PRAVNI FAKULTET
ZA PRIVREDU I PRAVOSUĐE
BIBLIOTEKA
Novi Sad

PRILAGOĐAVANJE PRAVNE REGULATIVE AKTUELNIM TRENDOVIMA U REGIONU

Priredio: Redovni profesor dr Milorad Bejatović

ADAPTING LEGAL REGULATIONS TO CURRENT TRENDS IN THE REGION

Edited by: Full Professor Milorad Bejatović, PhD

Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna akademija Novi Sad
Faculty of Law for Business and Justice
University Business Academy Novi Sad

Novi Sad 2015.

Zbornik referata sa međunarodnog naučnog skupa održanog
od 24. – 26. septembra 2015. godine u Novom Sadu
u organizaciji Pravnog fakulteta za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu.

Izdavač:
Pravni fakultet za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu,
Geri Karolja br. 1, telefon: 021 400 – 499
Web: www.pravni-fakultet.info

Recezenti:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Prof. dr Dragan Mrkšić
Prof. dr Bora Čejović
Prof. dr Miroslav Vitez
Prof. dr Milan Počuča
Prof. dr Milutin Đuričić
Prof. dr Zoran Pavlović
Prof. dr Ivan Joksić
Doc. dr Predrag Mirković

Za izdavača:
Prof. dr Marko Carić

Urednik:
Prof. dr Milorad Bejatović

Štampa:
Štamparija FELJTON, Novi Sad

Tiraž: 150

ISBN 978-86-6019-058-3

Štampanje Zbornika podržao
Sekretarijat za nauku i tehnološki razvoj AP Vojvodine

Članovi Programskog odbora:

Prof. dr Marko Carić
Dekan Pravnog fakulteta za privredu i pravosuđe u Novom Sadu,
Univerziteta Privredna akademija, Republika Srbija
Prof. dr Milorad Bejatović
Profesor Pravnog fakulteta za privredu i pravosuđe u Novom Sadu, Republika Srbija
Akademik prof. dr Miodrag Simović
Potpredsednik Ustavnog suda Bosne i Hercegovine
Prof. dr Borce Davitovski
Ss. Cyril nad Methodeus University, Republic of Macedonia
Prof. dr Kostadin Pušara
Predsednik Udruženja Lobista Crne Gore
Profesor Univerziteta Alfa u Beogradu, Republika Srbij**a**
Prof. dr Bora Čejović
Predsednik Krivičara Srbije
Prof. dr Miroslav Vitez
Ekonomski fakultet u Subotici, Republika Srbija
Prof. dr Dragan Mrkšić
Fakultet tehničkih nauka u Novom Sadu, Republika Srbija
Prof. dr Branko Vučković
Predsednik Osnovnog suda u Kotoru, Republika Crna Gora
Čedomir Backović
Pomoćnik ministra pravde Republike Srbije
Doc. dr Mirko Smoljić
Veleučilište „Lavoslav Ružička" u Vukovaru, Republika Hrvatska
Prof. dr Rok Lampe
Research Institute of European Faculty of Law in Nova Gorica, Republic of Slovenia
Sebastian Spinei
Faculty of Law, University „Lucian Blaga", Sibiu, Romania
Igor Denisov Yurevich
Vice President for Development at the Federal State Educational Institution of
Higher Professional Education, Omsk State Institute of Service, Russia

Članovi Organizacionog odbora:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Doc. dr Predrag Mirković
Doc. dr Darko Golić
Dr. Dragan Grahovac

Sekretar skupa:
Msr Nenad Stefanović

UDK: 343.963:004

Msr Joko Dragojlović / Joko Dragojlovic, LL.M.
Doktorand i asistent na Pravnom fakultetu za privredu i pravosuđe
Univerzitet Privredna akademija u Novom Sadu
PhD Student and Asistant at Faculty of Law,
University Business Academy in Novi Sad
E – mail : jdragojlovic@pravni-fakultet.info

Msr Miladin Danojlić / Miladin Danojlic, LL.M.
Saradnik u Višem sudu u Šapcu
Doktorand na Pravnom fakultetu za privredu i pravosuđe
Univerzitet Privredna akademija u Novom Sadu
Associate at a Higher Court in Sabac
PhD Student at Faculty of Law, University Business Academy in Novi Sad
E – mail: misadanojlic@yahoo.com

KRIVIČNO DELO PRAVLJENJE I UNOŠENJE RAČUNARSKIH VIRUSA KAO OBLIK UGROŽAVANJA RAČUNARSKIH SISTEMA

The Crime of Making and Inserting Computer Viruses As a Form of Compromising Computer Systems

A p s t r a k t :

Velike mogućnosti u svim sverama društvenog života koje su se čoveku ukazale razvojem informacione tehnologije, nesumnjivo za sobom su povukle i određene rizike i opasnosti koje se ogledaju u različitim vidovima zloupotreba kompjutera a samimim tim i kompjuterskih mreža, pre svega interneta. S tim u vezi, bez obzira koliko su računari doneli prednosti i koliki je njihov značaj u savremenom životu, oni nesumnjivo izlažu korisnike i brojnim rizicima kao što su narušavanje privatnosti, različitim vrstama krađa i prevara, destrukciji intelektualnih dobara, a sve to na način i obimu koji se pre dvadesetak godina nije mogao ni naslutiti. Dakle, sve ovo stvorilo je mogućnosti i atmosveru i za pojavu novih oblika kriminaliteta, tj. za pojavu visokotehnološkog kriminaliteta. U ovom radu, autori će analizirati krivično delo pravljenje i unošenje računarskih virusa. Kod ovog krivičnog dela prisutna je velika tamna brojka, stoga postoji naročita potreba da se ovaj vid kriminaliteta što više aktuelizuje kako u stručnoj tako i u opštoj javnosti, a sve to u cilju stvaranja svesti o potencijalnim opasnostima koje donosi ovo krivično delo.

Ključne reči: *Visokotehnološki kriminalitet, Računar, Virus, Unošenje virusa*

Abstract:

Great opportunities in all spheres of social life that came with the development of information technology, undoubtedly brought certain risks and dangers that are reflected in the various aspects of computer misuse and therefore computer networks, especially the Internet. In this connection, no matter how many advantages computers have brought and what is its significance in contemporary life, they also expose users to a number of risks such as invasion of privacy, the different types of theft and fraud, destruction of intellectual property, and all the way and extent that twenty years ago nobody could even imagine. So, all of this has created opportunities and the atmosphere for the emergence of new forms of crime, high-tech crime. In this paper, the authors will analyze the criminal act of creation and the insertion of computer viruses. For this crime there is a large dark figure, so there is a particular need for this type of crime to be more actualized in the professional as well as the general public, and all this in order to create awareness of the potential dangers of this crime.

Keywords: *high-tech crime, computer, virus, virus insertion*

UVOD

Danas smo svi svesni ogromnog značaja upotrebe kompjutera u savremenom društvu i činjenice da nema oblasti ljudske delatnosti u kojoj računari nisu našli svoju primenu, počevši od proizvodnje, prometa, vršenja usluga, komunikacija pa do različitih vidova bezbednosti. Drugim rečima, kompjuteri danas predstavljaju svakodnevnicu savremenog čoveka i gotovo je nemoguće zamisliti bilo kog pojedinca koji ne raspolaže sa osnovni znanjima i veštinama iz oblasti informacionih tehnologija. Međutim i pored široke primene i mnogo jednostavnijeg obavljanja različitih poslova, kompjuteri, nesporno, imaju i svoju negativnu stranu. Danas se kompjuteri i kompjuterska tehnologija mogu zloupotrebljavati na različite načine čime se pružaju mogućnosti za vršenje i planiranje različitih krivičnih dela.

Velike mogućnosti u svim sverama društvenog života koje su se čoveku ukazale razvojem informacione tehnologije, nesumnjivo za sobom su povukle i određene rizike i opasnosti koje se ogledaju u različitim vidovima zloupotreba kompjutera a samimim tim i kompjuterskih mreža, pre svega interneta. S tim u vezi, bez obzira koliko su računari doneli prednosti i koliki je njihov značaj u savremenom životu, oni nesumnjivo izlažu korisnike i brojnim rizicima kao što su narušavanje privatnosti, različitim vrstama krađa i prevara, destrukciji intelektualnih dobara, a sve to na način i obimu koji se pre dvadesetak godina nije mogao ni naslutiti. Dakle, sve ovo stvorilo je mogućnosti i atmosveru i za pojavu novih oblika kriminaliteta, tj. za pojavu visokotehnološkog kriminaliteta.

Mnogo nakon pojave prvih kompjutera možemo govotiti i o prvim vidovima zloupotrebe istih, a samim tim i o visokotehnološkom kriminalitetu, iz razloga što su kompjuteri u početku bili dostupni jako malom broju ljudi pa je stoga

broj onih koji su vršili zloupotrebe kao i onih koji su mogli biti žrtve, bio znatno manji. Shodno tome, kompjuterski kriminalitet je pojava koja je novijeg datuma i koja je potpunu „afirmaciju" doživela pojavom informatičke revolucije.

U tom smislu, autori će u ovom radu najpre napraviti kraći osvrt na pojam i karakteristike kompjuterskog kriminaliteta, a potom će analizirati krivično delo pravljenje i unošenje računarskih virusa, kao i posledice koje nastaju usled ovog krivičnog dela.

KRATAK OSVRT NA POJAM I OSNOVNE KARAKTERISTIKE VISOKOTEHNOLOŠKOG KRIMINALITETA

Iako je danas nemoguć život i funkcionisanje društva u celini bez upotrebe računara i savremene informatičke tehnologije, sazrela je svest da se ova korisna i potrebna sredstva mogu koristiti za nedopuštene, protivpravne ciljeve, u prvom redu za pribavljanje protivpravne imovinske koristi za neko lice ili za nanošenje štete drugima.[1]

Kada je reč o definisanju kompjuterskog kriminaliteta među autorima ne postoji saglasnost. Računarski kriminalitet je gotovo nemoguće definisati na jedinstven i precizan način s obzirom da je reč o kriminalitetu kod kojeg se novi pojavni oblici iz dana u dan pojavljuju, a već postojeći dodatno menjaju i usavršavaju. Međutim bez ambicija da uđemo u dublju analizu i definisanje ovog fenomena, za potrebe ovog rada istaći ćemo definiciju koja se nalazi u pozitivnopravnim propisima naše države. Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[2], po prvi put je i u domaćem zakonodavstvu definisan pojam visokotehnološkog kriminala i to kao: vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.[3] Dakle, možemo razlikovati krivična dela u kojima se računari koriste kao sredstvo izvršenja, objekat izvršenja kao i krivična dela koja se vrše na osnovu nezakonitog korišćenja interneta.

Računarski kriminalitet obiluje nizom specifičnosti u odnosu na "klasične" vidove kriminaliteta koje se pre svega ogledaju u velikoj fenomenološkoj raznovrsnosti, specifičnosti učinilaca ovih krivičnih dela, brzini vršenja krivičnog dela, težini posledice i visini štete, velikoj tamnoj brojci kao i proširenom prostoru

1 Bjelajac, Ž., Matijašević, J., Dimitrijević, D., (2012). Značaj uspostavljanja međunarodnih standarda u suzbijanju visokotehnološkog kriminala, *Međunarodna politika*, 63 (1146), str. 80.

2 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Sl. glasnik* RS, br. 61/05 i 104/09.

3 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Sl. glasnik* RS, br. 61/05 i 104/09, član 2. stav 1 i 2

kriminalnog delovanja koji ne zahteva prisustvo izvršioca na mestu izvršenja krivičnog dela.[4]

Računarski kriminalitet u odnosu na klasične vodove kriminaliteta karakteriše znatno proširen prostor kriminalnog delovanja koji ne zahteva prisustvo izvršioca na mestu izvršenja krivičnog dela. Dakle, kompjuterska krivična dela se vrše u specifičnom okruženju zvanom kibernetički ili *cyber* prostor. *Cyber* prostor je veštačka tvorevina koja zahteva visoku tehničku opremljenost, dobru informacionu infrastrukturu koja je ničija i svačija svojina, u kome paralelno koegzistiraju virtuelno i realno i kod koga je komunikacija kolektivna[5]. U takvom okruženju izuzetno je teško govoriti o nacionalnim razmerama kriminala i društvenoj opasnosti. Zato se ovaj kriminal svrstava u najizrazitiji oblik transnacionalnog kriminala protiv koga se uspešna borba ne može voditi unutar jedne države.

Prema tome, važna karakteristika *Cyber* prostora je globalna i transnacionalna dimenzija, koja prevazilazi granice jedne države. Naime, učinilac može radnju izvršenja preduzeti na jednom mestu, a da posledica nastupi na skroz drugom mestu, čak u drugoj državi ili pak kontinentu.

Imajući u obzir tehničke mogućnosti i automatizovani sistem, računarsko kriminalno delovanje se veoma brzo realizuje. Upravo ovakva vremenska dimenzija sprečava upravljanje i nadzor nad različitim aktivnostima i manipulacijama koje se preduzimaju putem kompjutera i kompjuterskih mreža. U tom smislu, vreme potrebno za izvršenje krivičnog dela skraćuje se na delove sekunde, što implicira visok nivo prikrivenosti i značajne teškoće u otkrivanju takve delatnosti, a na ovo se nadovezuju i suptilne tehnike i metodi koje se izvršavaju istim mehanizmima kao i legalne, ne ostavljaju tragove, niti ometaju redovan rad sistema, pa je samim tim mogućnost otkrivanja svedena na najmanju meru.[6]

U početku, učinioci kompjuterskog kriminala su po pravilu bila lica koja poseduju određena znanja i veštine iz oblasti informacionih tehnologija. Ovo je razumljivo iz razloga što je u prvim godinama razvoja računarske tehnologije, visoka stručnost i dobro poznavanje materije bio preduslov i za obično rukovanje kompjuterima, a samim tim i za vršenje određenih zloupotreba. Posedovanje određenih znanja i veština iz ove oblasti učiniocima uglavnom koristi u svrhe prikrivanja i težeg otkrivanja kriminalnih radnji. Danas se situacija u određenoj meri promenila i to pre svega usled široke dostupnost i jednostavnosti u rukovanju komponentama računarske tehnologije. Danas je gotovo nemoguće zamisliti da jedno domaćinstvo ili poslovni prostor ne poseduje kompjuter. Ovakva dinamika

4 Dragojlović, J., Krstinić, D., (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije, *Evropsko zakonodavstvo*, 13 (51/15), str. 93-94.

5 Matijašević-Obradović, J., (2014). The Significance and modalities of internet abuse as the primary global communication computer networks in cyberspace, *Megatrend revija*, 11 (1/2014), str. 280-281.

6 Petrović, S., (1994). Kompjuterski kriminal, *Bezbednost* 36 (1/94), str. 26

razvoja uslovila je i evoluciju različitih vrsta učinilaca računarskih krivičnih dela.[7]

Prilikom različitih zloupotreba komponenti računarske tehnologije, oštećeno lice često nije ni svesno da je u konkretnom slučaju žrtva krivičnog dela, pa samim tim izostaje podnošenje krivične prijave, a ako i dođe do otkrivanja izvršenog dela, često je već kasno da bi se mogla preduzeti neka efikasna mera.[8] Stoga, za ovaj vid kriminaliteta karakteriše jako velika tamna brojka.

KRIVIČNO DELO PRAVLJENJE I UNOŠENJE RAČUNARSKIH VIRUSA

Krivično delo pravljenje i unošenje računarskih virusa propisano je u članu 300 Krivičnog zakonika[9] Republike Srbije (u daljem tekstu KZ). Ovo delo se sastoji od osnovnog oblika koji je propisan u stavu 1 i kvalifikovanog oblika koji je propisan u stavu 2.

Krivično delo iz stava 1 čini onaj ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu. Računarski virus je definisan u članu 112 stav 20 KZ-a i predstavlja računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen tako da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka. Pravljenje računarskog virusa podrazumeva pisanje delova ili celih računarskih programa koji se nazivaju računarskim virusima.[10] Delo je dovršeno onda kada je računarski virus napravljen u nameri da se unese u tuđ računar. Dakle, potrebno je da postoji direktni umišljaj. Drugim rečima, za postojanje radnje, odnosno da bi se ispunio zakonski opis radnje izvršenja, bitno je da postoji subjektivno obeležje, a to je namera učinioca da napravljeni virus ubaci u tuđ računar.

Izvršilac ovog krivičnog dela može biti svako lice, ali posmatrano sa praktičnog aspekta, izvršilac može biti samo lice koje poseduje određena znanja iz oblasti informacionih tehnologija, tj. takozvani hakeri[11]. Izvršioci su po pravilu lica koja nemaju samo osnovno poznavanje rada na računaru već u mnogo kvalitetnijem nivou poznaju i način rada operativnog sistema, način funkcionisanja pojedinih

7 Matijašević, J., (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, Novi Sad, Pravni fakultet za privredu i pravosuđe u Novom Sadu, str. 20.

8 Matijašević, J., Krivičnopravna regulativa računarskog kriminaliteta, str. 21.

9 Krivični zakonik, *Sl. glasnik* RS, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09 i 111/09 i 121/12, 104/13, 108/14.

10 Mrvić-Petrović, N., (2010). *Krivično pravo-posebni deo*, Beograd, Pravni fakultet Univerziteta Union i JP Službeni glasnik, str. 243-244.

11 Više o hakerima u: Matijašević, O., J., Bingulac N., Dragojlović, J., (2014). Psihologija hakera i značaj njihovih aktivnosti u internet komunikacijama savremenog društva, u Zorka Grandov et al. (urednik) Moć komunikacije - 3. Međunarodni naučni skup, Beograd, Panevropski Univerzitet Apeiron, str. 147-160.

delova i međusobne povezanosti i operativnog sistema, osnove programiranja, izrade računarskih programa uz pomoć nekog od postojećih i poznatih programskih jezika ili alata.[12]

Za osnovni oblik krivičnog dela pravljenje i unošenje računarskih virusa iz člana 300 stav 1 KZ-a propisana je novčana kazna ili zatvor do šest meseci.

U stavu 2 propisan je teži (kvalifikovani) oblik koji čini onaj ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu. Dakle radnja izvršenja je kumulativno određena i sastoji se od unošenja virusa i prouzrokovanja štete. Dakle, neophodno je da postoji uzročna veza između unetog virusa i nastale štete. Nastanak štete se može manifestovati u bilo kom obliku tj. nije neophodno da je došlo do imovinske štete, već ona može da se odrazi i na zastoj u radu računara, ispoljavanju različitih grešaka u radu. Drugim rečima, neophodno je da uneti virus prouzrokuje štetne efekte po rad i funkcionisanje računara.[13] Za postojanje krivičnog dela nije od značaja na koji način je lice koje je unelo računarski virus u tuđ kompjuter do njega i došlo. Dakle, nije neophodno da ga je učinilac sam napravio, već krivično delo postoji i u slučaju kada je do računarskog virusa došao i na posredan način. Po pravilu, virusi se unose uobičajenim putevima zaraze putem disketa, menjajući sadržaj hard diska, CD ROM-om, preko e-maila, fleš memorije i slično.[14] Ovaj oblik krivičnog dela može biti izvršen samo sa umišljajem, te stoga onaj ko iz ne pažnje preko različitih disketa i fleš memorija koje koristi unese računarski virus u tuđ računar, ne čini pomenuto krivično delo.

Zaprećena kazna za krivično delo pravljenje i unošenje računarskih virusa iz člana 300 stav 2 KZ-a je novčana kazna ili zatvor do dve godine.

KRATAK OSVRT NA POSLEDICE KOJE NASTAJU USLED PRAVLJENJA I UNOŠENJA RAČUNARSKIH VIRUSA

Upotreba ručunarskih virusa je jedan od najrasprostranjenijih vidova računarskog kriminaliteta. Međutim, ovo je vid kriminaliteta kod koga je prisutna jako velika tamna brojka, jer veliki broj ovih krivičnih dela i ne bude prijavljen, jer žrtve nisu ni svesne da im je računar zaražen virusom.

Računarski virusi su mali programi koji se razmnožavaju tako što sami sebe ugnjezde na drugim fajlovima a štetu prave tako što mjenjaju ili brišu fajlove na računaru tj. na hard disku.[15] U suštini, usled unošenja računarskog virusa u do

12 Stamenković, B., et al. (2014). *Visokotehnološki kriminal-praktični vodič kroz savremeno krivično pravo i primjere iz prakse*, Podgorica, OEBS misija u Crnoj Gori, str. 124.

13 Stojanović, Z., (2012). *Komentar Krivičnog zakonika*, Beograd, JP Službeni glasnik, str. 825.

14 Mrvić-Petrović, N., *op. cit*. str. 244.

15 Matijašević, J., Krivičnopravna regulativa računarskog kriminaliteta, str. 29.

tada nezaraženom računaru, po pravilu računar počinje drugačije da se ponaša i javljaju se poteškoće i nepravilnosti u radu. Manifestacije usled ove pojave su razne. Može doći do pojavljivanja benignih poruka na monitoru računara, zamene komandi desnog i levog klika na mišu ili neplaniranog gašenja računara, pa sve do ozbiljnih oštećenja, poput brisanja programa i podataka u memoriji računara, onesposobljavanja operativnog sistema ili oštećenja hardvera.[16]

Posledice koje nastaju usled pravljenja i unošenja računarskih virusa mogu biti jako velike iako u prvi mah mogu izgledati beznačajne. Naime, tvorci virusa pomenute programe prave i u cilju realizacije različitih vidova špijunaže i krađe podataka koji imaju značaja u savremenom društvu. Takođe, nisu retki ni slučajevi internet reketiranja. Tvorci ovih virusa obično stvaraju mrežu zombi kompjutera osposobljenih da vode organizovani DoS napad.[17] Time oni ucenjuju kompanije preteći im DoS napadom na kompanijski vebsajt. Popularne mete uključuju e-prodavnice, bankovne i kockarske sajtove, npr. kompanije čiji se prihod ostvaruje direktno njihovim on-line prisustvom.

Koliko virusi mogu biti opasni, govori i slučaj iz 2010. godine kada je kompjuterski virus *Staksnet* napravio haos u svetu i uspeo da ugrozi i iranski nuklearni program. On je napao uređaje koji kontrolišu centrifuge uranijuma. Njegov zadatak bio je po svemu sudeći da omogući manipulisanje sistemom za upravljanje, odnosno obustavi rad centrifuga. Istovremeno je *Staksnet* uspeo da zavara sistem kontrole i prikrije svoje prisustvo.[18]

Takođe, izvršioci ovih krivičnih dela unošenjem virusa u tuđi računar imaju mogućnost slikanja aktivnog monitora, snimanja onoga što vlasnik zaraženog računara kuca na tastaturi, postavljanje različitih sadržaja na zaraženi računar, kao i skidanje sadržaja sa zaraženog računara. Naime, imajući u vidu da je savremeno društvo postalo zavisno od korišćenja računara i da se funkcionisanje bilo kog državnog organa i različitih privatnih firmi zasniva na kompjuterima, onda nije teško naslutiti posledice koje mogu nastati usled unošenja virusa u njihove računare. Ono što predstavlja ozbiljan problem kod ovih krivičnih dela jeste to što većina korisnika neće ni primetiti da im je računar zaražen virusom. Stoga, tamna brojka kod ovih krivičnih dela je jako velika.

16 Ibid.

17 Napad uskraćivanjem usluge (*eng. Denial-of-service attack*,) je napad na neki računar gde napadač želi resurse ili servise tog računara učiniti nedostupnim za njihove korisnike. Preuzeto sa: Napadi uskraćivanjem usluge, (22.05.2015.) preuzeto sa: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-01-321.pdf str. 3,

18 Kazne za pravljenje i unošenje računarskih virusa - visokotehnološki kriminal i ima li mu leka, (22. 05. 2015.) preuzeto sa: http://www.prekoramena.com/t.item.380/kazne-za-pravljenje-i-unosenje-virusa.html

ZAKLJUČNA RAZMATRANJA

Kao što smo videli, krivično delo pravljenje i unošenje računarskih virusa predstavlja krivično delo koje proizvodi niz negativnih posledica, počevši od usporenog i otežanog rada računara, pa sve do ozbiljnijih posledica koje se sastoje u menjanju i brisanju fajlova na zaraženom računaru. Ono što predstavlja problem kod gotovo svih oblika visokotehnološkog kriminaliteta, a samim tim i kod krivičnog dela pravljenje i unošenje računarskih virusa, jeste nepostojanje svesti kod korisnika o tome da je njihov računar zaražen. Isto tako, veliko broj korisnika računara nije ni svestan posledica koje mogu nastati usled toga.

Kada je reč o Republici Srbiji i krivičnom delu pravljenje i unošenje računarskih virusa, pre svega potrebno je napomenuti da sudska praksa u odnosu na pomenuto krivično delo gotovo i ne postoji. Razloge za ovu pojavu svakako pre treba tražiti u jako velikoj tamnoj brojci kada je reč o ovom krivičnom delu sa jedne strane, kao i nepostojanju svesti žrtava (korisnika kompjutera) da su postale žrtve ovog krivičnog dela sa druge strane. Stavovi da ovaj vid kriminalne aktivnosti u Republici Srbiji i ne postoji svakako se ne mogu smatrati prihvatljivim.

Međutim, i pored adekvatne zakonske regulative, glavne poteškoće koje sa javljaju u otkrivanju i suzbijanju krivičnih dela visokotehnološkog kriminaliteta, a samim tim i krivičnog dela pravljenje i unošenje računarskih virusa jeste nedostatak adekvatnog stručnog kadra. Dakle, otežavajuća okolnost kod procesuiranja u slučajevima krivičnih dela visokotehnološkog kriminaliteta a samim tim i kod ovog krivičnog dela jeste što je neophodno posedovanje određenog znanja. Naime za suzbijanje i efikasno otkrivanje, pa na kraju i za uspešno suđenje u postupcima gde se pojavljuju ova krivična dela, potrebno je angažovati lica koja poseduju znanja iz oblasti informatičke struke. Stoga i pored dobre zakonske regulative, za uspešnu borbu protiv ovog vida kriminaliteta neophodno je zapošljavanje stručnog kadra u svim institucijama koje vode borbu protiv ovog oblika kriminaliteta.

LITERATURA:

1. Bjelajac, Ž., Matijašević, J., Dimitrijević, D., (2012). Značaj uspostavljanja međunarodnih standarda u suzbijanju visokotehnološkog kriminala, *Međunarodna politika*, 63 (1146), str. 66-85.
2. Dragojlović, J., Krstinić, D., (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije, *Evropsko zakonodavstvo*, 14 (51/15), str. 92-103.
3. Kazne za pravljenje i unošenje računarskih virusa - visokotehnološki kriminal i ima li mu leka, (22. 05. 2015.) preuzeto sa: http://www.prekoramena.com/t.item.380/kazne-za-pravljenje-i-unosenje-virusa.html
4. Krivični zakonik, *Sl. glasnik* RS, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09 i 111/09 i 121/12, 104/13, 108/14.

5. Matijašević, J., (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, Novi Sad, Pravni fakultet za privredu i pravosuđe u Novom Sadu.
6. Matijašević, O., J., Bingulac N., Dragojlović, J., (2014). Psihologija hakera i značaj njihovih aktivnosti u internet komunikacijama savremenog društva, u Zorka Grandov et al. (urednik) Moć komunikacije - 3. Međunarodni naučni skup, Beograd, Panevropski Univerzitet Apeiron, str. 147-160.
7. Matijašević-Obradović, J., The Significance and modalities of internet abuse as the primary global communication computer networks in cyberspace, *Megatrend revija*, 11 (1/2014), str. 279-298.
8. Mrvić-Petrović, N., (2010). *Krivično pravo-posebni deo*, Beograd, Pravni fakultet Univerziteta Union i JP Službeni glasnik.
9. Napadi uskraćivanjem usluge, (22.05.2015.) preuzeto sa: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-01-321.pdf
10. Petrović, S., (1994). Kompjuterski kriminal, *Bezbednost* 36 (1/94), str. 17-38.
11. Stojanović, Z., (2012). *Komentar Krivičnog zakonika*, Beograd, JP Službeni glasnik.
12. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Sl. glasnik* RS, br. 61/05 i 104/09.
13. Stamenković, B., et al. (2014). *Visokotehnološki kriminal-praktični vodič kroz savremeno krivično pravo i primjere iz prakse*, Podgorica, OEBS misija u Crnoj Gori.

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

340.134(497)(082)

МЕЂУНАРОДНИ научни скуп "Прилагођавање правне регулативе актуелним трендовима у региону" (2015 ; Нови Сад)
[Zbornik referata sa Međunarodnog naučnog skupa "Prilagođavanje pravne regulative aktuelnim trendovima u regionu", 24-26. septembar 2015, Novi Sad] / [priredio Milorad Bejatović]. - Novi Sad : Pravni fakultet za privredu i pravosuđe, 2015 (Novi Sad : Feljton). - 825 str. : ilustr. ; 24 cm

Tiraž 150. - Bibliografija uz svaki rad. - Rezime na engl. jeziku uz većinu radova.

ISBN 978-86-6019-058-3

а) Правна регулатива - Усаглашавање - Балкан - Зборници
COBISS.SR-ID 299340807