Informacijska sigurnost (evropski standardi)

Puharić Predrag – *Univerzitet u Sarajevu*
Muhamed Budimlić – *Univerzitet u Sarajevu*

Sažetak

Sigurnost je u savremenom društvu jedan od preduslova funkcinisanja i postojanja države. U ovom radu bavićemo se dijelom sigurnosti okrenutom ka informacijima. Daćemo kratki istorijat informacijske sigurnosti te obraditi aktuelne globalne i evropske standarde koji regulišu tu materiju. Prikazaćemo i neke od inkriminacija vezanih uz pojam informacijske sigurnosti.

Klučne riječi

Informacije, sigurnost, evropski standardi, ISO

Abstract - Information Safety (European Standards)

Security is one of the pillars of functioning and existence of modern state. In this article we will elaborate information security. After introduction to the history of information security we will take a look into some of contemporary global and European standards of information security and present some of the incrimination related to it.

Key words

Information, security, European standards, ISO

Sigurnost

Riječ sigurnost (eng. security) potiče iz latinskog izraza securitas i znači odsustvo opasnosti, zaštićenost i sl. U savremenom društvu sigurnost je jedan od preduslova funkcionisanja i samog postojanja države. Također, smatra se da je sigurnost temeljna kategorija ljudskih prava i sloboda građana.

Polazeći od toga savremenu sigurnost u sistemskom smislu, možemo definirati kao dinamičnu, složenu i specifičnu kategoriju, kojom se obezbjeđuju sigurnosne i slobodne prostorne i egzistencijalne pretpostavke potrebne za odvijanje prirodnih i fundamentalnih sveukupnih ljudskih potreba i interesa, uz dosljedno priznanje i zaštitu osnovnih prava i sloboda čovjeka, održavanjem potrebne ravnoteže između slobode i sigurnosti, čovjeka i prirode, te potrebnu i efikasnu premoć pozitivnih konstruktivnih nad destruktivnim tendencijama u razvoju civilizacije u cilju unapređenja i zaštite sveukupnih vrijednosti društva.[1]

Kao što se može vidjeti na šemi, klasična podjela sigurnosti ne navodi implicitno informacijsku sigurnost, ali možemo reći da je ona prisutna na svakom nivou, te je danas uspješna

[1] Masleša R.: Teorije i sistemi sigurnosti

uspostavljena informacijska sigurnost presudna za funkcionisanje bilo kojeg navedenog nivoa sigurnosti.

Šema raznih nivoa sigurnosti[2]

Informacija i nauka o informacijama

Informacija je primljena i shvaćena poruka
(Prinston)

Riječ informacija potiče iz latinskog izraza in formare što znači stavljanje u određenu formu, davanje oblika nečemu, ali se današnje shvatanje pojma informacije ne poklapa sa tim prvobitnim značenjem. Neke od definicija informacije su da je informacija značenje koje dajemo podatku ili da je informacija podatak u nekom kontekstu.

Iz ovih navoda je vidljivo da, iako se često predstavljaju kao sinonimi, informacija i podatak predstavljaju različite pojmove. Možemo reći da je riječ terorista podatak i da kao takav nama nema neko posebno ili korisno značenje, ali rečenica „Bin Laden je terorista" je informacija, jer smo podatku dali neko značenje.

Iz prethodno navedenog možemo zaključiti da se informacija sastoji od podatka i značenja koje mu je dodijeljeno. Da ponovimo: ***Informacija je rezultat obrade, manipulacije i organiziranja podataka na način koji dodaje znanje primatelju. Drugim riječima, to je kontekst u kojem su podaci uzeti.***

Uz pojam informacije usko je vezan i pojam komunikacije. Komunikacija se sastoji od pošiljatelja informacije, primatelja informacije, medija kojim informacija putuje, te smetnji koje utiču na medij i informacije u njemu. Pošiljatelj i primalac mogu biti npr. dva sagovor-

[2] Ibid

nika u parku, informacijski medij je vazduh, a smetnju može predstavljati buka djece koja se igraju u parku.

Jasno je da svaki od faktora u komunikaciji nosi i određeni, veći ili manji, rizik po sigurnost informacije. Načinom prenosa informacije bavi se informacijska nauka, a sigurnošću tih informacija informacijska sigurnost.

Šta je informacijska sigurnost?

Već smo rekli da informacije, kao i svaka druga imovina, zahtijevaju odgovarajuću zaštitu. To je posebno važno u današnjem umreženom svijetu. Kao posljedica sve veće količine informacija u digitalnom obliku (finansijske informacije, podaci u zdravstvu, podaci osiguravajućih kompanija, obavještajni podaci, podaci građana vođeni od strane države i drugih upravnih organa) i sve veće umreženosti sve je veća i gama prijetnji sigurnosti tih informacija.

Da ponovimo, govorimo o informaciji u raznim oblicima, kako o onima u elektronskom obliku, tako i onima zapisanim na papir, pohranjenim na film, čak i o informacijama koje su samo izgovorene. Bez obzira u kojem obliku informacija bila, ona uvijek mora biti ispravno zaštićena.

Informacijska sigurnost je niz mjera i postupaka u cilju zaštite informacije od širokog spektra prijetnji sigurnosti da bi smo osigurali kontinuitet rada, minimizovali rizike i imali najbolji omjer uloženog i dobijene sigurnosti.

Zašto nam je potrebna informacijska sigurnost?

Informacija je u savremenom svijetu osnov kako poslovnih, tako i međudržavnih odnosa od najniže do najviše razine. Informacija je bitna i u međusobnom odnosu građana i države.

Gubitak neke informacije ili odlazak informacije „u pogrešne ruke" može izazvati širok spektar čak i veoma ozbiljnih posljedica (slučaj Aleksandra Litvenka, Societe General...)

Informacije su podložne čitavom spektru prijetnji uključujući, ali se ne zaustavljajući na kompjuterskim prevarama, špijunaži, sabotaži, vandalizmu, požaru, poplavama itd. Slučajevi malicioznog programskog koda, kompjuterskog hakinga i zabrane pristupa postaju sve uobičajeniji, ambiciozniji i sofisticiraniji.

Informacijska sigurnost je bitna i u privatnom i javnom sektoru, kao i pri zaštiti ključne infrastrukture. U svakom slučaju, informacijska sigurnost funcionira kao faktor uspostave e-vlada i e-biznisa. Povezanost javnih i privatnih mreža i dijeljenje informacijskih resursa samo naglašava potrebu za sveobuhvatnom sigurnošću, pa tako i onom informacijskom.

Kratka istorija informacijske sigurnosti

Može se slobodno reći da informacijska sigurnost postoji od kad postoje i civilizovana društva. Državnici, vođe i policijski i vojni službenici veoma rano su shvatili važnost sigurnosti informacija, te da je potrebno da uspostave mehanizme da bi osigurali tajnost službene prepiske.[3] Kao oca kriptografije čak bi mogli navesti Julija Cezara koji je koristio šifru koju je sam kreirao te njome šifrirao svoje tajne poruke.

Ratovi su se, kao i u ostalim sferama nauke, pokazali kao pokretači napretka i na polju kriptografije i sigurnosti, te označavaju početak formiranja modernih sigurnosnih stručnjaka. Drugi svjetski rat je tako doveo do napretka na polju fizičke sigurnosti prvi put uvodeći barijere i prepreke te obučene čuvare za zaštitu informacijskih centara. Također, prvi put se u širokom obimu uvodi formalna klasifikacija dokumenata te dozvole raznih nivoa za pristup informacija, te se uspostavlja praksa sigurnosne provjere pri izdavanju tih dozvola. Drugi svjetski rat te hladnoratovski period donose ogroman napredak na polju kriptografije.[4]

Kraj 20. i početak 21. vijeka, sa ogromnim tehnološkim napretkom donose i ogroman napredak na polju informacijske nauke i tehnologije. Pojavom Interneta i World Wide Web-a informacije svih vrsta postaju globalno dostupne. Obavještajna zajednica je također uočila prednosti ovih tehnologija, te 2006. godine obavještajne službe SAD-a osnivaju svojevrstnu verziju internet enciklopedije pod nazivom Intellipedia. Predviđeno je da ona sadrži obavještajne podatke svih agencija te time olakša i ubrza razmjenu obavještajnih informacija između pripadnika raznih agencija. Da li je potrebno naglasiti važnost sigurnosti ovih podataka?

Kako uspostaviti sigurnosne zahtjeve?

Svaka organizacija, pa tako i država treba da identificira svoje sigurnosne zahtjeve. Radi se o tri osnovna izvora sigurnosnih zahtjeva:

1. Procjena rizika organizaciji, uključujući sveobuhvatne ciljeve organizacije. Putem procjene rizika, identifikuju se prijetnje i njihova vjerovatnoća te uticaj na organizaciju.
2. Zakonski, statutarni i ugovorni zahtjevi koje organizacija mora ispuniti.
3. Dodatni izvor je skup principa i pravila koje je organizacija razvila da bi podržala vlastito djelovanje.

[3] Na primjer korištenje voštanih pečata

[4] Kao početak moderne kriptografije može se uzeti nacistički kriptografski sistem poznat pod kodnim imenom „Enigma"

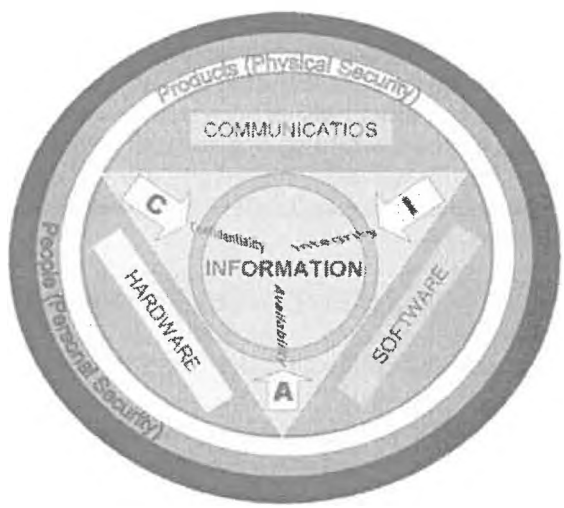
Osnovni aspekti informacijske sigurnosti

Osnovni faktori informacijske sigurnosti su:

- Tajnost (Confidentiality)
- Integritet (Integrity) i
- Dostupnost (Availability).

Ova tri faktora su poznata i pod pojmom CIA trokut (od početnih slova engleskog naziva).

CIA trokut – u sredini po podaci i usluge



Odnos tri ključna faktora prema raznim uticajima i nivoima sigurnosti

Na ovom mjestu nećemo se detaljno baviti objašnjavanjem ovih pojmova jer vjerujemo da su dovoljno poznati.

Standardizacija sigurnosti

U savremenom svijetu, pogotovo u vremenu poslije 11.9. sveobuhvatna sigurnost predstavlja prioritet svake države. Sigurnosni aspekti su postali tako važni da se i do tada nedodirljiva prava pojedinaca narušavaju pod opravdanjem „nacionalne sigurnosti".

Takvo stanje svijesti dovelo je i do standardizacije sigurnosti. Sigurnost više nije pitanje slobodne stručne i naučne procjene. Sigurnost je jasno definisana i određena. Osnovi sigurnosti više nisu niz naučnih teorema, manje ili više pretočenih u praksu. Sigurnost je niz dokumenata, koji veoma precizno i detaljno definišu uloge i zadatke svih učesnika u jasno definisanim sigurnosnim procesima i procedurama.

Ova standardizacija je i od krucijalne važnosti za sve zemlje regiona jugoistočne Evrope, čiji je proklamovani nacionalni interes i pridruženje euroatlantskim integracijama. Ili bi tako, barem trebalo biti. Nažalost, svjedoci smo da države regiona vrlo malo ili nikako, a nadasve sporo, implementiraju čitav niz evropskih standarda pa tako i one standarde koje se bave pitanjem sigurnosti.

Kao što smo već napomenuli, osnov savremene sigurnosti je informacija. Pravovremeno posjedovati relevantne informacije je ključ sigurnosti. Samim tim, informacijska sigurnost predstavlja i jedan od osnova sveobuhvatne sigurnosti.

Još jednom napominjemo, informacijska sigurnost obuhvata sve vidove prenosa i skladištenja informacija, a ne samo elektronske, ali naravno da će u savremenom okruženju ogromna većina informacija na kraju završiti u nekom elektronskom obliku. Tako će nešto izgovoreno, vjerovatno biti snimljeno na magnetnu traku pa zatim digitalizovano i arhivirano na nekom obliku elektronskog medija ili čak u startu biti digitalno snimljeno. Neki papirni dokument će vjerovatno vrlo brzo od svog nastanka završiti skeniran, prepoznat i konvertovan u digitalni tekst te kao takav i biti sačuvan. Jasno je da se savremena informacijska sigurnost velikim dijelom fokusira upravo na očuvanje sigurnosti i integriteta digitalnih podataka i informacija.

Upravo iz razloga rastuće važnosti digitalno zabilježenih informacija (ali i onih drugih) te sve brojnijih prijetnji po njihov integritet i tajnost, EU je donijela niz odluka i standarda kojima se uspostavljaju specifični, tačno određeni zahtjevi po sigurnosti.

Zbog prirode rada nije moguće navesti sve zakone koje se odnose na ovu problematiku, te ćemo nabrojati samo one najvažnije prisutne u EU, SAD-u, Velikoj Britaniji i Kanadi. Ovi zakoni mogu biti odlična početna tačka za donošenje sličnih zakona u zemljama regije.

1. European Union Data Protection Directive (EUDPD) iz 1995. godine[5]
2. UK Data Protection Act (1998) – donesen na osnovu EUDPD koji zahtijeva da sve članice unije u svoju legislativu uvedu odredbe o zaštiti podataka

[5] http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

3. Computer Misuse Act (1990) je propis kojim je u pravnu praksu Velike Britanije uvedeno krivično djelo hakinga. Poslužio je kao osnov sličnim zakonima u Kanadi i Republici Irskoj
4. EU Data Retention zakoni nalažu da svi telekomunikacijski operateri čuvaju podatke o svim transkacijama od 6 mjeseci pa sve do dvije godine.
5. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) – američki savezni zakon koji štiti studentske podatke
6. Health Insurance Portability and Accountability Act (HIPAA) – obaveza zaštite medicinskih podataka za medicinske ustanove, osiguravajuće kompanije i poslodavce
7. Gramm-Leach-Bliley Act of 1999 - (GLBA) – zaštita privatnih finansijskih transakcija
8. Sarbanes-Oxley Act of 2002 (SOX) – uspostavlja dužnost čuvanja finansijskih i sličnih podataka u svim organizacijama te uspostavlja jasnu odgovornost za ove mjere
9. Payment Card Industry Data Security Standard (PCI DSS) – Standard donesen od strane vodećih svjetskih kartičnih organizacija
10. Security Breach Notification Laws – zakoni pojedinih država SAD-a (prva ga je usvojila Kalifornija) koji obavezuje sve subjekte da obavijeste potencijalne oštećene da je došlo do otkrivanja zaštićenih podataka.
11. Personal Information Protection and Electronics Document Act (PIPEDA) – kanadski zakon o tajnosti elektronski prikupljenih podataka.

ISO/IEC 20000 skup standarda

Izvor svim ovim zakonima i njihova polazna tačka su standardi izrađeni od strane Međunarodne organizacije za standardizaciju (ISO) The ISO-15443: "Information technology - Security techniques - A framework for IT security assurance", ISO-17799: "Information technology - Security techniques - Code of practice for information security management", ISO-20000: "Information technology - Service management" i ISO-27001: "Information technology - Security techniques - Information security management systems".

Ipak kao najvažniji se uzima standard pod oznakom 27002:2005 jer je on najzanimljiviji ne tehničkom osoblju. On je standard koji se bavi uopštenom zaštitom informacija, bilo kojeg oblika i bilo koje vrste. On uspostavlja i savjetuje niz procedura kojima se osiguravaju tri ključna faktora pri sigurnosti bilo koje informacije, pa tako i informacije u sigurnosno-obavještajnoj zajednici: tajnost, integritet i dostupnost. Ukratko ćemo opisati ovaj standard.

ISO/IEC 27002 je dio rastućeg skupa ISO standarda vezanih uz informacijsku sigurnost objavljenih od strane ISO i IEC[6] pod prvobitnom oznakom 17799:2005 u julu 2007. godine nakon revizije pod oznakom 27002:2005. Nastao je na osnovu britanskog standarda BS

[6] Međunarodna elektrotehnička komisija

77991:1999. Britanski standard je, u stvari, i predstavljao prvu verziju ISO standarda, da bi kasnije doživio nekoliko revizija.

ISO/IEC 27002 predlaže najbolje načine za upravljanje informacijskom sigurnošću onima koji su odgovorni za pokretanje, uspostavljanje i održavanje sistema upravljanja informacijskom sigurnošću (ISMS).

Da bi osigurao održanje CIA trokuta ovaj standard se bavi sljedećom problematikom:

- Procjenom i otklanjanjem rizika
- Sigurnosnim politikama
- Organizacijom informacijske sigurnosti i to sa aspekta
  - Unutrašnje organizacije
  - Vanjskih stranaka
- Upravljanjem sredstvima
  - Odgovornost za sredstva
  - Klasifikacija informacija
- Upravljanje sigurnošću ljudskog faktora
  - Prije zaposlenja
  - Tokom zaposlenja
  - Prekid ili promjena posla
- Fizička i sigurnost okoline
  - Sigurne zone
  - Sigurnost opreme
- Komunikacije i upravljanje operacijama
  - Planiranje sistema
  - Razmjena informacija
  - Rukovanje medijima
  - Nadgledanje
  - ...
- Upravljanje pristupom informacijama
- Nabavka, razvoj i održavanje informacijskog sistema
  - Sigurnosni zahtjevi
  - Kriptografija
  - ...
- Upravljanje pri incidentu
- Osiguranje neprekidnosti dostupnosti
- Usklađenost sa zakonskim normama

Iz ovog prikaza sasvim je jasno da ovaj standard predstavlja izvanrednu osnovu za sigurnost te da je potrebno njegovo podrobno proučavanje i primjena u lokalnoj standardizaciji. Također, standard je zbog svoje opširnosti i preciznosti i veoma komplikovan za implementaciju te nije dobro primjenjivati ga djelimično, jer to može dovesti do osjećaja lažne sigurnosti. Ukoliko ovaj standard nije ispunjen u cijelosti nećemo imati ni instrumente kojima bi se mogli otkriti i popraviti propusti niti ispravno reagovati na već odigrani incident.

Ovdje ćemo još navesti da pri razumijevanju ovog standarda može pomoći prethodna upotreba tzv. Standarda dobre prakse kojeg je na osnovu ISO/IEC 27002 izradio Međunarodni forum za sigurnost.

Međunarodne pravne refleksije u oblasti suprotstavljanju kompjuterskom kriminalitetu kao segment informacijeske sigurnosti

U ovom dijelu rada prikazat ćemo najčešće oblike inkriminiranja različitih pojavnih oblika iz oblasti kompjuterskog kriminaliteta, što će nam omogućiti sticanje uvida o tretiranju ovog problema u zemljama sa savremenim sistemima sigurnosti.

Neovlašten pristup kompjuterskom sistemu

Neovlašten pristup kompjuterskom sistemu ili *"haking"*, predstavlja takvu radnju u kojoj napadač putem telekomunikacionih sistema, koji obezbjeđuju povezivanje više računara ili računarskih sistema, neovlašteno prodre u bazu podataka, pohranjenu u jednom takvom sistemu, sa namjerom manipulacije tim podacima.

Jedna od osnovnih karakteristika savremenih računarskih sistema jeste upravo mogućnost daljinskog upravljanja i povezivanja. Ipak, ova osobina, otvorenost prema okolini, računarske sisteme izlaže opasnosti neovlaštenog pristupa i stavlja ih u ulogu potencijalnih meta. Što su podaci, pohranjeni u bazama podataka, vrijedniji to je i vjerovatnoća neovlaštenog pristupa veća. Pored tehnoloških sistema zaštite, neophodno je bilo razviti i krivičnopravnu regulativu zaštite kompjuterskih sistema i informacija koje su oni sadržavali.

U novim se zakonima primjenjuju različiti pristupi, koji se kreću od inkriminiranja već i samog pristupa kompjuterskim sistemima (Austrija, Danska, Engleska, Grčka i većina država SAD-a), do onih koje kažnjavaju samo u slučajevima gdje su podaci kojima se pristupilo zaštićeni sigurnosnim mjerama (Njemačka, Nizozemska, Norveška), ili gdje počinitelj ima štetne namjere (Kanada, Francuska, Izrael, Novi Zeland, Škotska), ili gdje su podaci pribavljeni, izmjenjeni ili oštećeni (neke države u SAD), ili gdje je prouzročena makar i najmanja šteta (Španija).[7] Moderni trendovi u krivičnim zakonodavstvima, veoma često, djelo *"hakinga"* postavljaju u supsidijarni odnos sa nekim drugim, daljnjim, djelom koje može predstavljati kopiranje pohranjenih podataka, pribavljenje imovinske koristi ili korištenje tog sistema za posredstvo u komunikaciji sa nekim drugim sistemom.

Kompjuterska špijunaža i prisluškivanje

Tradicionalna forma inkriminacije špijunaže pretpostavlja odavanje tajne, koja može imati različit karakter (državne, vojne, ekonomske, službene itd.), gdje se pod odavanjem podrazumijevaju predaja ili činjenje dostupnim podataka sa karakterom tajnosti. Nematerijalni karakter podatka, pohranjenog u elektronskom obliku, ne može se primjeniti na ova tradicionalna rješenje o shvatanju objekta krivičnog djela. Podaci u memoriji kompjutera, po-

[7] Ibidem, str.153.

daci koji se prenose telefonskim, kablovskim ili satelitskim komunikacijama, upravo zbog svog netjelesnog karaktera, teško postaju predmetom tradicionalnih inkriminacija sa imovinskom osnovom.

Većina zemalja kontinentalnog prava, kao što su Austrija, Belgija, Njemačka, Grčka i Italija, protivi se primjeni tradicionalnih odredbi o krađi i pronevjeri, zato što ovi propisi traže da se tjelesna imovina prisvoji s namjerom da se trajno otuđi od žrtve. Drugačiji stav i mišljenje može se naći u nekim zemljama običajnog prava, kao što su SAD, Kanada, Australija i Izrael, u kojima se kompjuterski podaci izjednačavaju sa imovinom u tradicionalnom smislu, pa se i klasični propisi o krađi i pronevjeri mogu primjeniti na njih.[8]

Što se tiče prisluškivanja i presretanja komunikacija podataka, tradicionalni zakoni u većini pravnih sistema odnose se samo na presretanje govorne komunikacije, Njemačka, Italija Nizozemska i SAD, a ne i drugih sve širih oblika elektroničke komunikacije.[9]

Kompjuterska sabotaža

Osnovno obilježje ovog djela je prikriveno i podmuklo djelovanje u vršenju radne obaveze, čime se nanosi šteta drugima. U praksi su prisutni brojni oblici, kao i načini njihove realizacije. I u automatizovanom ambijentu sabotaže mogu imati različite forme, ali u osnovi postoje dvije tipične: fizička i logička. Ova posljednja je zbog svojih specifičnosti dobila i prefiks: kibersabotaža.[10] Pod sabotažom u fizičkom smislu podrazumjevaju se sva namjerna fizička oštećenja s ciljem privremenog ili trajnog onesposobljavanja rada računara ili računarskog sistema. Načini izvođenja mogu biti različiti, od presjecanja komunikacionih kablova, izlaganja sistema ekstremnim temperatutarama ili jakim magnetnim poljima pa sve do oštećenja izazvanih ubacivanjem stranih tjela u sklop elektronskih elemenata. Kao najčešći oblici logičkih sabotaža pojavljuju se brisanje, oštećenje ili modifikacija podataka, programa ili djelova operativnog sistema. Najprimjenjivija sredstva za izvršenje ovih oblika sabotaža jesu razni virusi.

Kada je u pitanju zakonodavna reakcija na kompjutersku špijunažu, onda se može reći da su tradicionalna zakonodavstva imala odgovor samo na oblike fizičke sabotaže i to one u kojoj su se kao predmet napada pojavljivali materijalni elementi računarskih sistema. Podaci sačuvani u elektronskom obliku nisu bili obuhvaćeni ovom zakonodavnom zaštitom.

U nekim zemljama vladalo je mišljenje kako je namjerno oštećivanje ili brisanje podataka, pohranjenih na nekom mediju (magnetni disk, magnetna disketa, magnetna traka), djelo oštećivanja stvari, jer se time oštećuje ili onemogućava normalno funkcioniranje tog medija. Međutim, čak i onda nisu obuhvaćene one situacije kada do toga nije došlo u času dok su se podaci nalazili na nekom nosiocu, već u unutrašnjoj memoriji kompjutera ili u toku prijenosa komunikacijskim kanalima. U nekim krivičnim zakonima, kao što je to slučaj u

[8] Sieber, U., *Legal Aspects of Computer Related Crime in the Informatin Society*, str. 72., prema Dragičević, D., *Kompjuterski kriminalitet i informacijski sustavi*. Zagreb: Informator, 1999., str. 128.
[9] Ibidem, str. 155.
[10] Petrović, S., *Kompjuterski kriminal*. Beograd: MUP R Srbije, 2001.,str. 139.

Belgiji ili Australiji, samo brisanje podataka bez oštećivanja fizičkog medija nije ispunjavalo biće djela o oštećivanju stvari, budući da se električni impulsi ne mogu smatrati "tjelesnom imovinom" a ometanje korištenja fizičkih medija nije se smatralo uništenjem.[11] Da bi se riješile takve nedoumice u većini se zemalja pristupilo nadopuni postojećeg zakonodavstva. Takve su promjene napravljene u Austriji, Kanadi, Danskoj, Njemačkoj, Finskoj, Francuskoj, Japanu i Nizozemskoj. Ali je i tu pristup bio različit. Neke zemlje (posebno Japan) pokrivaju sve vrste dokumenata, a ne samo kompjuterske podatke. Druge (Austrija, Njemačka, Francuska, Nizozemska, Novi Zeland, Španija i Velika Britanija) posebno štite integritet kompjuterskih podataka. Neke uključuju posebne kvalifikacije za kompjuterske sabotaže koje mogu dovesti do opstrukcije poslovanja ili značajnijih šteta na kompjuterskim sistemima s podacima o stanovništvu, nacionalnoj sigurnosti, pravnom sistemu ili administraciji.[12]

Kompjutersko krivotvorenje

Osnovno obilježje ovog djela je stvaranje lažnih ili prepravljanje pravih predmeta radi pribavljanja određene protivpravne koristi, a način realizacije može biti manuelan ili automatizovan. Tipični oblici falsifikovanja odnose se na falsifikovanje dokumenata (isprave, svjedočanstva, diplome, uvjerenja i sl.), znakova za vrijednost (poštanske i taksene marke), znakova za obilježavanje roba, novca, potpisa, pečata, štambilja i žigova te hartija od vrijednosti (mjenice, čekovi, kreditna pisma, nalozi za plaćanje i sl.).[13] Uvođenjem računara i računarske tehnologije u proces, poboljšava se kvalitet proizvoda krivotvorenja ali raste i sposobnost reprodukcije mnogo većeg broja primjeraka krivotvorina čime se pred zajednicu postavlja otvoreni zahtjev za reagovanje i efikasnije suzbijanje. Pored navedenih predmeta, sve češće se kao meta krivotvorenja pojavljuju elektronska pošta, telebanking, elektronsko poslovanje.

Zakonski propisi kojima se štiti vjerodostojnost i izvornost takvih dokumenata su propisi o krivotvorenju. Karakteristično je, međutim, da većina zakonodavstava ne sadrži dovoljno široko tumačenje oblika dokumenata (Austrija, Belgija, Njemačka, Francuska, Italija, Švicarska). Djelo krivotvorenja odnosli se samo na vidljivo čitane dokumente, tj. one dokumente koji se nalaze na takvom mediju s kojeg ih je moguće neposredno pročitati bez ikakve pomoći. Zbog toga se ti propisi nisu mogli primjeniti i na dokumenta u digitalnom obliku, koji šta više i ne moraju biti na fičkom mediju; mogu se nalaziti u postupku obrade ili prijenosu unutar mreže ili između udaljenih kompjutera. S namjerom da se elektronskim dokumentima pruži ista pravna zaštita kao i onima na papiru, neke zemlje – kao što su Australija, Kanada, Njemačka, Finska, Francuska, Grčka, Japan, Luksemburg, Velika Britanija i Norveška- donijele su ili predložile nove zakonske odredbe o krivotvorenju kojima se napušta nužnost vizualnog zapažanja.[14]

---

[11] Sieber, U., *Legal Aspects of Computer Related Crime in the Informatin Society*, str. 75., prema Dragičevlć, D., *Kompjuterski kriminalitet i informacijski sustavi*. Zagreb: Informator, 1999., str. 128.

[12] Dragičević, D., *Kompjuterski kriminalitet i informacijski sustavi*. Zagreb: Informator, 1999., str. 156.

[13] Petrović, S., *Kompjuterski kriminal*. Beograd: MUP R Srbije, 2001. str.133.

[14] U Kanadi-član 321. Krivičnog zakona, Njemačkoj- član 269, 271, 273, 274, 348. Krivičnog zakona, Finskoj- pog. 33. član 1-6 Krivičnog zakona, Francuskoj- član 462-5 i član 462-6 Krivičnog zakona, Grčkoj- član 13.C Krivičnog

Kompjuterska prevara

Osnovno obilježje ovog djela je dovođenje nekog u zabludu da bi se time pribavila protivpravna imovinska korist. Broj oblika prevara, kao i načina njihove realizacije je praktično neograničen i u praksi se susrećemo kako one vrlo primitivne i grube, tako i one kod kojih učinioci ispoljavaju veliki stepen vještine i rafiniranosti. Ipak se kao najtipičnije izdvajaju prevare povezane sa osiguranjem, porezima i taksama, penzionim fondovima, socijalnom pomoći i lažnim predstavljanjem.[15] Tipični načini izvršenja su svakako i danas prisutni ali značajnu pažnju treba posvetiti i oblicima prevara u kojima se koriste razni oblici kompjutersko-informatička tehnologije.

U odnosu na druge zloupotrebe, kompjuterske se prevareare odlikuju velikom raznolikošću i mnogobrojnošću pojavnih oblika i njihovih varijacija. Zato ne iznenađuje što se na takve zloupotrebe u tradicionalnim zakonodavstvima pokušalo odgovoriti na različite načine, brojnim već postojećim inkriminacijama, kao što su krivična djela krađe, prevareare, pronevjere, zloupotrebe povjerenja itd. Pokazalo se ipak da se i na području kompjuterske prevareare zatečeni propisi o krađi, kao zaštiti tjelesnih dobara, ne mogu valjano primjeniti na zaštitu podataka koji se nalaze u digitalnom obliku. Naročito u zemljama kontinentalnog prava u čijim se zakonskim opisima djela tražilo "varanje" neke osobe, što nije moguće primenjiti i na slučajeve kada je "prevaren stroj", tj. kompjuter.[16]

Zakonske odredbe o zloupotrebi povjerenja koje postoje u nekoliko zemalja, kao što su Austrija, Belgija, Njemačka, Francuska, Japan, Luksemburg ili Švicarska (i kod nas, član 287. KZFBiH[17]) primjenjuje se samo na počinitelje na visokom položaju a ne i na operatere, programere ili druge djelatnike. Zbog tih razloga, mnoga su zakonodavstva prihvatila rješenje *de lege lata* kako bi izbjegli širenje formulacije postojećih propisa, i unijeli u zakone nove odredbe o kompjuterskoj prevariari. Takva je nadopuna krivičnog zakonodavstva učinjena u Australiji, Austriji, Danskoj, Njemačkoj, Finskoj, Grčkoj, Luksemburgu, Japanu, Nizozemskoj, Norveškoj, Španiji, Švedskoj i SAD-u.[18]

---

zakona, Japanu- član 7-2, 157, 161-2 Krivičnog zakona, Luksemburgu- član 509-4 i 509-5 Krivičnog zakona, Norveškoj- član 179., 182. Krivičnog zakona.- Sieber, U., *Legal Aspects of Computer- Related Crime in the Information society*, str.80., prema Dragičević, str. 158.

[15] Petrović, S., *Kompjuterski kriminal*. Beograd: MUP Rsrbije. 2001.

[16] Naime, tradicionalne inkriminacije prevareare u zemljama kontinentalnog prava, (kao što je to i kod nas slučaj, član 282. KZFBiH), zahtjevaju kao element bića krivičnog djela dovođenje u zabludu druge osobe. S druge strane postojeće zakonske definicije krađe i pronevjere u mnogim se pravnim sistemima uslovljavaju počiniteljevom radnjom kojom se oduzima neka "stvar", odnosno neki predmet koji je vlasništvo druge osobe (npr. Austrija, Njemačka, Luksemburg ili Grčka). To dakako nije slučaj kada su u pitanju digitalni podaci, npr. digitalni novac ili isprave, koji u biti i nisu ništa drugo do informacija pohranjena na mediju, u memoriji kompjutera ili u prijenosu putem komunikacijskih kanala, a ne neki tjelesni, fizički predmet. – Dragičević D., *Kompjuterski kriminalitet i informacijski sustavi*, Zagreb: Informator, 1999.

[17] "Ko zastupajući imovinske interese neke osobe ili starajući se o njenoj imovini ne ispuni dužnost ili zloupotrijebi date mu ovlasti u namjeri da time pribavi sebi ili drugome kakvu imovinsku korist ili da ošteti osobu čije imovinske interese zastupa ili o čijoj se imovini stara, kaznit će se novčanom kaznom ili zatvorom do jedne godine." KZFBiH, Službene novine FBiH bnroj 43/ 98.

[18] Sieber,U., *Legal Aspects of Computer Related Crime in the Information Society*, str 81.

Izvori

- Masleša R.: Teorije i sistemi sigurnosti
- http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- Sieber, U., *Legal Aspects of Computer Related Crime in the Informatin Society*, str. 72., prema Dragičević, D., *Kompjuterski kriminalitet i informacijski sustavi*. Zagreb: Informator, 1999., str. 128.
- Petrović, S., *Kompjuterski kriminal*. Beograd: MUP R Srbije, 2001.,str. 139.
- Dragičević, D., *Kompjuterski kriminalitet i informacijski sustavi*. Zagreb: Informator, 1999., str. 156.