbog karakteristike ne posjedovanja fizičkih dokaza o napad odnosno provedenom zločinu. No ukoliko se počinjeni *cyber* zločin ipak uspije dokazati propisane kazne su u skladu sa ostalim konvencionalnim kriminalnim činovima[18].

Kako je navedeno u Kaznenom Zakonu Republike Hrvatske, 1997. je kazneno djelo *cybercrime*-a uvedeno pod nazivom „Oštećenje i uporaba tuđih podataka“ te je to prvi put da je *cybercrime* spomenut u Zakonu Republike Hrvatske iako je bio implementiran pod Glavom XVII. „Kaznenih djela protiv imovine“. 2004. godine su u Zakon implementirane odredbe Konvencije o računalnoj povredi privatnosti, krivotvorenju i prijevari.

Tek 2011. je u novom Kaznenom zakonu formirana Glava XXV.: „Kaznena djela protiv računalnih sustava, programa i podataka“ u kojoj su obuhvaćena kaznena djela u nastavku (KZ, 2019:68-71):

- Neovlašteni pristup
- Ometanje računalnog sustava
- Šteta na računalnim podacima
- Neovlašteno presretanje računalnih podataka
- Računalno krivotvorenje
- Računalna prijevara
- Zlouporaba uređaja
- Teška kaznena djela protiv računalnih sustava, programa i podataka[19]

[18] Usp. Vojković, G. Štambuk-Sunjić, M. Konvencija o kibernetičkom kriminalu i kaznenom zakonu Republike Hrvatske. Split: Pravni Fakultet, 2006.,URL: http://www.pravst.unist.hr/dokumenti/zbornik/200681/zb200601_123-136.pdf

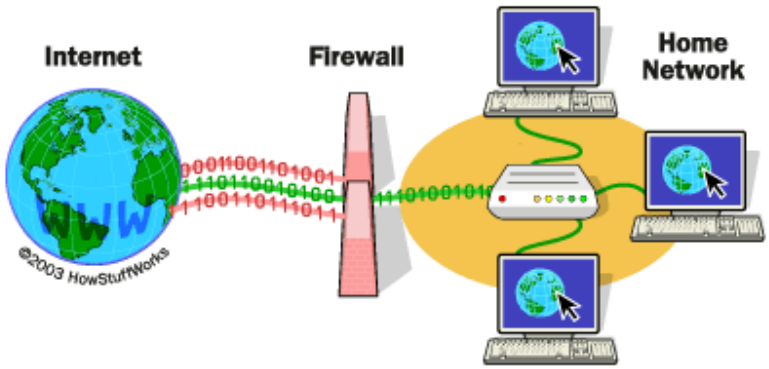
[19] Narodne novine br. 125 07.11.2011 Kazneni zakon: GLAVA DVADESET PETA (XXV.) Kaznena djela protiv računalnih sustava, programa i podataka

# 7. MJERE ZAŠTITE OD *CYBER* KRIMINALITETA

U tehnički vođenom društvu ljudi koriste razne uređaje kako bi život učinili jednostavnijim. Rezultat globalizacije je povezivanje ljudi širom svijeta putem Interneta. Internet povezuje ljude i tvrtke sa suprotnih strana svijeta brzo, lako i relativno ekonomično. Ipak, *cyber* kriminal opasnost je protiv različitih organizacija i ljudi čija su računala povezana s internetom, a posebno s mobilnom tehnologijom. Upravo zbog toga, korisnici računala mogu i trebali bi usvojiti razne tehnike za sprječavanje *cyber* kriminala, a neke od njih opisane su u nastavku.

## 7.1. Vatrozid

Korisnici računala trebali bi koristiti vatrozid kako bi zaštitili svoje računalo od hakera. Većina sigurnosnog softvera dolazi s vatrozidom. Prema Wikipediji, „vatrozid je mrežni sigurnosni sustav koji nadzire i kontrolira dolazni i odlazni mrežni promet na temelju unaprijed određenih sigurnosnih pravila i obično uspostavlja prepreku između pouzdane i nepouzdane mreže, poput Interneta“. Vatrozidi pažljivo analiziraju dolazni promet na temelju unaprijed utvrđenih pravila i filtriraju promet koji dolazi iz nesigurnih ili sumnjivih izvora kako bi spriječili napade. Vatrozidi čuvaju promet na ulaznoj točki računala (*port*[20]), na kojoj se razmjenjuju informacije s vanjskim uređajima.




*Slika 6 - Funkcija vatrozida*

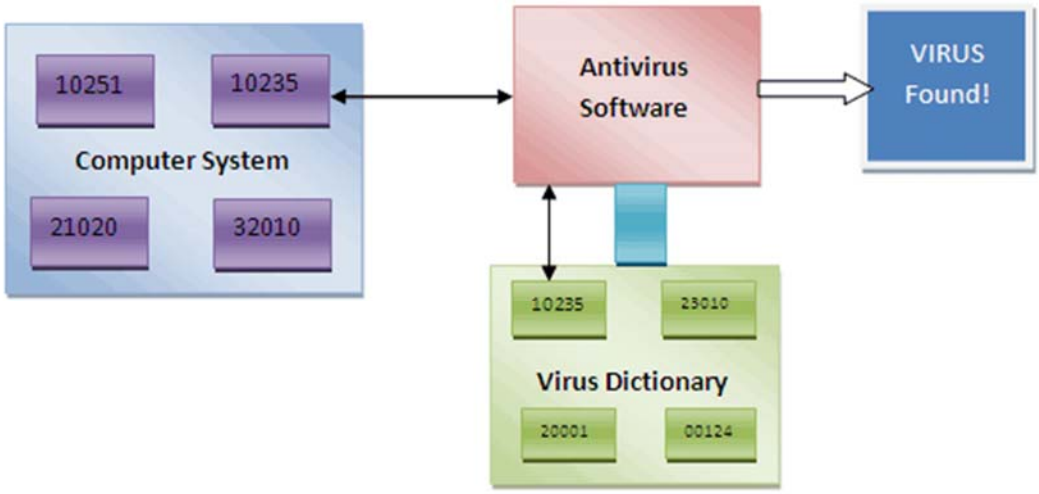
*Izvor: https://www.comodo.com/resources/home/how-firewalls-work.php*

[20] Port – U računalnom umrežavanju port je komunikacijska krajnja točka. Na softverskoj razini, unutar operativnog sustava, port je logična konstrukcija koja identificira određeni proces ili vrstu mrežne usluge. Port se za svaki transportni protokol i kombinaciju adresa identificira 16-bitnim nepotpisanim brojem, poznatim kao broj porta. Najčešći transportni protokoli koji koriste brojeve priključaka su Transmission Control Protocol (TCP) i User Datagram Protocol (UDP).Broj porta uvijek je povezan s IP adresom hosta i vrstom transportnog protokola koji se koristi za komunikaciju. (Wikipedia, pristupljeno 10.09.2020.)

Vatrozidi mogu biti softverski ili hardverski, iako je najbolje imati oboje. Softverski vatrozid je program instaliran na svakom računalu i regulira promet putem brojeva priključaka i aplikacija, dok je fizički vatrozid dio opreme instalirane između vaše mreže i mrežnog prolaza.

## 7.2. Antivirusni softver

Gotovo na svim internetskim izvorima preporuka zaštite od *cyber* kriminaliteta, korisnicima računala preporučuje se da kupe i instaliraju antivirusni softver poput McAfee ili Norton Anti-Virus te da AVG nudi besplatnu antivirusnu zaštitu ako ne žele kupiti softver. „Antivirusni softver ili antivirus je računalni softver koji se koristi za prevenciju, otkrivanje i uklanjanje štetnog softvera“ (Wikipedija, pristupljeno 10.09.2020.).




*Slika 7 - Rad antivirusnog softvera*

*Izvor: https://www.engineersgarage.com/how_to/how-antivirus-works/*

Antivirusni softver koristi razne tehnike za prepoznavanje zlonamjernog softvera, koji se često skriva duboko u operacijskom sustavu. Zbog velike površine napada u današnje vrijeme, antivirusni softver dizajniran je za rješavanje svih vrsta zlonamjernih opterećenja koji dolaze iz pouzdanih i nepouzdanih izvoraod kojih su neki: mrežni paketi, privici e-pošte, izvršni programi koji se izvode na operativnom sustavu i sl. (Koret, Bachaalany, 2015)

## 7.3. Ostale mjere prevencije

Mjere koje Veresha u Preventivnim mjerama protiv računalnog kriminala (2018) navodi biti će nabrojane uz savjete ostalih *cyber* stručnjaka kako bi se podigla svijest o zaštiti podataka u cyber prostoru.

Savjetuje se da se kupovine odvijaju na sigurnim web stranicama te ako ona izgleda sumnjivo ne bi trebali davati podatke o svojoj kreditnoj kartici. Jedna od najčešćih preporuka jest ta da bi korisnici na svojim računima morali razviti jake lozinke koje je teško pogoditi te u njih uključiti i slova i brojeve. Nadalje se savjetuje da se lozinke kontinuirano ažuriraju kao i detalji prijave. Promjenom podataka za prijavu, barem jednom ili dva puta mjesečno, manje su šanse postanka metom *cyber* kriminala.

Također se predlaže praćenje djece i načina na koji koriste Internet te u tu svrhu instaliravanje softvera za roditeljsku kontrolu kako bi se ograničilo gdje mogu surfati. Iznimno je važno provjeriti i profile društvenih mreža koji bi trebali biti postavljeni na „privatno".

*Cyber* kriminal se najčešće veže uz stolno računalo i računalne sustave, no u njega također spadaju i mobiteli i njegovi operativni sustavi. Aktiviranjem ugrađenih sigurnosnih značajki mogu se izbjeći nedopušteni pristupi osobnim podacima, a lozinke, pin brojevi, pa čak ni vlastita adresa ne bi smjeli biti pohranjeni ni na jednom mobilnom uređaju.

Hakiranje se može izbjeći korištenjem šifriranja za najosjetljivije datoteke kao što su porezne prijave ili financijske evidencije i redovitom izradom sigurnosnih kopija svih važnih podataka i njihova pohrana na drugo mjesto.

Korisnici Interneta moraju biti na oprezu dok koriste javne Wi-Fi pristupne točke. Iako su ove pristupne točke prikladne, daleko su od sigurnih. Poželjno je izbjegavati obavljanje financijskih ili korporativnih transakcija na tim mrežama.

Posebno je važna zaštita e-identiteta. Korisnici moraju biti oprezni kada na Internetu daju osobne podatke poput imena, adrese, telefonskog broja ili financijskih podataka.

Sugerira se da korisnici moraju procijeniti i razmisliti prije nego što kliknu na vezu ili datoteku nepoznatog podrijetla, da ne otvaraju nijednu e-poštu u pristigloj pošti prije provjere izvora poruke te da nikada ne odgovaraju na e-adrese koje traže od njih da provjere podatke ili potvrde svoj korisnički ID ili lozinku.

„Potrebno je podići razinu znanja o informacijskoj sigurnosti svih dijelova društva putem kampanja u koje su uključeni i javni mediji, a u školama na satovima razredne zajednice, roditeljskim sastancima, tematskim predavanjima i ostalim izvanškolskim aktivnostima učenike i roditelje osvješćivati o opasnostima unutar informacijskog društva."[21]

*Cyber* je glavni i možda najkompliciraniji problem u cyber domeni. Svjetske vlade, policijske uprave i obavještajne jedinice počele su reagirati protiv cyber kriminala. Na međunarodnoj se razini poduzimaju mnogi napori za suzbijanje prekograničnih cyber prijetnji. No ukoliko se ne pridržavamo barem preporučenih mjera zaštite, rizik nećemo smanjiti, već ćemo gotovo sigurno postati metom *cyber* napada.

[21] Nacionalna strategija kibernetičke sigurnosti, listopad 2015. (NN108/2015)

# 8. ZAKLJUČAK

Pravilna integracija tehnologije u poslovanju i privatnom životu može pružiti kvalitetnije i učinkovitije pružanje i korištenje usluga te olakšanje dnevnih procesa, no neki pojedinci te sustave iskorištavaju u svrhu ostvarenja osobnih ciljeva te to najčešće čine koristeći zloćudne programe i na nelegalni način.

Prije nego što su postojali digitalni podaci, svijet je imao samo fizičke prijetnje. Međutim, pojava interneta i globalne mreže stvara računalni i informacijski kriminalitet svugdje.

*Cybercrime* je kriminalna radnja koja se vrši pomoću računala i Interneta te uključuje sve, od preuzimanja ilegalnih datoteka do krađe milijuna dolara s mrežnih bankovnih računa. *Cyber* kriminal također uključuje nemonetarna kaznena djela, poput stvaranja i distribucije virusa na drugim računalima, pornografije, uhođenja ili objavljivanja povjerljivih podataka na Internetu.

Budući da kibernetički kriminal obuhvaća tako širok opseg kriminalnih radnji, primjeri u ovom radu su samo neki od tisuću kaznenih djela koja se smatraju cyber kriminalom. Iako su nam računala i Internet na mnogo načina olakšali život, žalosno je što ljudi također koriste ove tehnologije kako bi iskoristili prednosti drugih. Upravo zbog virtualnog odvijanja računalnog kriminaliteta i nedostatka fizičkih dokaza počinjenog zločina, potrebno je educirati korisnike računalnih tehnologija kako na vrijeme prepoznati i, ukoliko je moguće, na vrijeme otkloniti prijetnje.

*Cyber* kriminal previše je jednostavan za napraviti. Mnogi korisnici tehnologije ne provode najosnovnije mjere zaštite. Mnoge tvrtke razmišljaju samo o svom ekonomskom prometu, a da nemaju odgovarajuće obrambene proizvode, dok cyber kriminalci koriste sofisticiranu i izravnu tehnologiju za prepoznavanje ciljeva, distribuciju zlonamjernih softvera i lako unovčavanje onoga što ukradu.

Računala dodaju novu dimenziju kaznenom zakonu, iznoseći mnoga pitanja za provođenje zakona. Tehnička usavršenost potrebna da bi se slijedio "elektronički trag" daleko nadilazi tradicionalne metode istrage. Jednako su izazovna i politika i pravna pitanja. Potrebno je donijeti zakone koje će u dovoljnoj mjeri zabraniti zlouporabe nove tehnologije i tehnologije u razvoju. Internet također predstavlja zabrinutost za nacionalnu sigurnost jer računala imaju ključnu ulogu u pružanju hitnih službi, vladinim operacijama, bankarstvu, prijevozu, energiji i telekomunikacijama. Kako se tehnologija razvija, zakon mora odgovarati na ova nova zbivanja kako bi odvratio one koji bi zloupotrijebili i zloupotrijebili novu tehnologiju.

Možemo reći da je računalni kriminalitet možda najopasniji kriminalitet jer je sam „protivnik“ imaginaran, nevidljiv i nepredvidljiv. Upravo zato treba ulagati u obranu od njega, ali i na edukaciju

o njemu jer ako se podigne svijest o sigurnosti u kibernetičkom prostoru, možda će suzbijanje računalnog kriminaliteta postati mnogo lakše, a same usluge u kibernetičkom svijetu pouzdanije.

U zaključku ovog rada, ono što će računalni i cyber kriminal postati u budućnosti nije predvidljivo. Ono što se događalo prije nije ono što će se događati u budućnosti, jer računalni svijet svakodnevno napreduje te jedino što možemo poduzeti je na vrijeme se educirati i pokušati koristiti digitalne tehnologije za ono za što su u suštini i namijenjene – lakšu povezanost i jednostavniji život.

# 9. IZJAVA

**Izjava o autorstvu završnog rada i akademskoj čestitosti**

**Ime i prezime studenta: Kristina Jakolić**

**Matični broj studenta: 6-121/17 ITI**

**Naslov rada: INFORMACIJSKI KRIMINALITET**

Svojim potpisom jamčim:

- Da sam jedini autor ovog rada.
- Da su svi korišteni izvori, kako objavljeni, tako i neobjavljeni, adekvatno citirani i parafrazirani te popisani u bibliografiji na kraju rada.
- Da ovaj rad ne sadrži dijelove radova predanih na Veleučilište Baltazar Zaprešić ili drugim obrazovnim ustanovama.
- Da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio nastavnik.

Potpis studenta

K. Jakolić

# 10. POPIS LITERATURE

Varga M.: Upravljanje podacima, 2014.

L. Whitten, J.; D. Bentley, L.: Systems Analysis and Design Methods, McGraw-Hill/Irwin, USA, 2007., preuzeto s https://www.academia.edu/8787830/Whitten_and_Bentley_2007_System_Analysis_and_Design_Methods_7th_Edition / Pristupljeno 07.09.2020

Varga, M.: Baze podataka –Konceptualno, logičko i fizičko modeliranje podataka, Društvo za razvoj informacijske pismenosti, Zagreb, 1994

Srića, V., Spremić, M.: Informacijskom tehnologijom do uspjeha, Sinergija, Zagreb, 2000.

Moore, R.: Cyber crime: Investigating High-Technology Computer Crime, 2005.

Moise, A.C.: Some considerations on the phenomenon of *cybercrime*. Journal of Advanced Research in Law and Economics, 2014., str 38-43

B.H.Schell, C. Martin: *Cybercrime*: A Reference Handbook (2004)

M. Yar: *Cybercrime* and Society, 2006.

Conry-Murray, A., Weafer, V.: Sigurni na Internetu, 2005.

Chawki, M.: A critical look at the regulation of cybercrime (2005), preuzeto s http://www.crime-research.org/articles/Critical / Pristupljeno 28.08.2020.

Napadi uskraćivanjem usluge NCERT-PUBDOC-2011-01-321, preuzeto s https://www.cert.hr/napadi-uskracivanjem-usluge/ / Pristupljeno 28.08.2020.

Povijest računalnih virusa, preuzeto s https://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml / / Pristupljeno 07.09.2020.

Morris worm, https://en.wikipedia.org/wiki/Morris_worm / Pristupljeno 07.09.2020

Vijeće Europe, Konvencija o kibernetičkom kriminalitetu, članak 5. i članak 6., preuzeto s https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000001680081561 / Pristupljeno 07.09.2020.

Lin, H. – Offensive Cyber Operations and the Use of Force, preuzeto s https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf / Pristupljeno 07.09.2020.

Kramer, F., Starr, S., Wentz, L., Wilson, C.: Cyberpower and National Security (2009), Chapter 18: Cybercrime, preuzeto s https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/ / Pristupljeno 07.09.2020.

Koret, J., Bachaalany, E.: The Antivirus Hacker's Handbook (2015), preuzeto s https://repo.zenk-security.com/Magazine%20E-book/Antivirus%20hackers%20handbook.pdf / Pristupljeno 10.09.2020.

# 11. POPIS SLIKA, TABLICA I GRAFIKONA

**Popis slika**



**Popis tablica**

# 12. ŽIVOTOPIS

**OSOBNE INFORMACIJE** Jakolić Kristina

Dubravička ulica 153, Kraj Donji, 10299 Marija Gorica (Hrvatska)
0995157931
kristina.jakolic@gmail.com

Spol Žensko | Datum rođenja 13. rujna 1996. | Državljanstvo hrvatsko

**RADNO ISKUSTVO**

**17. lipnja 2019.–danas** Administrativni asistent / administrativna asistentica
AT BAS d.o.o., Zagreb (Hrvatska)
Izrada ponuda i obračuna
Fakturiranje
Dokumentacija podataka

**siječanj 2017.–16. lipnja 2019.**
Piacanis d.o.o., Zaprešić (Hrvatska)

**lipanj 2016.–siječanj 2017.**
Ferretti, Zaprešić (Hrvatska)

**OBRAZOVANJE I OSPOSOBLJAVANJE**

**rujan 2017.–danas** Informacijske tehnologije
Veleučilište s pravom javnosti Baltazar, Zaprešić (Hrvatska)

**rujan 2011.–lipanj 2015.** Opća gimnazija
Srednja škola Ban Josip Jelačić, Zaprešić (Hrvatska)

**OSOBNE VJEŠTINE**

**Materinski jezik** hrvatski

**Strani jezici**

| | RAZUMIJEVANJE | | GOVOR | | PISANJE |
|---|---|---|---|---|---|
| | Slušanje | Čitanje | Govorna interakcija | Govorna produkcija | |
| engleski | C1 | C1 | C1 | C1 | |
| | C1 njemački | B1 | B1 | A2 | |
| | A2 | A2 | | | |

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik
Zajednički europski referentni okvir za jezike

**Komunikacijske vještine**

Pristupačna sam i druželjubiva osoba, uvijek otvorena za razgovore i diskusije različitih tema.

Vodim brigu o suradnicima te nastojim uvažiti tuđa mišljenja i postići kompromis. Bitno mi je da su kolege međusobno složni i zadovoljni.

**Organizacijske / rukovoditeljske vještine**

- Izrada rasporeda (planova) radnog vremena i slobodnih dana
- Inventura
- Naručivanje robe i materijala
- Izvedba manjih zadataka iz područja računovodstva i financija - Izrada ponuda i obračuna, slanje i unos računa

**Poslovne vještine**

U firmi Piacanis bila sam zaposlena kao prodavač. Nakon određenog vremena prebačena sam kod istog poslodavca na stalnu poziciju u caffe bar, a po potrebi sam radila i kao zamjena u fast food restoranu iste tvrtke.

Na trenutnom radnom mjestu u administraciji započela sam sa dokumentacijom podataka i izradom ponuda i obračuna. Trudom i kontinuiranim poboljšanjem prepustio mi se posao fakturiranja, vođenja računa o naplatama te mi se povjeruju sitni knjigovodstveni poslovi.

Dobrom prioretizacijom uspijevam kvalitetno obaviti sve radne zadatke, a nastojim unaprijed riješiti sve dodatne izazove koje uočim.

Kao radniku izrazito mi je bitno da moj trud i zalaganje budu zamijećeni, te da o obavljenom poslu dobivam povratne informacije, kako bi svoj profesionalni razvoj mogla podići na višu razinu te time postati bolja i efikasnija u poslovnom svijetu.

**Digitalne vještine**

SAMOPROCJENA

| Obrada informacija | Komunikacija | Stvaranje sadržaja | Sigurnost | Rješavanje problema |
|---|---|---|---|---|
| Iskusni korisnik | Iskusni korisnik | Samostalni korisnik | Samostalni korisnik | Samostalni korisnik |

Digitalne vještine - Tablica za samoprocjenu

- Dobro poznavanje MS Office alata
- U toku s trenutnom tehnologijom
- Konstantno usavršavanje informacijskih vještina studiranjem na veleučilištu te samostalno u slobodno vrijeme

**Vozačka dozvola**

B