Računalni kriminal i njegov utjecaj na ekonomsko poslovanje u 21. stoljeću

Strabić, Dalibor

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **The University of Applied Sciences Baltazar Zaprešić / Veleučilište s pravom javnosti Baltazar Zaprešić**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:129:871262

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Digital Repository of the University of Applied Sciences Baltazar Zaprešić - The aim of Digital Repository is to collect and publish diploma works, dissertations, scientific and professional publications





VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Poslovanje i upravljanje

DALIBOR STRABIĆ

RAČUNALNI KRIMINAL I NJEGOV UTJECAJ NA EKONOMSKO POSLOVANJE U 21. STOLJEĆU

STRUČNI ZAVRŠNI RAD

Zaprešić, 2020. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Poslovanje i upravljanje

STRUČNI ZAVRŠNI RAD

RAČUNALNI KRIMINAL I NJEGOV UTJECAJ NA EKONOMSKO POSLOVANJE U 21. STOLJEĆU

Mentor:
dr. sc. Dafne Vidanec, v. pred.

JMBAG studenta:
0303027534

Naziv kolegija:
Poslovna etika

Student:
Dalibor Strabić

SADRŽAJ

SAŽETAK 1
ABSTRACT 2
1. UVOD 3
2. RAČUNALNI KRIMINAL – KONCEPTUALNI OKVIR I TEORIJSKE ODREDNICE 5
2.1. Teorijske determinante računalnog kriminala 5
2.2. Metode i tipologija računalnog kriminala 9
2.2.1. Hakerski napadi 12
2.2.2. Računalne prevare 16
2.2.3. Kršenje online autorskih prava i računalno nasilje 18
2.3. Prevencija računalnog kriminala 19
3. RAČUNALNI KRIMINAL I POSLOVNA ETIKA 22
3.1. Teorijske odrednice poslovne etike 22
3.2. Primjena etike u poslovanju 27
3.3. Moralno stajalište poslovne etike prema računalnom kriminalu 29
4. RAČUNALNI KRIMINAL I UTJECAJ NA POSLOVANJE 32
4.1. Metode utjecaja na suvremeno poslovanje 32
4.2. WikiLeaks – organizacija računalnog kriminala 34
4.3. Hakerski napadi na svjetske burze i financijske institucije 37
5. ZAKLJUČAK 38
LITERATURA 40
POPIS SLIKA 43
IZJAVA 44
ŽIVOTOPIS 45

SAŽETAK

Danas na Internetu postoje brojni računalni kriminalci koji svjesno i ciljano napadaju fizičke i pravne osobe sa ciljem krađe osobnih podataka, autorskih prava, fotografija i drugih podataka koje potom zloupotrebljavaju, gdje dolazi do velike opasnosti od strane računalnih terorista za poduzeća i njihov opstanak. Računalni kriminal i njegovi sudionici danas su razvijeni s namjerom da šire i primjenjuju računalni terorizam nad žrtvama koje koriste Internet, a njihov su primarni cilj velike korporacije, financijske institucije, vladine institucije i organizacije od svjetskog značaja jer posjeduju veoma značajne informacije, kao i veliku količinu novčanih sredstava, gdje se učinkovitim metodama računalnog kriminala može doći do istih i time ozbiljno ugroziti poslovanje i opstanak i javnih i privatnih institucija.

Cilj rada je prikazati konceptualni okvir računalnog kriminala sa njegovim metodama implementacije u poslovanju, prikazati stajalište poslovne etike prema računalnom kriminalu te metode utjecaja računalnog kriminala na suvremeno poslovanje sa apliaktivnim primjerima WikiLeaksa i organiziranog napada poznatih svjetskih hackera na svjetske financijske institucije i burze. Svrha je rada spoznati važnost opasnosti računalnog kriminala za suvremeno poslovanje, ali i iznaći način kako se od istoga učinkovito zaštititi.

Ključne riječi: računalni kriminal, poslovanje, ekonomija, hacker, poslovna etika

ABSTRACT

Today, there are numerous computer criminals on the Internet who knowingly and taretly attack individuals and legal entities with a goal to stole personal data, copyrights, photographs and other data that are then misused, and where there is a great danger from other computer terrorists in companies and their opponents. Cybercrime and its stakeholders have developed an intent to crack down on and apply cyber terrorism to victims of the Internet, and their private target are large corporations, financial institutions, government institutions and world-class organizations, as they visit very important data as well as large amounts of money, where using the methods of computer crime can occur the same and time to seriously impair the business and survival of both public and private institutions.

The aim of the paper is to present the conceptual framework of cybercrime with its methods of implementation in business, the attitude of business ethics towards cybercrime and the methods of influencing cybercrime on modern work using the example of WikiLeaks and organized attacks by world hackers on financial institutions and stock exchanges. The purpose of the paper was to understand the important dangers of computer crime for modern business, but also to find a way to get out of the same protective place.

Keywords: computer crime, business, economics, hacker, business ethics

1. UVOD

Internet je u 21. stoljeću postao toliko važan dio života svakog čovjeka, kako u privatnom, tako i u poslovnom životu, da je bez njega danas poslovni i privatni smisao izgubio na važnosti. Danas mnogobrojni ljudi i poduzeća koriste Internet sa potpunom sviješću o njegovoj korisnosti u poslovanju i napretku koji pruža online poslovanje. Međutim, isti ne posjeduju dovoljno informacija o potencijalnim ugrozama koje im korištenje Interneta može donijeti te kako isti može posredno ili neposredno utjecati na njihovu privatnost, podatke koje posjeduju, a od važnosti su za poslovanje tvrtki.

Danas na Internetu postoje brojni računalni kriminalci koji svjesno i ciljano napadaju fizičke i pravne osobe sa ciljem krađe osobnih podataka, autorskih prava, fotografija i drugih podataka koje potom zloupotrebljavaju, gdje dolazi do velike opasnosti od strane računalnih terorista za poduzeća i njihov opstanak. Računalni kriminal i njegovi sudionici danas su razvijeni s namjerom da šire i primjenjuju računalni terorizam nad žrtvama koje koriste Internet, a njihov su primarni cilj velike korporacije, financijske institucije, vladine institucije i organizacije od svjetskog značaja jer posjeduju veoma značajne informacije, kao i veliku količinu novčanih sredstava, gdje se učinkovitim metodama računalnog kriminala može doći do istih i time ozbiljno ugroziti poslovanje i opstanak i javnih i privatnih institucija. Takvi računalni kriminalci se služe Internetom u pripremi i provedbi napada na tvrtke i javne institucije, gdje im Internet služi kao primarna platforma njihova računalnog kriminalnog čina.

Borba protiv računalnog kriminala, kako u poslovanju, tako i u drugim domenama, regulirana je zakonskim aktima te se javlja u obliku pravno formalne i informatičke naravi. Pravni akti su danas dobro regulirani, međutim, njihova provedba je dugotrajna i implementira se kad je šteta već nanesena. Instrumenti informatičke naravi protiv računalnog kriminala u poslovanju su vrlo učinkoviti, a javljaju se u vidu postojanja zaštitnih programa od virusa, statusa provjere identiteta, posjedovanja zaštitnih lozinki i slično.

Predmet istraživanja ovog završnog rada je računalni kriminal u poslovanju 21. stoljeća te prikaz načina na koji dolazi do ugroza i posljedica poslovanja, primarno sa stajališta poslovne etike.

Cilj rada je prikazati konceptualni okvir računalnog kriminala sa njegovim metodama implementacije u poslovanju, prikazati stajalište poslovne etike prema računalnom kriminalu

te metode utjecaja računalnog kriminala na suvremeno poslovanje sa apliaktivnim primjerima WikiLeaksa i organiziranog napada poznatih svjetskih hackera na svjetske financijske institucije i burze. Svrha je rada spoznati važnost opasnosti računalnog kriminala za suvremeno poslovanje, ali i iznaći način kako se od istoga učinkovito zaštititi.

Struktura rada sačinjena je od pet međusobno povezanih cjelina. U prvom poglavlju data je uvodna riječ problematike teme, prikazan je predmet, svrha i cilj istraživanja, struktura rada te znanstvene metode. U drugom dijelu prikazan je konceptualni okvir računalnog kriminala sa teorijskim odrednicama i metodama računalnih napada, kao i prevencija računalnog kriminala. U trećem dijelu dat je opis poslovne etike i njezina primjena u poslovanju, kao i njezino moralno stajalište prema računalnom kriminalu. U četvrtom poglavlju opisane su metode utjecaja računalnog kriminala na suvremeno poslovanje, prikazani su aplikativni primjeri računalnog kriminala na primjeru WikiLeaksa i napada svjetskih hackera na svjetske burze i financijske institucije sa posljedicama. U zaključku su date završne misli autora teme o istraženoj problematici koje predstavljaju znanstveni doprinos istraženoj temi.

U znanstvenom istraživanju, formuliranju i prezentiranju rezultata istraživanja u ovom završnom radu koristit će se u odgovarajućim kombinacijama brojne znanstvene metode, a od kojih se navode one najvažnije: metoda analize i sinteze, induktivna i deduktivna metoda, komparativna metoda, metoda apstrakcije i konkretizacije, metode specijalizacije i generalizacije, metoda klasifikacije i deskripcije, te metoda ukazivanja prednosti i nedostataka.

2. RAČUNALNI KRIMINAL – KONCEPTUALNI OKVIR I TEORIJSKE ODREDNICE

Danas su sa suvremenim razvojem IT tehnologije informacijski sustavi vrlo složeni i kao takvi zahtijevaju brojne investicije da bi se moglo kontinuirano razvijati i napredovati, kao i izgrađivati svoju sigurnost. U tom smislu, sa njihovim razvojem događa se računalni kriminal koji predstavlja ozbiljnu opasnost za sigurnost informacijskih sustava, narušava njihov rad, ugrožava njihovu opstojnost , ograničava im funkcioniranje te onemogućava postizanje zadanih ciljeva.

Dio opasnosti u tom području je kriminal koji je danas vrlo učinkovit, a provodi se virtualno uz pomoć informacijskih tehnologija gdje im je Internet glavna platforma. Kao takav, on je izuzetna opasnost, kako pojedincima koji posjeduju računala i u njima važne podatke, tako i poduzećima, malim i velikim organizacijama koje u virtualnom svijetu imaju niz poslovnih podataka i tajni, ali i važne međunarodne projekte od velike važnosti. Probijanjem sigurnosti računalnih sustava pojedinaca i poduzeća informatički napadači vrlo lako dolaze do takvih podataka, uništavaju ih ili kradu i nanose veliku štetu pojedincima i poslovanju poduzeća, odnosno gubitke s kojima se isti teško nose. Stoga je potrebno imati saznanja kako se informacijski napadi i kriminal izvršava putem suvremenih IT tehnologija te je potrebno pružiti svijest suvremenom društvu o posljedicama tih napada. Računalni kriminal razvio je kao takav brojne metode pomoću kojih se izvršava napad na informacijske sustave pa je stoga napadnutim stranama potrebno na vrijeme se zaštititi i prepoznati nepravilnosti u radu svojih IT sustava da bi se unaprijed spriječilo potencijalne počinitelje da ugroze njihovu informacijsku imovinu. Stoga će u ovom poglavlju biti riječi o konceptualnom okviru i teorijskim odrednicama računalnog kriminala, njegovu povijesnom razvoju, metodama napada te prevenciji istoga u poslovanju.

2.1. Teorijske determinante računalnog kriminala

Računalni kriminal je danas prisutan u cijelom svijetu te u svim domenama informacijskih sustava onih koje ih posjeduju. Računalna automatizacija i aplikacije temeljito su počele djelovati na radna mjesta što je dovelo do eliminiranja starih radnih mjesta te stvorilo nova radna mjesta s tim da su novi poslovi promijenjeni poradi prilagodbe uporabe računala (Babić, 2009: 43). Sve te raznolike aplikacije koje su nazočne u svijetu računala, od zbrajanja

pa sve do pripremanja kalkulacija za brzu razmjenu podataka, imaju jedinstven cilj - povećavanje produktivnosti. Danas je prisutnost računala i informatizacije u poslovanju posve izmijenio način na koji svako poduzeće posluje, olakšao je način rada, a računalni programi omogućili su djelatnicima povećanje radnog učinka plus skraćivanje vremena obavljanja posla i povećanje izvršavanja opsega posla u zadanom vremenu za razliku otprije nekoliko desetljeća kada se obavljalo manje posla u zadanom radnom vremenu.

Postojanje računala je osim prednosti donijelo i temeljnu opasnost za poslovanje pravnih osoba, ali i za pojedince koji posjeduju računala, a to je računalni kriminal. Danas se događaju računalni prijestupi napadača koji su od progresivnog značaja za poslovanje tvrtki, gdje nastaje sukob u poslovanju te je nužnost za zaštitu poslovanja u nekim slučajevima angažirati odvjetnika da bi se to poslovanje zaštitilo. Udruženje odvjetnika SAD – a je izdalo pregled rastućih problema računalnog kriminala, a posljednji podaci pokazali su sljedeće (Babić, 2009: 46): "...vidljivo je da 70 tvrtki godišnje pokazuje rezultate nastalih šteta računalnog kriminaliteta, a gubici se kreću između 145 do 730 milijuna američkih dolara".

Računalni kriminal podrazumijeva metode manipuliranja računalima poput neovlaštenog pristupa računalnom sustavu, na zaraze sustava virusima, manipuliranje podacima, trojanskim konjima i slično. Autori Šimunić i suradnici (2009) navode poseban oblik računalnog kriminala koji se naziva HOAX, u hrvatskom prijevodu „obmana", koji podrazumijeva blažu verziju računalnog kriminala u obliku e – mailova neistinitog sadržaja, koji se šalju s ciljem zastrašivanja ili dezinformiranja primatelja.

Međutim, računalni kriminal je puno obuhvatniji od navedenih e – mailova i podrazumijeva niz opasnih metoda napada na računalne sustave. Neki računalni napadi idu do te mjere ozbiljnosti da ugrožavaju nacionalnu sigurnost, a primjer je NASA koja je nekoliko puta otkrila napade na njihove informacijske sustave i neovlašten pristup podacima. U tom smislu postoje veoma educirani napadači, odnosno hackeri koji mogu otkriti tajne lozinke te s lakoćom uči u računalni sustav određene tvrtke. Zlouporabu računala olakšava loš sustav sigurnosti što nije začuđujuće kod pojedinaca, ali je uočeno da velike tvrtke, institucije, banke i drugi imaju začuđujuće niske stupnjeve sigurnosti. Čak se dogodi da otpušteni djelatnik ode od poslodavca, a da se nakon njegova odlaska ne izmijeni lozinka kojom se on služio, odnosno ne deaktivira se njegov korisnički račun (Babić, 2009.).

Babić (2009) navodi u svom djelu "Kompjuterski kriminal metodologija kriminalističkih istraživanja i razjašnjavanje i suzbijanje kompjuterskog kriminala" da zaposlenici između

sebe znaju ili lako otkriju lozinke kojima se drugi zaposlenici služe te da obično za lozinku uzimaju nešto što lako pamte, kao na primjer ime djevojke, supruge, broj telefona, datum rođenja, ime djeteta, kućnog ljubimca i slično.

Računalni kriminal ima svoj povijesni razvoj, a do snažnog napretka dobio je na razvoju sa progresivnim razvojem Interneta. Početak njegova snažnijeg razvoja datira još iz 1997. godine kada je Vijeće Europe osnovalo Ekspertnu komisiju za kriminalitet u kibernetičkom prostoru čiji zadatak je izrada međunarodnog instrumenta za suzbijanje kriminaliteta u kibernetičkom prostoru. Vijeće Europe objašnjava da pojava razvoja informacijsko-komunikacijskih tehnologija, prije svega interneta, a time i kaznenih djela na internetu, čime je kazneno pravo usmjereno na kompjutorski kriminalitet, postalo preusko pa se kazneno pravna zaštita proširila na cijeli kibernetički prostor te time dovela do potrebe stvaranja navedene ekspertne komisije (Kokot, 2014.).

Sam računalni kriminal se nije oduvijek smatrao kaznenim djelom. Njegove primjene je bilo i ranije, samo u manjoj mjeri jer računala nisu bila toliko razvijena. Tek je SAD prepoznao računalni kriminal kao potencijalnu i ozbiljnu opasnost za poslovanje i poduzeća 1979. godine te je iste godine definiralo računalni kriminal kao bilo koji nelegalni akt za čije počinjenje je upotrebljeno računalo ili računalna tehnologija (Babić, 2009.). Potrebu za ovim nametnula je činjenica, da je samo krajem 70-ih godina već bilo više stotina (preko 500) kaznenih djela učinjenih upotrebom računala (Babić, 2009.).

Računalni kriminal je u tom smislu napad i ilegalni akt na informacijske sustave pojedinaca i poduzeća gdje dolazi do krađe virtualnog identiteta i podataka koji su od iznimne važnosti te neki od njih posjeduju i financijsku vrijednost. Osim toga, računalni kriminal ima karakteristiku napada nematerijalne prirode i kao takav je objekt kaznenog djela koji nije materijalan te predstavlja napad koji nije opipljiv. Na njega se primjenjuju u svakoj državi opća načela kaznenog prava, ali njegova virtualna narav zahtijeva složenost procedure i problematike razrade cjelokupne problematike jer se tu javlja i anonimnost korisnika i anonimnost napadača te globalna računalna povezanost putem Interneta.

Sam povijesni razvoj računalnog kriminala ima svoje korijene daleko u 3. stoljeću prije Krista, kada se u Kini, Japanu i Indiji počinje koristiti prva ručna računala koja su se nazivala abak ili abakus. To daleko razdoblje je temelj razvoja suvremenih računalnih sustava, a razvoj je stagnirao do 17. stoljeća kada su se razvila prva mehanička računala te u 19. stoljeću sa razvojem elektronike , međutim, sa ovim razvojem je teško utvrditi kada je začetak

računalnog kriminala uistinu započeo. Stoga mogu postojati samo određene pretpostavke da se u najranijoj dobi njihova korištenja, u vrijeme prije Krista, netko sjetio kako ih zloupotrijebiti. Navodno se pojava i primjena računalnog kriminaliteta vezuje uz primjenu prvih računala te uz izum Josepha Marie Jacquarda, koji je 1808. godine usavršio prvi tkalački stroj, tako da je automatski utiskivao uzorke na tkaninu uz pomoć bušene kartice (Dragičević, 2004: 67). Navedeno otkriće je iskoristio Charles Babbage, koji je prvi poznat kao osoba koja je postavila temelje u radu suvremenih računala. Tada je Babbage počeo razvijati svoja računala, međutim ostali radnici su poduzimali niz aktivnosti u cilju zaustavljanja uvođenja novih tehnologija u industriju kako ne bi ostali bez posla. Tu je bila riječ o sabotažama, gdje su te počinjene sabotaže predstavljale prva kaznena djela iz gospodarskog kriminala - računalni kriminalitet (Dragičević, 2009.). Konačno, suvremeni začeci računalnog kriminala javljaju se u suvremenom poslovanju i njegovu kriminalu, koji je poznat pod nazivom kriminal bijelih ovratnika“, a razvio se početkom 20. stoljeća kada je razvoj računala dobio progresivan rast.

Računalni kriminal dalje dobiva na razvojnom značaju tokom 1960 – tih i 1970 – tih godina jer se izmišlja niz računalnih alata koji su omogućili provale u tuđe informacijske sustave te dobivanje tuđih podataka te njihovu zlouporabu. Počinju se razvijati ambiciozni računalni programi kao virusi, crvi i trojanski konji (Babić, 2009.). Osim, toga 1960 – tih godina počinje progresivni razvoj telekomunikacija, a s njima i kriminal u toj domeni, gdje se računalni napadači počinju nazivati phreakeri. Phreakeri su osobe koje rabe različite metode kako bi besplatno koristile telefonske usluge (Šimundić i Franjić, 2009: 23). Stečena znanja u smislu zlouporabe računalne tehnologije u telekomunikacijama su ubrzo rapidno primjenjene a ista znanja su se počela primjenivati sveobuhvatno i u razvoju informacijskih sustava. Na taj način, mnogi freakeri (engl. phreakeri) postaju hakeri (engl. hackeri) što dovodi i do brisanja granice između telekomunikacijskog i računalnog kriminaliteta (Šimundić i Franjić, 2009.).

Kako su se računala razvijala, njihova prva primjena je bila u znanstvene i vojne svrhe te za poslovanje gospodarskih subjekata. Poticaj za razvoj računalnog kriminaliteta je bio primjena modema, koja omogućava vezu između međusobno udaljenih sustava. Na to se nadovezuje razvoj osobnih računala s čime počinje snažniji val računalnog kriminaliteta.

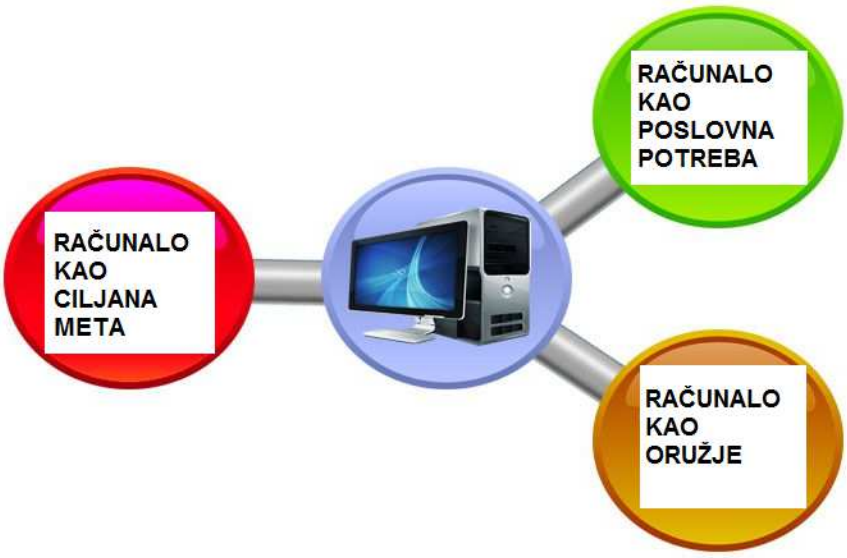
2.2. Metode i tipologija računalnog kriminala

Danas računalni kriminal ima status kaznenog djela. Tako brojna djela računalnog kriminala se mogu klasificirati sukladno različitim metodama napada. U tom smislu brojna djela računalnog kriminala spadaju u kategoriju djela „bijelog ovratnika“, dok se također koriste i djela računalnog kriminala u obliku dječje pornografije koja se, osim računalnog kriminala može tretirati i kao kazneno djelo seksualnog prijestupa gdje se javljaju elementi nasilja. Ovakvi prijelazi između kategorija te raznolikost aktivnosti koje prepoznajemo kao cyber-kriminalitet otežavaju razvrstavanje kaznenih djela u uže potkategorije.

Raščlamba metoda i pojavnih oblika računalnog kriminala je potrebna u smislu diferencijacije istih, ali i kategorizacije počinitelja, kao i težine određenog djela računalnog kriminala. Tu je prilično bitna detekcija počinitelja. U smislu same definicije računalnog kriminala moguće je izvršiti klasifikaciju djela koje on uključuje te ih kategorizirati prema značaju, važnosti, snazi , opasnosti i težini djela. Stoga se kaznena djela računalnog kriminala mogu klasificirati na sljedeći način (Yar, 2006):

1) Kaznena djela počinjena pomoću računala - prva skupina kaznenih djela postojala je i prije izuma Interneta, međutim ista se danas izvršavaju uz pomoć računala i unutar cyber-prostora. Primjeri ovakvih kaznenih djela su: prijevara, krađa, pranje novca, seksualno uznemiravanje, govor mržnje te pornografija.

2) Kaznena djela s računalom u fokusu - suprotno navedenom, kaznena djela s računalom u fokusu su nastala s pojavom Interneta i bez istog ne bi mogla postojati. Ova djela su prepoznatljiva i specifična za cyber-prostor, na primjer: „hakiranje“, virtualni napadi te oštećenja web-stranica.



Slika 1. Prikaz tipologije i procesa računalnog kriminala

Izvor: obrada autora prema Pinterest (2020): What is cyber crime, dostupno na https://in.pinterest.com/pin/834995587131907729/, pristupljeno 11.08.2020.

Prilikom kategorizacije i tipologije oblika računalnog kriminala, prijeko je potrebno utvrdit da li je računalo sporadičan ili neizostavan element djela računalnog kriminala. Razlike dvije navedene kategorije imaju elemente socio – ekonomske prirode te mogu biti korisne u kategorizaciji, ali kao takve su ograničene u kriminološkoj obradi. Stoga je jedna od alternativa mobilizirati postojeće klasifikacije izvedene iz kaznenih zakona u odgovarajuće kategorije kaznenih djela počinjenih uz pomoć računala. Sukladno navedenome, Yar (2006) definira četiri pravne kategorije kaznenih djela cyber-kriminala:

- Neovlašteni pristup: neovlašteni pristup vlasništvu druge osobe i /ili činjenje štete istom (npr. „hakiranje“, računalni virusi, obezličenje web-stranica)
- Cyber-prijevare i krađe: krađa novca i privatnog vlasništva (npr. prijevare s kreditnim karticama; povrede intelektualnog vlasništva - poput „piratstva”)
- Cyber-pornografija: aktivnosti koje krše zakone opscenosti i pristojnosti
- Cyber-nasilje: nanošenje psihološke štete ili poticanje fizičkog nasilja, tj. kršenja prava osoba koje su napadnute (npr. govor mržnje; uhođenje).

Yar (2006) je najprecizniji znanstveni istraživač računalnog kriminala koji je izvršio preciznu klasifikaciju tipologije djela računalnog kriminala te je definirao postojeće koncepte nedozvoljenog virtualnog ponašanja- On također smatra da ova podjela ne onemogućava

kvalitativno razlikovanje i izdvajanje računalnog kriminala kroz definiranje specifičnosti i obilježja istoga. Zato se kriminologija u domeni obrade računalnog kriminala orijentira a pronalazak inovacija koje obilježavaju socio – strukturalne značajke cyber prostora gdje se virtualni napadi manifestiraju. Osim Yara, tu su još i autori McGuire i Dowling

Navedena klasifikacija je korisna u povezivanju cyber-kriminaliteta s postojećim konceptima nedozvoljenih ponašanja. Međutim, Yar (2005) smatra da ne omogućava kvalitativno razlikovanje i izdvajanje cyber-kriminaliteta kroz uočavanje specifičnosti istog. Posljedično, većina kriminologa se (posebice oni koji naginju sociološkim objašnjenjima) fokusira na pronalazak noviteta unutar socio-strukturalnih značajki okruženja (cyber-prostora) u kojem se takva nedozvoljena ponašanja manifestiraju (Yar, 2005). McGuire i Dowling (2013) kaznena djela s računalom u fokusu nazivaju „čistim“ cyber-kriminalom ili djelima koja ovise o računalu. Dakle, radi se o aktivnostima koje se primarno usmjeravaju protiv računala ili računalnih mreža, no isti autori smatraju da mogu postojati sekundarne dobiti ovakvih napada. Na primjer, podatci dobiveni neovlaštenim pristupom određenoj elektroničkoj pošti mogu se koristiti za počinjenje prijevare (McGuire i Dowling, 2013). Nadalje, McGuire i Dowling (2013) kaznena djela s računalom u fokusu dijele na dvije široke kategorije:

- Neovlašteni pristup računalnim mrežama (npr. „hakiranje“)
- Narušavanje ili smanjivanje funkcionalnosti računala i mreže (npr. virusi i DoS napadi- eng. Distributed Denial-of-service Attack)

Prema ovim autorima računalni kriminal spada u domenu kriminala protiv ili uz pomoć računala, gdje su obuhvaćena kaznena djela počinjena pomoću računala te kaznena djela s računalom u fokusu. Ista autorica dodaje da postoje i politički motivirana kaznena djela, tj. tehnički „ne-prijestupi“ u svijetu cyber-kriminala.

Navodeći ovu definiciju, McGuire i Dowling (2013) specificiraju tri velike kategorije računalnog kriminala koje za sobom vuku štetu koja je nanesena:

- Prva kategorija se odnosi na cyber-kriminalitet koji rezultira imovinskom štetom. Za činjenje ovakvih kaznenih djela se najčešće koristi tehnika „krekiranja“ (neovlašteni pristup računalnom sustavu radi činjenja kaznenog djela) te uključuje sljedeće pojavne oblike: flooding, proizvodnju i distribuciju računalnih virusa i crva, spoofing, phreaking te povredu prava intelektualnog vlasništva.

- Druga kategorija obuhvaća cyber-kriminalitet koji rezultira štetom za osobu koji se generalno dijeli na cyber-uhođenje (eng. Cyberstalking) i cyber-pornografiju.
- Naposljetku, treća kategorija se odnosi na djela koja Brenner (2001) naziva tehničkim „ne-prijestupima“ poput „haktivizma“ (eng. Hacktivism) i „cyber-vigilantizma“.

Navedena tipologija i pojavni oblici računalnog kriminala su precizno definirani od strane značajnih navedenih autora te su kao takvi relevantni za obradu u znanstvenoj literaturi. Računalni kriminal se stoga javlja u različitim pojavnim oblicima specifične težine kaznenog djela.

2.2.1. Hakerski napadi

Pojmovni termini „haker“ i „hakiranje“ su u suvremenm informatičkom svijetu danas opće poznati te su jedan od najčešćih oblika računalnog kriminala. Trenutne rasprave stručnjaka o „hakiranju“ su dovele do zajedničke definicije koja glasi: *„hakiranje je neovlašteni pristup i naknadna uporaba tuđeg računalnog sustava“* (Yar, 2006: 22). Sukladno navedenome, najpreciznija definiciju hakiranja daje Yar (2006) gdje se isto definira kao računalna provala, što bi obilježilo „hakera“ kao provalnika. Stoga se može smatrati kako je hakiranje najčešći oblik računalnog kriminala te je njegov neizostavan element kojim se nanosi imovinska šteta žrtvama.

Sam termin „haker“ se počeo primarno koristiti 1960 – tih godina među računalnim programerima, ali tada nije imao negativnu konotaciju računalnih kriminalaca. Tad je hacker označavao osobu natprosječnih informatičkih sposobnosti i vještina koje je primjenjivao te koje su rezultirale inovativnim informatičkim rješenjima te djelotvornim rješavanjem računalnih problema. Iz navedenog se može zaključiti da je „hakiranje“ jedan od ključnih, ako ne i neizostavnih elemenata *cyber* - kriminala koji rezultira imovinskom štetom (Schell i Martin, 2004). Dodatno, „hack“ je sam po sebi označavao inovativno korištenje tehnologije koje je dovelo do pozitivnih rezultata i prednosti (Yar, 2006). Tad su te osobe imale pristup Internetu, koji je u to doba bio ograničen i omogućen samo specijaliziranim stručnjacima, hrabrim pionirima u računalnoj revoluciji (Yar, 2006).

1980 – tih godina kada se progresivno počeo razvijati računalni kriminal, da bi se diferencirao pojam hackera, za računalne kriminalce je uveden pojam „crackera“, a koji je opisivao osobe koji su informatičkim znanjem rušili sigurnost informacijskih sustava. Tada je

razlika hackera i crackera bila u motivaciji njihova ponašanja u virtualnom svijetu, međutim, preuzet je pojam hacker koji je tada diferenciran kao „hacker bijelog šešira“ za nadarene specijalizirane stručnjake te „hacker crnog šešira“ za osobe koje su rušile sigurnosne informatičke sustave. Tako su hackeri crnog šešira u svojim informatičkim napadima koristili za motiv napada osvetu, sabotažu konkurentnih poduzeća, krađu informacija te vršenje terora nad određenim skupinama. Yar (2006) je naveo razliku između hakera i crakera gdje motivacija leži u razlikama koje će olakšati kriminološku obradu, a u daljnjem razvoju hakiranja su sociolozi opisali hakere procesom etiketiranja kao osobne napadače u virtualnom svijetu koji svijesno i ciljano nanose štetu napadom na računalne sustave. Radi se o procesu kroz koji se kreiraju kategorije kriminalnih i devijantnih aktivnosti i identiteta od strane društva. Posljedično, reakcije na „hakiranje“ i „hakere“ ne mogu se shvatiti odvojeno od činjenice da je značenje ovih termina društveno raspravljano i stvoreno (Yar, 2006).



Slika 2. Prikaz pada računalnog sustava napadom hackera

Izvor: Lepitak, S. (2017): World's biggest agency networks claim all clear from cyber attack following WPP hacking, dostupno na https://www.thedrum.com/news/2017/06/28/worlds-biggest-agency-networks-claim-all-clear-cyber-attack-following-wpp-hacking, pristupljeno 11.08.2020.

Motivacija za hakiranje je danas potrebna da bi se shvatilo na koje načine hackeri vrše svoje virtualne operacije napada i rušenja računalnih sustava te nanose štete. Yar (2006) smatra da aktivnosti u kojima sudjeluju gotovo uvijek uključuju neku vrstu manipulacije, remećenja i upada u računalni sustav. Yar (2006) je definirao nekoliko načina na koje hackeri uništavaju računalne sustave, a oni su sljedeći:

- a) KRAĐA RAČUNALNIH RESURSA/OSOBNIH I POVJERLJIVIH INFORMACIJA - Objekt krađe može biti resurs (npr. glazba, film, transkript i sl.) ili informacija (npr. poslovna tajna, osobni podatci, detalji kreditnih kartica). Yar (2006) spominje slučaj švedskog „hakera“ koji je preuzeo ogromnu količinu glazbe te ju dijelio putem Interneta. Međutim, otuđeni podaci se mogu koristiti i u kaznenim djelima s mnogo značajnijim posljedicama (Yar, 2006). Yar spominje i autora Riema (2006) koji navodi incident kada su „hakeri“ ukrali detalje nekoliko tisuća kreditnih kartica te ove informacije iskoristili (kroz manipulaciju bankovnog sustava) za prisvajanje sredstava.
- b) IZMJENA, SABOTAŽA I UNIŠTAVANJE RAČUNALNOG SUSTAVA - Jednom kada uspiju ući u računalni sustav, „hakeri“ mogu učiniti značajnu štetu. Dok je uništavanje sadržaja relativno rijetko, postoji nekoliko zabilježenih slučajeva nezadovoljnih korisnika koji su sabotirali svoje nekadašnje poslodavce brisanjem bitnih informacija. Češći oblik je selektivna izmjena podataka unutar računalnog sustava. „Hakeri“ ovu metodu koriste kako bi prikrili dokaze svojih aktivnosti te si tako omogućavaju nesmetani upad u sustav u budućnosti.
- c) „OBEZLIČENJE“ WEB-STRANICA I „SPOOFING“ - Prilikom „obezličenja“ web-stranice, za razliku od ranije navedenih aktivnosti, nije potrebno upasti u tuđi računalni sustav. „Haker“ (putem Interneta) može preuzeti kontrolu nad web-stranicom te mijenjati sadržaj iste. Motiv za ovakva ponašanja može biti želja da „zabavi“ posjetitelje stranice uz pomoć neslane šale, može se raditi o treniranju vještina „hakiranja“ ili o ideološki i politički motiviranim oblicima prosvjeda protiv država ili korporacija. Drugi oblik „hakiranja“ web-stranica je „spoofing“ (hrv. podvala). Radi se o prisvajanju identiteta legitimnog korisnika unutar cyber-prostora od strane neovlaštene osobe (Schell i Martin, 2004). Prilikom ove aktivnosti, „haker“ ne upada u web-stranicu legitimnog korisnika, već kreira vlastitu inačicu koja podsjeća na originalnu. Posljedice ovakvih aktivnosti mogu biti relativno bezopasne, npr. neugodnosti za pravog vlasnika stranice (budući da promjene web-stranice često uključuju prikazivanje pornografskog sadržaja i sl.), no mogu imati i ozbiljnije posljedice za velik broj ljudi.
- d) NAPAD USKRAĆIVANJEM RESURSA („FLOODING“) DoS-napadi (eng. Denial of Service Attack) mogu rezultirati prisilnim resetiranjem napadnutog računala, no mogu se koristiti i za iskorištavanje njegovih resursa (poput rada procesora,

memorije ili mreže). Rezultat je nemogućnost korištenja računala od strane legitimnog vlasnika.

- e) DISTRIBUCIJA MALICIOZNOG SOFTVERA - Maliciozni softver ili kod (izv. *Malware*) je program koji je tajno implementiran u drugi program ili računalni sustav s ciljem: „*uništavanja podataka, pokretanja razornih programa, ugrožavanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija i operacijskog sustava legitimnom korisniku*“ (Yar, 2006.). Kao takav, maliciozni softver jedan od najizvjesnijih prijetnji većini korisnika te uzrokuje rasprostranjenu štetu i nemir unutar većine organizacija.

McGuire i Dowling (2013) su otišli korak dalje te su naveli i kategorizirali računalne programe koji se koriste u zlouporabi napadima na računalne sustave. Tako su isti autori naveli podjelu zlonamjernih računalnih programa kako slijedi (McGuire i Dowling, 2013: 77

- **Računalni virus** je program koji kreira svoje kopije te ih implementira u postojeće programe ili datoteke. Često se aktivira putem interakcije s računalom poput otvaranja datoteke ili pokretanja programa.
- **Crv** također stvara vlastite kopije te je samostalan program koji se aktivira bez interakcije s računalom. Može se širiti putem Interneta ili elektroničke pošte.
- **Trojanski konj** je samostalan program koji, premda izgleda bezazleno, ima skrivenu malicioznu namjenu. Trojanski konj može zamijeniti postojeće datoteke sa „zaraženima“, ili dodavati takve datoteke u računalni sustav.
- **Mobilni maliciozni kod** (izv. *Malicious Mobile Code*) je zlonamjerni program koji se, bez pristanka, prenosi s računala počinitelja na računalo legitimnog korisnika.
- **Miješani napadi** (izv. *Blended Attacks*) uključuju kombiniranje ranije navedenih napada usmjerenih na jedno računalo.

Hackeri se danas smatraju malom, ali visoko učinkovitom i motiviranom skupinom koja djeluje u virtualnom svijetu napadom na računalne sustave sa ciljem da uništi iste, podatkovne podatke i informacije te svjesno nanese štetu napadnutim tvrtkama ili institucijama koje napada. Oni ne djeluju u realnom svijetu i njihovi napadi nisu materijalne i opipljive prirode, već isti djeluju putem automatiziranih softverskih alata koji imaju status tehnološke inovacije.

2.2.2. Računalne prevare

Računalne prevare su vrlo česte u virtualnom svijetu i hackeri ih često koriste da bi se okoristili. Najprecizniju definiciju računalne prevare dali su autori Button i Cross (2017:6) gdje su istu opisali kao „*široki spektar aktivnosti čije je zajedničko obilježje neistinito predstavljanje od strane počinitelja kako bi si osigurao korist ili prouzročio štetu drugima*“. Aktualne definicije računalnih prevara su povezane s razvojem IT tehnologija i kako iste idu rapidno naprijed tako i računalne prevare dobivaju nove dimenzije. Međutim, računalne prevare su postojale od trenutka kada se razvio računalni kriminal i kada su hackeri otkrili mogućnosti korištenja istih da bi ostvarili vlastitu korist. IT tehnologija je omogućila da se one razviju do razine gdje hackeri soficisticiranim alatima napadaju računalne sustave i vrše krađe koje mogu biti informacijske ili financijske prirode.

Button i Cross (2017) naglašavaju da tehnologija nije utjecala na želju niti spremnost počinitelja da sudjeluju u prijevari, već na same metode počinjenja kaznenog djela. Pa je tako razvojem pošte došlo do prijevare putem pisama, a izumom telefona nastale su telekomunikacijske prijevare. Slijedom navedenog, pojavom Interneta nastaje računalna prijevara (eng. *cyber-fraud*) (Button i Cross, 2017).

Računalne prevare obilježava njihovo odvijanje u virtualnom svijetu, primjenu virtualnih sofisticiranih alata u napadima, anonimnost hackera, zaštitu njihova identiteta, spoznaju da je počinitelj anoniman od strane žrtve te da napadnuta žrtva nije u mogućnosti vratiti ukradeno jer je to počinjeno na vrlo sofisticiran način, gdje je i kriminološkoj obradi otežan posao u pronalasku krivca.

Button i Cross (2017:7) razlikuju prijevaru (eng. *fraud*) i „*scam*“ (hrv. obmana; podvala) koju definiraju kao: „*obmanjujuće ponašanje kojem je cilj pridobiti materijalna sredstva ili informacije od prevarene osobe te se može shvatiti kao neetično postupanje, građansko ili upravno pitanje ili nezakonita prijevara*“. Prema tome, termin „*scam*“ obuhvaća ponašanja koja nisu nužno nezakonita (poput neetičnog postupanja), dok termin prijevara podrazumijeva samo nezakonitu stranu na kontinuumu (Button i Cross, 2017).

Button i Cross (2017) su naveli nekoliko klasificiranih vrsta računalnih prevara koje se primjenjuju u virtualnom svijetu. Iste su opisane u nastavku, kako su ih definirali Button i Cross (2017):

- „Romantična prijevara“ - Ovakav oblik prijevare obuhvaća širok spektar ponašanja koji uključuju povredu raznih prava. S jedne strane, situaciju kada se osoba prijavi na *web*-stranicu za pronalaženje partnera i neiskrena je o svom bračnom statusu možemo obilježiti kao neetično ponašanje, no ne i nezakonito (barem ne u većini država). S druge strane, kada počinitelj koristi lažni identitet da ostvari romantične odnose s više partnera kako bi pridobio materijalna sredstva, radi se o nezakonitom ponašanju.
- „Nigerijski princ“ - Jedan od klasika računalne prijevare je „*Nigerian 419 scam*“. Tijekom ove vrste prijevare ciljanu osobu kontaktira „korumpirani službenik“, koji joj nudi naknadu ako mu dozvoli da joj na račun prenese ilegalno stečena sredstva. U slučaju da ostane na navedenom, radi se o kaznenom djelu pranja novca. Međutim, „korumpirani službenik“ često prvo traži uplatu od strane žrtve kako bi „pridobio povjerenje“ što rezultira financijskim gubitkom za žrtvu. a) Prijevara bez kartice (izv. *Card Not Present Fraud*; počinitelji prisvoje potrebne brojeve s kreditne kartice te ih koriste za *online* trgovinu)
- Lažna prodaja (izv. *Fraudulent Sales*; prodaja pogrešno predstavljene ili nepostojeće robe).
- Prijevara putem krađe identiteta (izv. *Phishing Scams*; predstavljanje, putem elektroničke pošte u ime legitimne organizacije s ciljem uvjeravanja korisnika te pribavljanja povjerljivih informacija).
- Masovne marketinške prijevare (izv. *Mass Marketing Frauds*; uključuje raznolike oblike prijevare s ciljem osiguravanja plaćanja od strane žrtve; može se raditi o lažnim dobitcima na lutriji, informacijama o ostavštini, prilikama za poslovanje).

Sve navedene računalne prevare su iznimno česte i događaju se svugdje u svijetu računalnih komunikacija. Najčešći napadi računalnih prevara su velike kompanije i državne institucije, ali i srednja poduzeća, kao i dioničke burze gdje hackeri nastoje ukrasti povjerljive informacije koje će potom prodavati za novac javnosti ili krađa financijskih sredstava kojima se mogu financijski okoristiti, a žrtvama nanijeti veliku financijsku štetu i ozbiljno narušiti njihov opstanak i poslovanje.

2.2.3. Kršenje online autorskih prava i računalno nasilje

Autorska prava u Hrvatskoj definira Zakon o autorskom pravu i srodnim pravima (NN 127/14). Sukladno Zakonu, autorsko pravo pripada fizičkoj osobi koja stvori autorsko djelo, dok djelo umjetnika ili izvođača pripada fizičkoj osobi koja proizvede djelo iz književnog ili umjetničkog područja. Autorska djela koja spadaju pod domenu računalnog i virtualnog svijeta u smislu ovog Zakona su fotografska i audiovizualna djela te djela znanstvene i tehničke prirode.

Takvu vrstu autorskih prava hackeri i korisnici Interneta mogu zloupotrebljavati na način da preuzimaju tuđa autorska djela predstavljajući ih kao svoja ili preuzimaju iste te ih ilegalno distribuiraju i dobavljaju bez pristanka autora takvih djela.

Najčešći oblik povrede autorskih prava na Internetu je digitalno piratstvo. Digitalno „piratstvo“ je oblik kršenja autorskih prava na Internetu čiju je najprecizniju definiciju dao Sampat (2009), opisujući ga kao metodu ilegalnog dobavljanja i distribuiranja računalnih programa, igara, videa, glazbe i drugih medija, putem računala ili telekomunikacijskih uređaja. On je naglasio kako ovo kršenje uključuje reprodukciju i distribuciju autorskog materijala bez pristanka samog autora.

Ova vrsta kršenja online autorskih prava nema svojstvo prevare same po sebi, međutim, neki autori ga klasificiraju kao vezano kazneno djelo jer se osobe koje ilegalno koriste tuđa autorska prava direktno miješaju u vlasništvo druge osobe, bez obzira što je to objavljeno na Internetu. Ovo kršenje ima obilježje računalne krađe, odnosno preuzimanja i distribucije tuđeg autorskog djela u sebi korisne svrhe.

Danas su autorski materijali sve prisutni na Internetu i svatko se danas može smatrati autorom, kako određene fotografije ili filma, tako i određenog pisanog djela u obliku bloga, novinarskog ili znanstvenog članka, knjige ili sličnih djela objavjenih u online izdanju. Tu se također ubrajaju pjesme, filmovi, kratki video uradci i ostali video zapisi, video igrice i ostalo. Takva autorska djela mogu biti nezakonito preuzeta te distribuirana ilegalno bez pristanka autora gdje počinitelji mogu steći materijalnu korist od tuđeg djela i time se stvara kazneno

djelo. Iako je kršenje autorskih prava prepoznato kao nezakonito, provedba zakona o autorskim pravima je tradicionalno bila (i ostala) pitanje građanskog prava (Clough, 2010).

Što se tiče online nasilja, isto se često primjenjuje nad određenom skupinom stanovništva koja koristi Internet, a koja je neupućena u zle namjere računalnih online zlostavljača. Radi se često o ranjivim skupinama poput adolescenata, djece ili žena koji koriste brojne online portale za komunikaciju, igrice, društvene mreže i slično. S obzirom da svake godine raste sve veći broj korisnika računala i društvenih mreža gdje isti objavljuju svoje osobne podatke, s druge strane postoje osobe koje mogu koristiti iste s namjerama da povrijede svoje žrtve.

U sklopu implementacije online nasilja često se koristi termin „Cyber – bullying“, gdje se namjerno uzmemirava i povređuje djecu i mlade kao korisnike društvenih mreža i Interneta. Drugi termin je online uznemiravanje koje se često primjenjuje na nedefiniranoj skupini ljudi, a često se radi o emocionalno ranjivim skupinama koje ustupaju svoje podatke počiniteljima koji potom iste koriste da bi ih uznemiravali u oblik ucjena ili ometanja u svakodnevnom realnom životu. Ne postoji univerzalna definicija online uznemiravanja jer nema konkretnih zakonskih odredbi kojima se može obilježiti zakonski što se smatra online uznemiravanjem ili povredom socijalnih normi. Clough (2010) je ipak precizirao u svom djelu Cybercrime online nasilje kao set nasilničkih ponašanja koje uključuju korištenje Interneta za slanje štetnih poruka ciljanoj osobi te objavljivanje štetnog sadržaja o osobi. Ovdje se radi o online ponašanju koje je svjesno zlonamjerno, kontinuirano ponavljajuće i agresivno, a koje djeluje uzmemirujuće na osobu kojoj je upućeno u stvarnom svijetu. Takav oblik nasilja rješava se odredbama Kaznenog zakona, gdje maltretirana osoba može slučaj prijaviti policiji te potom ista primjenjuje kriminološku obradu ovisno o težini online nasilja.

2.3. Prevencija računalnog kriminala

Postoje brojni zakonski akti kojima se reguliraju sankcije zbog primjene računalnog kriminala, ali i stručna literatura obrađuje slučajeve i dokaze o prevenciji i posljedicama, kao i o sankcijama računalnog kriminala te zaštiti žrtava koje su izložene istome u bilo kojem obliku. Tako brojni stručnjaci stvaraju kompaktivne veze između prirode računalnog kriminala te kako on svojim vrijednostima te demografskim obilježjima utječe na počinjenje kaznenog djela te koji su oblici sankcija za iste.

Prevencija računalnog kriminala se stoga provodi u svrhu pronalaska, kažnjavanja i eliminacije sa online cyber prostora onih aktivnih sudionika koji provode računalni kriminal jer oni svjesno odabiru da sudjeluju u kriminalnim online aktivnostima jer od njih očekuju određenu nagradu u obliku ukradenih informacija, financijske koristi ili bilo kakve druge potencijalne osobne ili emocionalne nagrade.

Holt i Bossler (2016) su slijedom navedenog definirali pet kategorija aktivnosti koje direktno utječu na mogućnosti činjenja kaznenih djela, a one su sljedeće:

- otežavanje činjenja kaznenih djela;
- povećanje rizika detekcije;
- smanjivanje potencijalne nagrade;
- smanjivanje provokacija za činjenje kaznenih djela;
- uklanjanje opravdanja za spomenute aktivnosti

Prevencija računalnog kriminala koja se može implementirati u svrhu njegova daljnjeg širenja je primarno orijentirana na pokušaje otežavanja počinjenja takvih kaznenih djela. To se primarno čini neposrednom ugradnjom sigurnosnih zaštita na sva računala koja su potencijalni izvor opasnosti od takvih napada, počevši od kućnih računala za osobnu uporabu, do velikih računala značajnih svjetskih institucija poput NASA – e, Pentagona, Svjetske banke, svjetskih financijskih burzi i ostalih značajnih institucija kojima je od velike važnosti računalna zaštita zbog posjedovanja značajnih podataka i financijskih sredstava u velikim iznosima i važnosti. Postoji i razvijanje strategije gdje se korisnici educiraju o samozaštiti i razvijanju vještina kako zaštititi osobni identitet na Internetu, ali i zaštititi vlastito računalo korištenjem lozinki, zaštitnih računalnih programa i ostalih softverskih alata zaštite od računalnog kriminala.

Iako gotovo svi sustavi (uključujući *web*-stranice, elektroničku poštu te pristupe internim bazama podataka), zahtijevaju upotrebu korisničkog imena i lozinke zbog autorizacije pristupa, jedan od najutjecajnijih ograničenja računalne sigurnosti je problem sigurnosti lozinke. Spomenuti problem proizlazi iz korištenja lozinki koje nemaju odgovarajuću razinu sigurnosti ili lozinki koje korisnik već koristi prilikom pristupa drugim sustavima (Holt i Bossler, 2016). Napretkom IT tehnologija došlo je do revolucije gdje se pruža zaštita

razvojem ekrana na dodir koji može prepoznati lice ili otisak prsta pa nije potrebna lozinka te je automatski stupanj sigurnosti veći. Time je otežan pristup napadačima i sudionicima računalnog kriminala, a još je razvijenija metoda ugrađivanja biometrijskih mjera sigurnosti.

Danas stručnjaci za zaštitu od računalnog kriminala razvijaju inovacijske metode kojima lakše detektiraju napadače te mogu na vrijeme spriječiti određene napade i prouzrokovanje štete. Ključan resurs u povećanju rizika detekcije je sustav detekcije upada ili *Intrusion Detection System* (IDS) koji se koristi za identifikaciju dvije vrste prometa(Holt i Bossler, 2016):

- zlouporaba resursa baziranih na općenitim obilježjima poznatih malicioznih programa i
- anomalija u standardnim obrascima korištenja mreže koje nagovještavaju zlouporabu računalnog sustava

Danas postoje i mehanizmi koji se u redukciji računalnog kriminala odnose na primjenu kaznenih djela koja su povezana s obmanom i računalnom krađom. To se odnosi na počinitelja koji uspije uspješno pristupiti određenom računalnom sustavu poduzeća ili važne organizacije i pri tome traži određene povjerljive podatke kojima bi potencijalno mogao ostvariti materijalnu dobit. Velike korporacije su toga svjesne pa su kao takve angažirale informatiče stručnjake koji su im razvile mehanizme skrivanja ili maskiranja podataka (Holt i Bossler, 2016.). Dodatno, osmišljena je tehnika smanjivanja potencijalne nagrade koja utječe na mehanizme plaćanja ilegalnih usluga, podataka ili materijala. Kroz eliminiranje usluga *online* plaćanja, koje koriste počinitelji, agencije za provedbu zakona mogu ograničiti ilegalne aktivnosti koje uključuju razmjenu materijalnih sredstava (Holt i Bossler, 2016).
Može se zaključiti da je prevencija računalnog kriminala danas dosljedna, zakonski uređena, kao i informacijski brojnim sustavima zaštite. Međutim, znanja suvremenih računalnih napadača, online zlostavljača ili osoba loših namjera koji uvijek mogu koristiti određene metode su velika i uvijek postoje prilike i situacije kada isti toliko napredno znaju provaliti u računalne sustave razbijajući sve sigurnosne zaštite. Takvih situacija je bilo i uvijek će ih biti unatoč višestruko i sofisticirano razvijenim sustavima zaštite, a prevencija mora ići u korak sa suvremenim razvojem IT tehnologija jer će se jedino tako pokazati učinkovitom.

3. RAČUNALNI KRIMINAL I POSLOVNA ETIKA

Računalni kriminal je danas prije svega etičko pitanje i pitanje morala osobe koja ga vrši jer ga primjenjuje svjesno s ciljem nanošenja štete drugom korisniku bilo koje vrste. U suvremenom poslovanju sveobuhvatna je primjena poslovne etike s čijeg se stajališta promatra računalni kriminal kao domena negativnog utjecaja na poslovanje svakog poduzeća i potencijalne opasnosti da se istome mnogostruko našteti. Stoga se javljaju brojna moralna pitanja koji su ciljevi takvih napadača i čemu štetiti određenom poduzeću ili instituciji. Stoga će u ovom poglavlju biti riječ o poslovnoj etici, njezinoj primjeni u poslovanju te njenom moralnom stajalištu prema računalnom kriminalu.

3.1. Teorijske odrednice poslovne etike

Danas se u poslovnoj etici primjenjuju visoki standardi ponašanja u međuljudskim odnosima. Ona od čovjeka zahtijeva moralno, korektno i odgovorno ponašanje spram drugih da bi se održali korektni i pozitivni međuljudski odnosi. Stoga se primjena etičkog kodeksa u poslovanju odnosi na svaku osobu pojedinačno i obuhvaća individualno pojedinca, odnosno pomoću nje se nastoji potaknuti pojedinca da u svom djelovanju koristi moral i poštenje.

Sama poslovna etika obuhvaća sustav vrijednosti koje čovjek posjeduje i koje primjenjuje u svom djelovanju te koje iskazuje svojim ponašanjem. Poslovna etika je, kao znanstvena disciplina, primijenjena u modernom poslovnom svijetu te je usvojena kao temeljni moralni koncept koji ljudi usvajaju u izgradnji svojih međuljudskih odnosa u nekoj sredini, u ovom slučaju, u poslovnoj sredini. Primjenom poslovne etike gradi se pozitivan imidž cijele jedne organizacije, a upravo tome doprinose njeni sudionici koji primjenjuju tu poslovnu etiku. U svome djelovanju u poslovanju ljudi se susreću s brojnim zahtjevnim situacijama u kojima moraju donijeti odluku sukladno svojoj savjesti. Budući da promjene u modernom životu donose promjene u načinu života, znanju, radu, zakonima i vrijednostima, ljudi se tim promjenama moraju prilagoditi te moraju voditi brigu o svome ponašanju te primjeni toga ponašanja u poslovnoj etici. Zato su pitanja poslovne etike danas sveprisutna te su postala kompleksan i objedinjen dio svake poslovne prakse te uvjet izgradnje dobrih međuljudskih odnosa unutar jedne sredine i organizacije.

Danas uvjeti globalnog poslovanja pred svaku poslovnu i radnu organizaciju stavljaju potrebe da ostvare konkurentsku prednost, zacrtane ciljeve te uspješne financijske rezultate. Da bi se uspjeli ostvariti ti ciljevi, postupci i djelovanje te organizacije moraju se temeljiti na etičkim principima, načelima poslovanja, stavovima i vrijednostima. Upravo će organizacije koje uspijevaju uskladiti i uspostaviti ravnotežu između načela profitabilnosti etičnosti biti one organizacije koje će imati dugoročnu perspektivu rasta i razvoja (Aleksić, 2007.).

Suradnjom etike i ekonomije kao znanstvenih disciplina u suvremeno doba, preciznije u 20. stoljeću, razvila se disciplina poslovne etike. Sama riječ etika potiče od grčke riječi ethos, što znači običaj ili karakter, a kao takva se u najranije doba javlja u vrijeme Homera i Hezioda, te je tada označavala način kako neko biće živi u svojoj životnoj okolini (Talanga, 1999.). Tako je etika dobila status filozofske discipline koja se bavi ciljevima moralnog htijenja te istražuje moralne činove i izvore morala. Tako etika daje uputstva i odgovore na pitanja kako se treba živjeti, kako djelovati i postupati u određenim situacijama te kakve karakterne osobine primjenjivati. Njen je zadatak da nas upozna sa pojmom morala i njegovim komponentama te da zauzme kritičko stajalište prema postojećoj moralnoj praksi (Talanga, 1999.). Iako se danas pojavljuju kao sinonimi, moral i etika nisu dva istoznačna pojma. Moral dolazi od latinske riječi mos, moris te predstavlja Ciceronov prijevod grčke riječi ethos. Iako se tako ova dva pojma mogu poistovjetiti, ipak se moral mora diferencirati od etike jer on predstavlja skup pravila određenog društva o sadržaju i načinu međusobnih odnosa i ljudskih zajednica (Bebek, 2005.). Zato se može reći da je etika filozofija morala, a moral je temeljni način ljudskog odnosa spram svijeta.

Čovjek se svakodnevno bavi etikom i njenim istraživanjem te često ne razmišljaju o pravom značenju te riječi. Moralan i etičan čovjek je prema drugima pošten i čestit te razlikuje dobro od zla. U svojim djelima o etici i moralu autori Čehok i Koprek donijeli su jednu zanimljivu konstataciju koja se odnosi na etiku – ta konstatacija kaže da umjesto da se na moral gleda pozitivno, često se etiku u životu promatra u negativnom smislu te se ograničava njezino značenje. Međutim, velik značaj poimanju etike kao pojma dao je Aristotel, koji je etiku usko vezao uz poimanje lijepoga, dobroga, korisnoga, te time efikasnog i ekonomičnog. Platon se koristio pojmom etike da bi ukazao na put ili način spoznaje dobroga i lijepoga.

Sumirajući tako različite definicije i stajališta o etici, može se konstatirati sljedeće (Bebek, 2005.): etiku se definira kao znanost o moralu s tim da je moral u izvjesnom smislu latinska riječ za etiku. S druge strane se etika odvaja od morala, s tim da se moral definira kao osobni ili društveni putokaz, a etika se vidi kao filozofija ili sustav objašnjavanja tog morala.

Etika se kao znanstvena disciplina kategorizira u dvije kategorije: etiku duha, koja podrazumijeva načelnu i osjećajnu etiku te etiku slova, koja podrazumijeva pisana ili verbalna pravila. Ove dvije kategorije etike polaze od činjenice da je čovjek u svom djelovanju vođen prirodnim motivima te da nastoji izbjeći bol, patnju i nelagodu – to su temeljni stavovi Hutchesona (Čehok, 1996.). On se u svom predstavljanju etike drži temeljnog načela da se postigne najveća moguća sreća sa najvećim brojem ljudi – to je načelo korisnosti koje u etici ima veoma važnu ulogu. Osim ove kategorizacije etike, postoje još dvije njezine klasifikacije. Te klasifikacije su sljedeće (Benek, 2005.):

- Deontološka etika – tu se grupiraju norme i načela potrebnog djelovanja koje etiku čini dobrom u skladu s normom ili načinom djelovanja.
- Teološka etika – tu učenja o etici traže dobro koje određuje etiku u svrsi ili cilju.

Važnost etike u ljudskom životu je velika jer ona postavlja imperativ da čovjek mora djelovati moralno, ispravno i korektno. Zato etika predstavlja proces takvog djelovanja. Etička pitanja postavljaju temelje za opravdano djelovanje te se pomoću nje promišljaju moralni činovi da bi se vidjelo kakva je uopće prava čovjekova moralnost. Stoga se važnost etike očituje u traganju za ispravnom odlukom, a to je odluka koja se može opravdati i iza koje čovjek odgovorno stoji. Svojim djelovanjem čovjek redovito postiže uspjeh ili neuspjeh i ne postoje situacije u kojima je ljudsko ponašanje definirano određenim pravilima. Zato je smisao etike moralnost ljudskih postupaka. Tu je najvažnije etičko pitanje što, zašto i kako nešto učiniti, a da se to učini pravedno, moralno i odgovorno. Zato je primjena etike važna jer je bitno zašto nešto činiti dobro i po čemu će to dobro biti zaista dobro. Stoga realizacija etičkih i moralnih vrijednosti dolazi u obzir samo ako ju čovjek prihvaća i ako djeluje zbog nje same.

Iz cijele takve kompleksnosti etike razvila se poslovna etika. Ona podrazumijeva primjenu etičkih principa u poslovnim odnosima i aktivnostima s tim da mnoga poduzeća imaju u pisanom obliku formalne etičke kodove (Bebek, 2005.). Ključno pitanje poslovne etike jest da li se zaposlenici pridržavaju etičkih principa ili ne. Ono što je potrebno i čega bi se ljudi trebali pridržavati jest upravo poslovna etika. Tako se poslovna etika može okarakterizirati kao primjena etičkih vrijednosti u poslovnoj praksi te obuhvaća sve elemente etičkog ponašanja u poslovanju. Prema Weihrichu i Koontzu, glavne karakteristike poslovne etike su istinitost i pravednost (Weihrich i Koontz, 2005.), a to su aspekti koje društvo očekuje od ponašanja čovjeka.

Poslovna etika je, dakle, način koncipiranja, sklapanja, komuniciranja i izvođenja poslova u istovremenom skladu s duhovnim, sociološkim, biološkim i prirodnim zakonitostima čovjeka i okruženja (Bebek, 2005.). Adam Smith, kao jedan od najznačajnijih ekonomista u povijesti, smatra da je svaki autentični gospodarski potez onaj koji u skladu s prirodom pridonosi realizaciji poslovnih interesa kao subjekta tog sustava koji proizvodi posao. Bit je poslovne etike da ona istražuje sudove i odlučivanje u gospodarstvu te ciljeve kojima će se etički i racionalno djelovati.

Velik dio poslovanja u suvremenom društvu obavlja se za novac pa poslovna etika objašnjava poslovanje tržišta – znači da ljudi u svome poslovnom djelovanju razmjenjuju svoj rad za ugled, društveni status i samospoznaju da čine dobro i za društvo i za svoju organizaciju. Zato je poslovna etika vezana uz interakciju koja ima za svrhu uspješno obaviti zadatak, ali i obaviti zadatak tako da druga strana kompenzira neku našu potrebu. Stoga poslovna etika zahtijeva dvostruko zadovoljavanje ciljeva i potreba.

Etika se u poslovnom svijetu primjenjuje kao znanost o pravilnom postupanju čovjeka koji posluje kada se radi o egzistencijalnim pitanjima. Ovdje orijentacija na ekonomske motive nije dovoljna, već se mora uzeti u obzir i moralna komponenta karakternih osobina čovjeka. Zato se tu radi o individualnoj etici jer se vodi briga o potrebi svakog čovjeka pojedinačno. Čovjek koji posluje mora poslovati odgovorno, zato je poslovna etika i etika odgovornosti, gdje postupati etički znači slijediti svoju savjest.

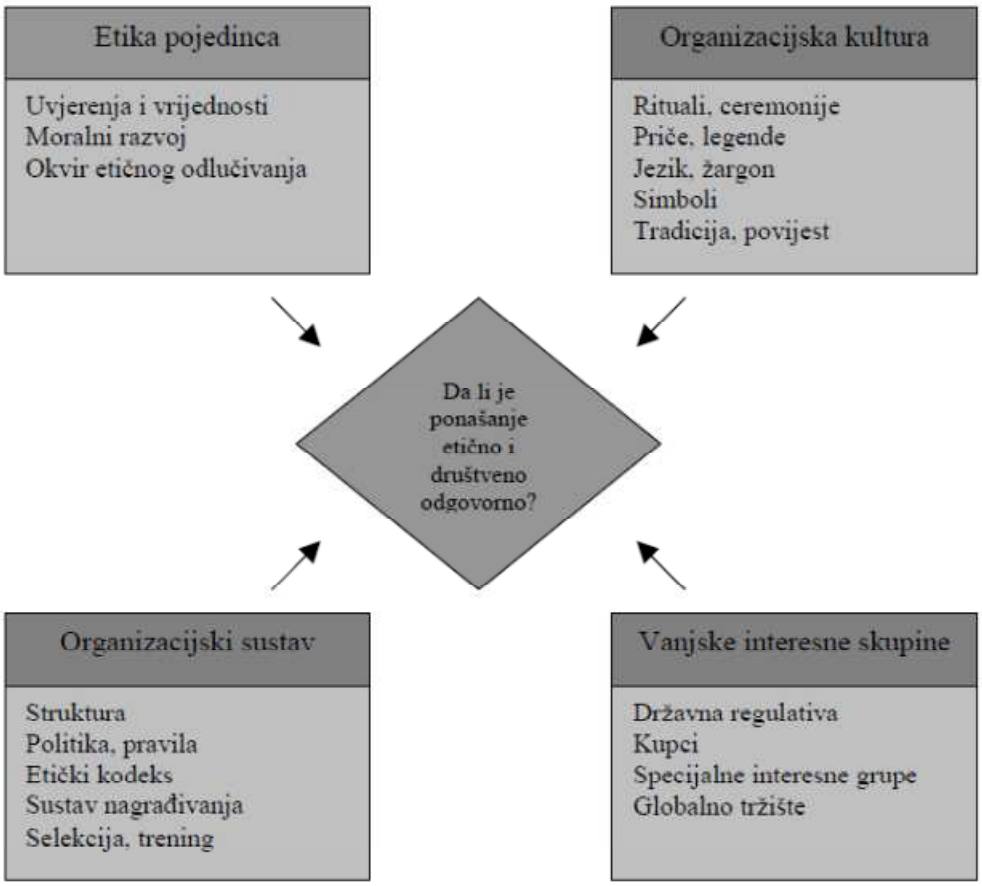
Uzimajući u obzir razrađeni sistematski pristup poslovnoj etici, moguće je razlučiti određene zahtjeve koje postavlja elementarna poslovna etika. U tim zahtjevima glavnu ulogu ima subjekt poslovne etike, a to je nositelj moralne dužnosti ili odgovornosti u poslovanju. Zahtjevi subjekta poslovne etike su sljedeći (Bebek, 2005.):

- Da subjekt po horizontali obavlja onu funkciju po vrsti u kojoj ima komparativnu prednost,
- Da subjekt funkciju u kojoj ima komparativnu prednost izvršava na onoj razini po vertikali koja mu ontološki pripada,
- Da subjekt radi onu vrstu posla, onoliko dugo i u takvo vrijeme koje odgovara prirodi samoga posla.

Danas su u poslovnoj etici najvažniji interesi pojedinca. Prioriteti pojedinca su tako samosvijest, samoopredjeljenje i samoodržavanje. Ako netko želi biti etičan u poslovanju, on mora znati ostvariti interakciju na način da obje strane budu zadovoljne njegovim

djelovanjem. Zato u etičko djelovanje treba ulagati međusobno poštenje i motivaciju za rad, da bi se postiglo uspješno i moralno djelovanje.

Slika 1. Faktori koji utječu na etičko ponašanje organizacije



Izvor: Aleksić, A.: Poslovna etika – element uspješnog poslovanja, Zbornik ekonomskog fakulteta u Zagrebu, Vol. 5, No. 1, prosinac 2007., str. 422

Standardi za etičko i odgovorno poštovanje uključeni su u karakter svakoga pojedinca te njegovi stavovi, norme i uvjerenja utječu na poslovnu okolinu u kojoj se nalazi. Slika 1. prikazuje kako etika pojedinca, organizacijska kultura, organizacijski sustav i vanjske interesne skupine utječu na etičko ponašanje neke organizacije. Sve su to faktori koji utječu na organizaciju, oblikujući njenu poslovnu etiku, koja mora biti temeljena na moralnom djelovanju svakog pojedinca zasebno. Tako svi navedeni faktori utječu na standarde etičnosti neke organizacije.

Danas u konkurentskoj areni poslovna etika omogućuje osobni rast i razvoj te povećava efikasnost i produktivnost (Aleksić, 2007.). Poslovno okruženje u kojem su ljudi etični i izvršavaju svoje obveze časno je ekonomski efikasno i smanjuje troškove rizika. Stoga se

može zaključiti da poslovna etika ima interdisciplinarni karakter te da ekonomsku praksu spaja s politikom, a sve je skupa utemeljeno na filozofiji.

Poslovna etika temelji svoje koncepte na određenim vrijednostima koje obuhvaćaju različite stavove i norme. U poslovnoj etici svaki pojedinac posjeduje određene vrijednosti koje upravljaju njihovim emocijama i odlukama, a ti pojedinci toga ponekad nisu ni svjesni. Iz vrijednosti poslovne etike izvode se norme koje čine temelj za donošenje etičkih odluka. Te vrijednosti su uglavnom univerzalne, ali i relativne. Tako univerzalne vrijednosti imaju opće ljudske značajke i nalaze se u čovjekovoj prirodi, dok relativne vrijednosti imaju korijene u kulturi i načinu života svakoga čovjeka (Pupovac, 2006.).

Tako svaka poslovna organizacija ima svoje vrijednosti te se fokusira na one koje joj donose ostanak i vodeći tržišni položaj, a te svoje vrijednosti ona povezuje u jedinstven vrijednosni sustav. Te vrijednosti pružaju dostojanstvo u odnosu među zaposlenicima, ali i u njihovu odnosu s nadređenima te svima zajedno omogućuju egzistenciju i poštivanje osobnosti svakog pojedinca individualno u organizaciji. Tako se vrijednosti poslovne etike izražavaju putem normi koje sadrže i poštuju sve poslovne organizacije, a upravo su te vrijednosti bit etičkih sudova u poslovnoj etici.

Sukladno svemu navedenome, može se zaključiti da se poslovna etika temelji na istinitosti, pravednosti i moralnoj savjesti te je kao takva nezamjenjiva komponenta svake organizacije i sredine u kojoj neki čovjek djeluje na etičan i moralan način.

3.2. Primjena etike u poslovanju

U današnjem ubrzanom poslovnom svijetu je etičko poslovanje moral koji predstavlja temelj poslovanja i organizacijske kulture svake organizacije. U etičkom poslovanju treba primjenjivati, kako je ranije navedeno, istinitost i pravednost te se mora tim vrlinama prilagođavati uvjetima globalnog poslovanja.

Etičko poslovanje sastoji se od niza normi i moralnih pravila koji usmjeravaju ponašanje čovjeka u odnosu na druge. Primjena etike u poslovanju je povezana s pravednošću i smišljeno donesenim odlukama što je dobro, a što nije. Također, sukladno etičkom poslovanju, trebaju se poduzimati one poslovne aktivnosti koje će imati moralnu komponentu. Zato je potrebno da etika poslovanja postane cilj poduzeća i da uključi sve koji u njemu rade.

Kod primjene etike u poslovanju mora se djelovati ispravno, a to djelovanje mora biti temeljeno na etičkim načelima. Zato je etika nužna sastavnica poslovanja u svakoj organizaciji. Poduzeće treba sadržavati etička pravila koja mora primjenjivati dugoročno te treba poticati svoje zaposlenike da ta pravila poštuju te da se ponašaju moralno i savjesno jer se dobar glas poduzeća postiže samo poštenim i moralnim radom uz znatna odricanja, a tako teško izgrađeni dobar glas se može vrlo lako prokockati jednom pogrešnom odlukom (Karpati, 2001.).

Etika u poslovanju mora obuhvatiti svakoga pojedinačno te se mora primjenjivati u svakoj poslovnoj situaciji. Etičkim poslovanjem se poduzeće prepoznaje na tržištu kao dobro i ugledno, a samim time privlači i zaposlenike koji su sličnih osobina. Na taj način se stvara poslovno okruženje gdje su ljudi časni i moralni te odgovorno izvršavaju svoje obveze.

U etici poslovanja to poslovanje mora biti obilježeno poštenjem te se mora u njega uložiti golema etička energija da bi se moglo djelovati u svrhu promicanja moralnih vrijednosti. Etičko ponašanje u poslovanju diktirano je osobinama pojedinaca koji posluju u određenoj organizaciji te je stoga potrebno da ti pojedinci posjeduju temeljne etičke i moralne karakterne osobine.

Glavnu odgovornost u primjeni etike u poslovanju ima rukovoditelj koji mora ukazati zaposlenicima na postojanje etičkih problema i načine kako se s njima nositi. Zato se u organizaciji i definira postojanje etičkog kodeksa koji može pomoći zaposlenicima da postanu uzor jedni drugima. Zato je poslovnu etiku potrebno kontinuirano učiti i usavršavati jer se na taj način ljudi potiču na razmišljanje i snalaženje. Tako oni mogu formirati vlastite moralne stavove koje mogu primijeniti u određenim poslovnim situacijama – na taj način će postati sposobniji da se nose sa kritičnim situacijama u kojima se nađu.

U primjeni etike u poslovanju bitno je postojanje svjesnosti u donošenju neke odluke jer je time osoba koja donosi odluku odgovorna za njenu implementaciju. Zato se prvo trebaju procijeniti etičke vrijednosti, pratiti etičko ponašanje ljudi u okruženju te ukoliko se pojave slučajevi povrede etike, treba ih znati riješiti. Međutim, osobi koja donosi odluku može biti teško primjenjivati takav koncept etike. U tom slučaju treba uspostaviti dobar odnos sa onima koje odluka uključuje, jer se zajednički problem etičkih pitanja može učinkovitije riješiti.

Etično će se poslovati u onoj organizaciji koja ima usvojen etički kodeks – on je garancija etičkog poslovanja jer njegovo postojanje jednostavno primorava zaposlenike da ga poštuju. Na taj način postoje temeljne vrijednosti i norme koje treba poštivati. Stoga prihvaćanje

etičkog kodeksa znači prihvaćanje minimalnih standarda u upravljanju etikom. U organizaciji se moraju razviti strategije koje će osigurati da etičke standarde provode svi u organizaciji. Zato se od svakog čovjeka očekuje ne samo provođenje, već i poticanje ostalih na etičko ponašanje u poslovanju.

Ljudi moraju primjenjivati etičke vrijednosti, ali moraju ostati i vjerni svojim etičkim stavovima, međutim, oni moraju biti usklađeni sa vrijednostima poduzeća u kojem rade. Djelatnici moraju zajednički provoditi etička načela te se suočavati sa kriznim etičkim situacijama jer na taj način razvijaju zajedničku etičku savjest. Zato je najvažniji preduvjet za etičko poslovanje postojanje svijesti o provedbi nekih aktivnosti i njezine etičnosti.

Konačno, poslovna etika mora se primjenjivati jer je ona element uspješnog poslovanja. Organizacija mora imati usvojene vlastite moralne vrijednosti, ali ih i mora znati uskladiti sa moralnim vrijednostima društva. Poduzeća koja u svoj sustav imaju inkorporiranu poslovnu etiku bit će uspješnija i prepoznatljivija od ostalih te će pokazati bolje poslovne rezultate. Zato uvođenje etike u poslovanje omogućava svim sudionicima da djeluju moralno i savjesno, te da odgovorno izvršavaju svoje obveze. To omogućuje organizaciji primjenu jedinstvenog procesa upravljanja, jer zaposlenici koji poštuju etički kodeks doprinose odgovornom poslovanju i učinkovitom ostvarenju rezultata poslovanja. Ako se uvede poslovna etika u poduzeće, poboljšat će se zadovoljstvo zaposlenika, osigurat će se stabilan razvoj poduzeća te će isti zaposlenici radije ostati u tom poduzeću nego izabrati neko drugo. Stoga se može reći da primjena etike u poslovanju povećava vrijednost same organizacije te ona postaje poželjan partner i suradnik onima koji su za nju zainteresirani.

3.3. Moralno stajalište poslovne etike prema računalnom kriminalu

Tvrtke vođene politikom raznolikosti imaju izvrsne izglede za rast na globalnoj sceni, tako da ima smisla implementirati raznolikost u gotovo sve poslovne aktivnosti. Raznolikost dolazi s izazovima, od nedostataka generacija, komunikacije do etike na radnom mjestu. Da bismo bili etični, donosimo moralni izbor da poštujemo ljude i imovinu, igramo se po pravilima i pridržavamo se zakona. Ništa se ne razlikuje od bilo koje druge vrste etike - cyber etike. Sigurnost je najrazornije etičko pitanje svakog pojedinca i organizacije. Ključna je zaštita računala i ručnih uređaja od virusa i hakera.

Cyber kriminal sa stajališta poslovne etike predstavlja kriminalne aktivnosti koje se vrše pomoću računala i interneta, a koje su same po sebi neetične te moralno neprihvatljive sa stajališta poduzeća koje posluje i koje predstavlja računalnim napadačima žrtvu kojoj će biti nanesena velika materijalna, financijska ili informacijska šteta računalnim napadom na poduzeće. To uključuje sve, od preuzimanja ilegalnih glazbenih datoteka do krađe milijuna dolara s mrežnih bankovnih računa. Cyber kriminal uključuje i novčana kaznena djela, poput stvaranja i distribucije virusa na drugim računalima ili objavljivanja povjerljivih poslovnih informacija na Internetu.

Najistaknutiji oblik cyber-kriminala je krađa identiteta, u kojoj kriminalci koriste Internet za krađu osobnih podataka od drugih korisnika. Dva najčešća načina da se to postigne je phishing i pharming. Obje ove metode povlače korisnike na lažne web stranice (koje izgledaju zakonito), gdje se od njih traži da unose osobne podatke. To uključuje podatke za prijavu, kao što su korisnička imena i lozinke, telefonski brojevi, adrese, brojevi kreditnih kartica, brojevi bankovnih računa i druge informacije koje kriminalci mogu upotrijebiti za "krađu" identiteta druge osobe. Iz tog razloga prije unošenja svojih osobnih podataka poduzeća uvijek trebaju provjeriti URL ili web adresu web mjesta kako bi bili sigurni da je zakonita. Nadalje, pametno se zaštititi korištenjem softvera za blokiranje antivirusa i špijunskog softvera i biti oprezan gdje unosite svoje osobne podatke.

Koristeći ništa drugo osim savršeno legalnih tehnika, svaka tvrtka može sebi priuštiti zaštitu od računalnih napada te tako spriječiti potencijalnu štetu koju joj mogu nanijeti računalni kriminalci. Svako poduzeće koje nastupa na tržištu, kako zauzima stav prema tržišnom natjecanju u konkurenciji, gdje mora vladati poštena konkurentna utrka na tržištu te poslovanje mora biti pošteno i u skladu sa zakonom, isti stavovi su i prema računalnom kriminalu. Stav je poslovnih poduzeća univerzalan te se također prema računalnom kriminalu odnosi sa negativnog, odnosno osuđujućeg stajališta.

Svako poduzeće je svjesno koliko može imati negativnih posljedica računalnim napadom te je stav poduzeća prema takvim osobama u principu negativan, odnosno dvosmisleno korektan u smislu osuđivanja takvih postupaka gdje se svjesno i namjerno nanosi materijalna šteta i ugroza njegovu poslovanju.

Poduzeća su mišljenja i stajališta o upitno moralnom karakteru takvih osoba koje na ilegalan način vrše virtualnu krađu, svjesni činjenice da posjeduju specijalizirana znanja i vještine koje im omogućuju takav vid krađe, kao i svijesti da je njihov identitet teško otkriti.

Takvo ponašanje, koje podliježe kaznenom djelu i kriminološkoj obradi, je u principu osuđujuće i neetično prema poslovanju. Ono spada u domenu neetičnosti poslovanja te je dio negativnih izazova za poduzeće koji dolaze sa tržišta. Poduzeće time postaje ugroženo pa je i očekivano da prema računalnom kriminalu zauzima stav koji je nemoralan, ima elemente zlobnosti, nemoralnih vrijednosti poput patoloških stanja ličnosti osoba koje to rade i slično.

Stoga svako poduzeće slijedi pravila poslovne etike gdje poslovanje mora biti legalno, pošteno i transparentno. U tom smislu, i sam računalni kriminal je osuđujući i opasan za poslovanje svakog poduzeća jer ga direktno ugrožava i nanosi mu štetu koju je kasnije teško nadoknaditi.

4. RAČUNALNI KRIMINAL I UTJECAJ NA POSLOVANJE

Računalni kriminal je u suvremenom poslovanju u 21. stoljeću, sa snažnim razvojem IT tehnologija, u porastu među tvrtkama i to ih skupo košta. Tako računalni kriminal uključuje bezbroj zlokobnih kriminalnih praksi namijenjenih narušavanju računalne sigurnosti tvrtke. Svrha elektroničkog prekida i ulaska može biti ukrasti financijske podatke tvrtke ili njegovih kupaca, uskratiti uslugu na web mjestu tvrtke ili instalirati virus koji u budućnosti nadzire internetsku aktivnost tvrtke. Sva poduzeća koja posluju putem interneta moraju se na jedan ili drugi način suočiti sa cyber kriminalom. Nacionalnim istraživanjem računalne sigurnosti (NCSS) iz 2005. utvrđeno je da je 67% anketiranih tvrtki otkrilo barem jedan oblik računalnog kriminala (Investopedia, 2020.). Borba protiv računalnog kriminala je skupa i uvijek se mora razvijati kako nastaju nove prijetnje i metode. Stoga će u ovom poglavlju biti riječi o utjecaju računalnog kriminala na poslovanje u 21. stoljeću sa dva opisana apliaktivna primjera, koja uključuju WikiLeaks te napade svjetski poznatih hackera na svjetske dioničke burze i financijske institucije.

4.1. Metode utjecaja na suvremeno poslovanje

Danas je utjecaj računalnog kriminala na suvremeno poslovanje eksponencijalan. Poslovanje mnogih tvrtki, od malih poduzeća do velikih kompanija je postalo globalno i kao takvo postaje prilagodljivo suvremenim trendovima razvoja IT tehnologija. Danas nema poduzeća koje u svom poslovanju ne primjenjuje računalne sustave. A sa njihovom implementacijom sama narav primjene IT tehnologije u svom poslovanju zahtijeva zaštitu poslovnih podataka, tajni, financijskih sredstava, računa u bankama, poslovnih transakcija i svih drugih poslovnih operacija koje se poduzimaju u redovnom poslovanju.

Prisutnost računalnog kriminala je prisutna u svim oblicima na Internetu te je usmjerena prema fizičkim i pravnim osobama u različitim tipologijama napada na pojedince i poduzeća. U smislu napada na poslovanje tvrtki metode su specifične i uključuju brojne metode napada. Tvrtke koje se žele zaštititi od internih lopova moraju znati raspolagati svojim novčanim sredstvima kako bi to učinile. Troškovi su identificiranja rizika, izgradnje novih i sigurnijih operativnih postupaka, te kupovine zaštitnog softvera i hardvera. Za tvrtke sa složenim ili

osjetljivim operacijama to često uključuje angažiranje savjetnika za cyber-sigurnost za izradu prilagođenog rješenja.

Ne samo da su skupi troškovi zaštite, već se sustavi moraju redovito testirati i nadzirati kako bi se osiguralo da su još uvijek učinkoviti protiv novih cyber napada. Ti se troškovi često prenose na kupca putem viših cijena robe i usluga. Računalni kriminal stoga više nije samo za hackere koji napadaju poduzeća. U posljednjih nekoliko godina pojavila se nova subkultura: cyber-aktivist. To su internetski ekvivalenti prosvjednika koji vrše prosvjede na ulicama iz različitih razloga. Njihova je svrha isključivanje mrežnih operacija tvrtke kako bi se poslala poruka o poslovnoj praksi tvrtke (Investopedia, 2020.). U posljednje dvije godine na ovaj način su napadnute velike korporacije, poput PayPala i MasterCarda. U prosincu 2010., web mjesto PayPal napale su desetine ljudi koji su tvrdili da su dio grupe, Anonymous. Pokušali su izvršiti napad za odbijanje usluge u znak odmazde za PayPal gašenje usluga plaćanja putem WikiLeaksa (Investopedia, 2020.). U tom zločinu je uhićeno više desetina hakera. Iako PayPal nije doživio potpuno zatvaranje, mnoge druge tvrtke nisu toliko dobro prošle prilikom napada na njihovo poslovanje (Investopedia, 2020.). Odbijanje napada rezultira manjom prodajom jer kupci ne mogu pristupiti internetskoj trgovini tvrtke. To čak može rezultirati manjim prihodom dugoročno ako se neki kupci odluče više ne poslovati s tvrtkom koja je ranjiva za napad. Računalni kriminal može utjecati na poduzeća više nego samo na financijske načine. Tvrtke moraju preispitati na koji način prikupljaju i pohranjuju informacije kako bi osigurale da osjetljive informacije nisu ranjive. Mnoge tvrtke prestale su pohranjivati financijske i osobne podatke kupaca, poput brojeva kreditnih kartica, brojeva socijalnog osiguranja i datuma rođenja. Neke tvrtke zatvorile su svoje internetske trgovine iz zabrinutosti da se ne mogu adekvatno zaštititi od krađe uzrokovane računalnim kriminalom. Kupce je također više zanimalo kako tvrtke koje se bave sigurnosnim pitanjima primjenjuju zaštitu od računalnog kriminala. Uspješan računalni napad može nanijeti veliku štetu poslu tvrtke. To može utjecati na njezinu konačnu vrijednost, kao i na stanje njenog poslovanja i povjerenje potrošača. Učinak kršenja sigurnosti može se široko podijeliti u tri kategorije: financijsku, reputacijsku i pravnu.

Ekonomski trošak računalnog napada je prioritetni i najviše vidljiv. Računalni napadi često rezultiraju znatnim financijskim gubicima koji proizlaze iz: krađa korporativnih podataka krađa financijskih podataka (npr. bankovni podaci ili podaci o platnoj kartici), krađa novca i ometanje trgovanja (npr. nemogućnost obavljanja transakcija na mreži), gubitak posla ili

ugovora sa poslovnim partnerima. Tvrtke koje su pretrpjele kibernetsko kršenje također će uglavnom imati troškove povezane sa popravkom pogođenih sustava, mreža i uređaja.

Povjerenje je bitan element odnosa s kupcima. Računalni napadi mogu naštetiti ugledu napadnute tvrtke i urušiti povjerenje klijenata u nju. Na primjer, podvala hackera i bankovni sustav banke te krađa novca sa računa klijenata, unatoč jamstvu banke da će novac vratiti, može uzrokovati gubitak mnogih klijenata te odabir druge banke uz objašnjenje i sumnju kako sigurnosni sustav predmetne banke nije bio dovoljno osiguran od napada pa su klijenti ostali bez svog novca, oteta im je lozinka, korišten je njihov novac za brojne transakcije i slično.To bi zauzvrat moglo dovesti do gubitka kupaca, gubitka prodaje, smanjenja profita i sličnih gubitaka koji su primarno financijske prirode, a odražavaju se na poslovanje poduzeća uzrokujući da isto počne poslovati s gubicima, kako financijskim, tako i gubicima klijenata. Učinak oštećenja reputacije može čak utjecati na dobavljače ili utjecati na odnose s partnerima, investitorima i drugim trećim stranama u poslovanju tvrtki. Računalni napadi na tvrtke i njihovo poslovanje stoga mogu biti pogubni. Sve je ovisno kolika je snaga napada, koliko je štete naneseno te koliko je tvrtka poznata i da li je situacija računalnog napada poznata klijentima. Mogu se dogoditi situacije samo krađe određenih poslovnih informacija tvrtki za koje klijenti ne moraju ni znati te tvrtke takve situacije rješavaju internim strategijama. Međutim, ukoliko dođe do računalnog napada koji rezultira krađom financijskih sredstava, krađom identiteta, oštećenjem klijenata i dobavljača te drugih tada tvrtke mogu imati pogubne posljedice za svoje poslovanje jer mogu otići u stečaj zbog gubitka i financija, i poslovnog uspjeha, ali i povjerenja klijenata, poslovnih partnera i investitora.

Stoga je računalni kriminal opasna tenzija koja negativno utječe na suvremeno poslovanje i veliki je izazov tvrtkama koje posluju globalno. Takve tvrtke trebaju primarno poraditi na prioritetnoj i snažnoj računalnoj zaštiti svojih informacijskih sustava da bi spriječile računalne napade i opstale u snažnom konkurentnom poslovnom svijetu.

4.2. WikiLeaks – organizacija računalnog kriminala

WikiLeaks je međunarodna neprofitna organizacija koja objavljuje vijesti i klasificirane medije koje pružaju anonimni izvori (Wikileaks.info, 2020.). Njegova web stranica, koju je na Islandu pokrenula 2006. godine organizacija Sunshine Press, tvrdi da je 2015. objavila na internetu 10 milijuna dokumenata u prvih 10 godina. Julian Assange, australijski internetski

aktivist, općenito je opisan kao njegov osnivač i direktor. Od rujna 2018. godine Kristinn Hrafnsson obnaša dužnost svoje glavne urednice. Grupa je objavila brojne ugledne predmemorije dokumenata. Rana izdanja uključivala su dokumentaciju troškova i opreme u ratu u Afganistanu, izvješće o istrazi korupcije u Keniji i priručnik za operacije u američkom zatvoru u zaljevu Guantanamo, na Kubi. U travnju 2010., WikiLeaks je objavio snimke Collateral Murder od zrakoplova Bagdada 12. srpnja 2007. u kojem su među ubijenim bili irački novinari (WikiLeaks, 2020.). Ostala izdanja u 2010. godini uključivala su Afganistanski ratni dnevnik i „Iračke ratne dnevnike“. Potonje je omogućilo mapiranje 109.032 smrtnih slučajeva u "značajnim" napadima pobunjenika na Irak koji su prijavljeni Multi-National Force - Irak, uključujući oko 15.000 koji prethodno nisu objavljeni.

2010. godine WikiLeaks je objavio i diplomatske dokumente američkog State Departmenta, klasificirane dokumente koji su poslani u State Department. U travnju 2011. godine WikiLeaks je počeo objavljivati 779 tajnih dosijea koji se odnose na zatvorenike zatvorene u logoru Guantanamo Bay. 2012. godine WikiLeaks je objavio "Sirijske dosjee", preko dva milijuna e-mailova koje su poslali sirijski političari, ukazujući na korporacije i vladina ministarstva (WikiLeaks, 2020.).

2015. godine WikiLeaks je objavio diplomatske kanale Saudijske Arabije, dokumente koji detaljno navode špijuniranje američke Agencije za nacionalnu sigurnost za uzastopnim francuskim predsjednicima i poglavlje o intelektualnom vlasništvu Trans-pacifičkog partnerstva, odnosno kontroverzno međunarodni trgovinski sporazum koji je pregovaran u tajnosti. Tijekom kampanje za predsjedničke izbore u SAD-u 2016. godine WikiLeaks je objavio e-mailove i druge dokumente Demokratskog nacionalnog odbora i voditelja kampanje Hillary Clinton, Johna Podesta. Ta su izdanja nanijela značajnu štetu Clintonovoj kampanji i pripisana su kao potencijalni faktor njezinog gubitka. Američka obavještajna zajednica izrazila je "veliko povjerenje" da je procurjelu e-poštu Rusija hakirala i dostavila WikiLeaksu, dok je WikiLeaks negirao da je njihov izvor Rusija ili bilo koja druga država. Tijekom kampanje WikiLeaks je promicao teorije zavjere o Hillary Clinton i Demokratskoj stranci. Tijekom 2016. godine WikiLeaks je objavio gotovo 300.000 e - poruka koje je opisao kao da stižu iz turske vladajuće Stranke pravde i razvoja, a za koje je kasnije utvrđeno da su uzeti iz javnih arhiva pošte, i preko 50.000 e - mailova od turskog ministra energije. 2017. godine WikiLeaks je objavio interne CIA dokumente koji opisuju alate koje agencija koristi za hakiranje uređaja, uključujući mobilne telefone i usmjerivače.



Slika 3. Logo WikiLeaksa

Izvor: WikiLeaks (2020): Corporations, www.wikileaks.org, pristupljeno 13.08.2020.

WikiLeaks je izvukao kritiku zbog njegove navodne odsutnosti zviždanja ili kritike Rusije i zbog kritiziranja izloženosti poduzeća i pojedinaca s Panama Papers, koji imaju offshore bankovne račune. Organizaciju su također kritizirale zbog neprimjerenog prilagođavanja sadržaja i povrede osobne privatnosti pojedinaca. WikiLeaks je, primjerice, otkrio brojeve socijalnog osiguranja, medicinske podatke, brojeve kreditnih kartica i detalje pokušaja. Navedene aktivnosti WikiLeaksa imaju karakteristike neprofitne organizacije koja je usmjerena na računalne napade svjetskih javnih institucija s namjerom krađe tajnih podataka sumnjive prirode, korupcije i malverzacija za koje WikiLeaks smatra da javnost treba znati. Oni u tom smislu kontinuirano poduzimaju računalni kriminal koji ne rezultira financijskim štetama po javne institucije, ali ruši ugled i reputaciju ovih institucija u javnosti. Iako je objava njihovih dokumenata činjenično nevjerodostojna, ova organizacija ipak prakticira dio računalnog kriminala putem kojeg dolazi do tajnih informacija država i javnih institucija o suspektnim malverzacijama koje su upitne problematike u smislu vjerodostojnosti. WikiLeaks organizacija je sama po sebi kontroverzna organizacija i predmet je svjetske kriminološke obrade. Njezina djela se tretiraju kao kaznena djela računalnog kriminala te je često podložna brojnim kriminološkim istragama, gašenju web stranice, privođenju njihovih aktivista i hackera, različitim novčanim kaznama, a sam osnivač Julian Assange je bjegunac pred zakonom i državnim potjerama jer je osuđivan za svoja kaznena zlodjela računalnog kriminala. Stoga je ova organizacija najmjerodavniji primjer računalnog kriminala globalne javne prepoznatljivosti i indikativan je primjer kako se ponašaju hackeri u računalnim napadima na važne državne institucije.

4.3. Hakerski napadi na svjetske burze i financijske institucije

Hakerski napadi na svjetski poznate tvrtke su učestali i svakodnevni. Bitno je izdvojiti snažan primjer takvog napada da bi se uvidio utjecaj računalnog kriminala na suvremeno poslovanje. Stoga je odabran primjer dva značajna ruska hackera koji su dugo vremena napadali svjetske dioničke burze, poput Nasdaqa i Londonske burze, te svjetske javne institucije, poput Svjetske banke. Dva ruska državljanina osuđena su u zatvoru zbog zavjere o masovnim kršenjima podataka. Hakeri su usmjereni na velike procese plaćanja, maloprodaje i financijske institucije širom svijeta. Dvojica ruskih državljana osuđena su na kazne saveznog zatvora zbog svojih uloga u svjetskom sustavu hakiranja i kršenja podataka koji su ciljali na velike korporativne mreže, kompromitirali 160 milijuna brojeva kreditnih kartica i rezultirali gubicima od stotine milijuna dolara - jednim od najvećih takvih shema ikada procesuirane u Sjedinjenim Državama (Justice.gov, 2018.). Kazne su odredili vršilac dužnosti glavnog tužitelja John P. Cronan iz Kaznenog odjela Ministarstva pravosuđa, prvi pomoćnik američkog odvjetnika William E. Fitzpatrick iz okruga New Jersey i direktor Randolph D. Alles iz američke tajne službe. Vladimir Drinkman (37) iz Syktyvkara i Moskve u Rusiji osuđen je na 144 mjeseca zatvora. Drinkman se prije izjasnio krivim pred američkim okružnim sucem Jeromeom B. Simandleom iz okruga New Jersey po jednoj točki zavjere za počinjenje neovlaštenog pristupa zaštićenim računalima i jednoj točki zavjere za počinjenje prijevara na način koji utječe na financijsku instituciju. Dmitrij Smilianets (34) iz Moskve, ranije se izjasnio krivim za zavjeru u svrhu izvršenja prijevara na način koji utječe na financijsku instituciju i osuđen je na 51 mjesec i 21 dan zatvora. Obojica su priznali krivnju u rujnu 2015. pred sucem Simandleom, koji je izrekao kazne na Camdenu, saveznom sudu u New Jerseyju. Uz zatvorske kazne, sudac Simandle je Drinkmana osudio na tri godine pod nadzorom puštanja na slobodu, a Smilianets na pet godina nadzora. Drinkman i Smilianets uhićeni su u Nizozemskoj 28. lipnja 2012. godine (Justice.gov, 2018.). Drinkman je izručen distriktu New Jersey 17. veljače 2015., a Smilianets je izručen 7. rujna 2012. "Drinkman i Smilianets nisu samo ukrali više od 160 milijuna brojeva kreditnih kartica od prerađivača kreditnih kartica, banaka, trgovaca i drugih korporativnih žrtava, već su i koristili svoje bogatstvo za podsticanje snažnog podzemnog tržišta za hakirane podatke (Justice.gov, 2020.) Dok velika kršenja računalnog kriminala poput ovog i dalje utječu na milijune pojedinaca

širom svijeta, hakeri i potencijalni hakeri trebali bi znati da će Ministarstvo pravosuđa upotrijebiti sve dostupne alate za prepoznavanje, uhićenje i progon svih koji napadnu mreže na koje tvrtke i klijenti se pouzdaju. Ovaj primjer ukazuje na činjenicu kako vrlo sposobni educirani hakeri mogu biti u stanju napasti svjetske financijske institucije i burze, uzrokujući velike financijske štete, krađu osobnih podataka, identiteta i drugih brojnih posljedica koje rezultiraju negativno na suvremeno poslovanje.

5. ZAKLJUČAK

U suvremenom svijetu globalnog poslovanja nema poduzeća i pojedinca koji nema pristup Internetu. Kao takvi, mnogi primjenjuju računalne sustave za osobne i poslovne potrebe. Poduzeća danas posluju na globalnoj razini i nema više tvrtke, od malih poduzeća do globalnih svjetskih kompanija, koje u svom poslovanju ne primjenjuju računalne sustave koji im uvelike olakšavaju učinkovitost poslovanja. Računalni kriminal je danas prisutan u cijelom svijetu na fizičkoj razini, a na virtualnoj u svakom kutku gdje je dostupan Internet. To je ilegalni akt vršenja napada na računalne sustave poduzeća i pojedinaca s ciljem krađe podataka, financijskih sredstava, identiteta, lozinki i drugih metoda svjesnog nanošenja štete, uslijed čega nastaju posljedice u poslovanju u vidu smanjenja profitabilnosti, gubitka klijenata, dobavljača, poslovnih partnera i investitora, ali i velikog pada reputacije tvrtki u očima javnosti. Danas se stoga sve veći broj poduzeća diljem svijeta susreće s nekim od oblika računalnog kriminala što ne začuđuje s obzirom da baš svako poduzeće posjeduje jedno ili više računala. U tom posjedovanju nužnost je primjena zaštite od računalnog kriminala jer se sve više javlja pitanje problematike sigurnosti od napada istoga. Povijest računalnog kriminaliteta ima svoje korijene u razvoju sustava računala još u Indiji i Africi gdje su se primati računala nazivali abakus, a već tada su se primjenjivale metode kriminala i prijevare primjerene toj povijesnoj dobi. Međutim, računalni kriminal se počeo snažno razvijati 1980 – tih godina, gdje se primarno odnosio na napade samo na svjetski važne institucije jer su samo iste tada imale pristup Internetu. Kako je Internet postao globalna pojava koju danas koristi svatko, ta kategorija je danas dobila jedan čvrsti suvremeni okvir, s tim da su se usavršile metode računalnih napada kao na primjer hakerstvo i računalna prijevara.

U suvremenom poslovanju, kao i progresivnim razvojem IT tehnologija uočen je značajan porast računalnih prijevara i računalnog krivotvorenja u poslovanju brojnih svjetskih poduzeća. Danas se primjenjuju brojne metode računalnog kriminala u poslovanju poduzeća, od kojih su najčešće provale u računalne sustave tvrtki sa ciljem krađe poslovnih podataka, lozinki i financijskih sredstava Danas opće priznat tzv. "Tallinnski priručnik" koji pruža smjernice državama u provođenju međunarodnih politika po pitanju računalnog kriminaliteta. Posljedice koje ostavlja računalni kriminalitet sve više su nesagledive. Došlo se do spoznaje da je godišnja potrošnja za prevenciju računalnog kriminaliteta iznosi 600 milijardi dolara godišnje. Najviše stradavaju kompanije i nacionalne ekonomije te istovremeno to šteti trgovini, kompetitivnosti, inovacijama i globalnom ekonomskom rastu.
Kršenja podataka događaju se sve dok tvrtke vode evidenciju i pohranjuju privatne podatke. Međutim, porast broja podataka, tehnološki napredak i digitalizacija pohrane podataka u posljednjem desetljeću ili većoj mjeri zabilježili su nagli porast broja kršenja podataka. Koristeći ove događaje, računalni kriminal se sve više razvija. Zločinci su skrenuli pozornost na meki korak korporacija, odnosno njihove pohranjene podatke. Stoga je sada rizik od gubitka ili izlaganja osjetljivih informacija veći nego ikad. Poduzeća moraju znati da se moraju zaštititi od računalnog kriminala imlementacijom sve suvremenijih zaštitnih sustava i programa da bi zaštitili svoje podatke, financijska sredstva i ukupno poslovanje. U protivnom mogu biti izloženi računalnim napadima sa brojnim posljedicama, gdje uglavnom počinitelji ostaju anonimni, a ako ih se i otkrije, podliježu kriminološkoj obradi i kaznama koje nisu mjerodavne prema šteti koju nanesu poduzećima.

LITERATURA

Knjige:

1. Babić, V. (2009): Kompjuterski kriminal: metodologija kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminala, Sarajevo, BiH: RABIC Sarajevo.
2. Bebek, B., Kolumbić, A. (2005): Poslovna etika, Sinergija nakladništvo: Zagreb.
3. Button, M., i Cross, C. (2017): Cyber Frauds, Scams and their Victims. New York: Routledge.
4. Clough, J. (2010): Principles of Cybercrime. New York: Cambridge University Press.
5. Čehok, I., Koprek, I. (1996): Etika – priručnik jedne discipline, Školska knjiga: Zagreb.
6. D. Dragičević, D. (2004): Kompjuterski kriminalitet i informacijski sustav, Zagreb: IBS.
7. Holt, T. and Bossler, A. (2016): Cybercrime in Progress. New York: Routledge.
8. Karpati, T. (2001): Etika u gospodarstvu, Ekonomski fakultet u Osijeku i Grafika: Osijek.
9. McGuire, M., Dowling, S. (2013): Cyber crime: A review of the evidence, University of Surrey,USA
10. Panian, Ž. (2005): Poslovna informatika za ekonomiste, Zagreb: MASMEDIA, 2005.
11. Šimundić, S., Franjić, S. (2009): Računalni kriminalitet,, Split: Sveučilište u Splitu, Pravni fakultet.
12. Talanga, J. (1999): Uvod u etiku, Hrvatski studiji – Studia Croatica: Zagreb. 1999.
13. Vidanec, D. (2011): Uvod u etiku poslovanja, Visoka škola za poslovanje i upravljanje s pravom javnosti „Baltazar Adam Krčelić“: Zaprešić.
14. Weihrich, H., Koontz, H. (2005): Menadžment, deseto izdanje**,** Mate: Zagreb.
15. Yar, M. (2006): Cybercrime and society, SAGE Publications, USA

Znanstveni članci:

1. Aleksić, A. (2007): Poslovna etika – element uspješnog poslovanja, Zbornik ekonomskog fakulteta u Zagrebu, Vol. 5, No. 1, prosinac 2007., str. 419 – 429
2. Kokot, I. (2014): Kaznenopravna zaštita računalnih sustava, ZPR, Vol. 3, No. 3, str. 303-330
3. Sampat, N. (2009): Piracy. U McQuade, S. (2009): Encyclopedia of Cybercrime, (str. 143-157, Westport: Greenwood Press.
4. Šimundić, S., Franjić, S., Vdovjak, K. (2012): »HOAX,« Zbornik radova Pravnog fakulteta u Splitu, Vol. 49, No. 3, str. 459 – 480

Internet izvori:

1. Investopedia (2020): 3 ways cyber crime impacts business, dostupno na https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx, pristupljeno 12.08.2020.
2. Justice.gov (2018): Two Russian Nationals Sentenced to Prison for Massive Data Breach Conspiracy, dostupno na https://www.justice.gov/opa/pr/two-russian-nationals-sentenced-prison-massive-data-breach-conspiracy, pristupljen 13.08.2020.
3. Lepitak, S. (2017): World's biggest agency networks claim all clear from cyber attack following WPP hacking, dostupno na https://www.thedrum.com/news/2017/06/28/worlds-biggest-agency-networks-claim-all-clear-cyber-attack-following-wpp-hacking, pristupljeno 11.08.2020.
4. Pinterest (2020): What is cyber crime, dostupno na https://in.pinterest.com/pin/834995587131907729/, pristupljeno 11.08.2020.
5. Wikileaks (2020): WikiLeaks Mirrors, dostupno nahttp://wikileaks.info/, pristupljeno 13.08.2020.
6. WikiLeaks.org (2020): Corporations, dostupno na https://wikileaks.org/+-Corporations-+.html, pristupljeno 13.08.2020.

Zakoni i propisi:

1. Zakon.hr (2020): zakon o autorskom pravu i srodnim pravima, NN 127/14, dostupno na https://www.zakon.hr/z/106/Zakon-o-autorskom-pravu-i-srodnim-pravima, pristupljeno 11.08.2020.

POPIS SLIKA

Naziv **Broj stranice**

Slika 1. Prikaz tipologije i procesa računalnog kriminala.....13

Slika 2. Prikaz pada računalnog sustava napadom hackera.....16

Slika 3. Logo WikiLeaksa.....39

IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Dalibor Strabić

Matični broj studenta: 0303027534

Naslov rada: Računalni kriminal i njegov utjecaj na ekonomsko poslovanje u 21. stoljeću

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum	Potpis studenta
_____	_____

ŽIVOTOPIS

O MENI

Zovem se Dalibor Strabić , imam 30 godina, zaposlen sam kao vozač tramvaja u Zagrebu. Živim sa roditeljima ,neoženjen.

Dalibor
Strabić

DATUM ROĐENJA:
27/02/1990

KONTAKT

Državljanstvo: hrvatsko
Spol: Muško
Facebook: https://
www.facebook.com/
Whatsapp Messenger:
whatsapp
Štuparje 77a
49234 Petrovsko, Hrvatska
dstrabi@gmail.com
(+385) 0981725821