

DIGITALNA ANTI-FORENZIKA KAO KRIMINOGENO SREDSTVO ZAŠTITE KIBER KRIMINALA

mr Zoran Milanović¹, dipl. maš. inž. i Tanja Milanović², dipl. maš. inž.
mzt@eunet.rs

Rezime: Shodno duhu našeg vremena sa eksplozivnim razvojem i primenom informaciono-komunikacionih tehnologija i njihovog rapidnog širenja, paralelno su se razvijala i sredstva kriminogenog karaktera kao što su anti-forenzičke metode i tehnike. Intenzivan razvoj i izučavanje anti-forenzike, danas omogućava da se na lak i jednostavan način sakriju, modifikuju, uklone i/ili unište validni digitalni dokazi, kao i drugi vitalni podaci i informacije koji bi mogli da pomognu u rešavanju sudskog spora. S tim u vezi ovaj rad pored edukativno-teorijskog značaja definisanjem termina, kategorizacijom anti-forenzičkih tehnika i koncipiranjem opštih smernica za zaštitu forenzičkog integriteta daje praktičan doprinos istraživanju konkretnih situacija koje treba da ukažu na široku lepezu opasnosti i mogućnosti, kako bi se na vreme inicirale adekvatne mere i akcije radi suzbijanja, suprotstavljanja i sprečavanja širih negativnih posledica.

Ključne reči: Digitalni dokaz, Digitalna forenzika, Digitalna anti-forenzika.

Uvod

Danas se posebna pažnja posvećuje zaštiti **informacija** i **znanju** kao najvažnijim resursima za organizaciju, instituciju ili pojedinca. Bezbednost informacija i informacionih procesa postaje prioritetna za očuvanje poslovnih i svih drugih društvenih procesa, jer ko poseduje informaciju on ima sve.

Informaciona pismenost u sve većoj meri postaje glavna odrednica vremena u kojem živimo, a poznavanje **bezbednosnih problema** postaje jedan od elemenata opšte kulture, dok za informatičare i neke specifične profesije (vojska, policija, sudstvo, tužilaštvo) i deo njihovih profesionalnih obaveza. Iz tog razloga neophodno je utvrditi „kućni red“ koji treba da definiše sistem u kome se zna ko, šta, kada i kako treba, može i mora da radi, tj. koja određuje šta se smatra prihvatljivim i kakve su sankcije za neprihvatljivo ponašanje. Pored toga, one, s jedne strane, predstavljaju "temelj" na kojem će se nadograditi sistem zaštite, a s druge strane, predstavljaju kohezivne spone koje sva ostala sredstva, mere i procedure povezuju u jedinstven zaštitni mehanizam, pretvarajući klasičnu lančanu u mrežnu zaštitu, sa svim prednostima koje takav oblik zaštitnog mehanizma nosi sa sobom: kod lančane zaštite pucanje jedne karike dovodi do raspada celog sistema, dok pucanjem jedne spone na mreži nastaje "problem", ali sistem opstaje, njegova funkcionalna sposobnost jeste umanjena, ali nije neutralisana.

Kada se govori i razmišlja o bezbednosti i zaštiti računarskih sistema posebno je značajno mesto i uloga koju računar ima u tim procesima i to kroz nekoliko sledećih načina:

- računar kao objekat napada,
 - računar kao subjekat napada (sredstvo izvršenja),
 - računar kao sredstvo za prikrivanje ili planiranje i rukovođenje realizacijom kriminalnih aktivnosti,
 - računar kao simbol za obmanu,
 - računar kao sredstvo za sprečavanje, razjašnjavanje i dokazivanje kriminalnog dela.
- [2]

¹ Kriminalističko-policijska akademija, Beograd

² T.P. Laser d.o.o., Beograd

Naučna disciplina koja izučava i istražuje digitalne dokaze u svim navedenim kriminalnim aktivnostima, u kojima računarski sistem ima glavnu ili značajnu ulogu, zove se **digitalna** ili **računarska forenzika**.

Digitalni dokazi

Da bi se dokazalo neko krivično delo neophodno je prikupiti dokaze. Međutim, kada je reč o računarskim kriminalnim delima mora se imati u vidu da „digitalni dokazi“ često nisu jednaki ostalim oblicima fizičkih dokaza³ u odnosu na koje su osetljiviji i podložni menjanju strukture i sadržaja, te se prema njima treba posebno odnositi.

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje. Dokazi mogu potvrditi ili oboriti hipotezu pa je njihov integritet ključna stvar u njihovom prihvatanju odnosno odbacivanju pred sudom. Postoji nekoliko specijalnih karakteristika digitalnog dokaza koje ih čine posebno izazovnim. Pre svega potrebno je jasno i precizno definisati digitalni dokaz. Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja učestvuje u sudskom procesu ili nekom drugom sporu. Digitalna forma po svojoj prirodi podrazumeva da se radi o nekom elektronskom ili magnetnom uređaju pa to mogu biti podaci u operativnoj memoriji, na hard disku, *flash* karticama, ali i podaci koji se nalaze u transmisiji npr. radio talasi. Digitalni dokaz nije nešto što ljudi mogu na prvi pogled protumačiti. U bukvalnom smislu digitalni dokaz predstavlja niz nula i jedinica koje neki elektronski uređaj prevodi u ljudima razumljivu formu koju oni mogu koristiti kao potkrepljenje svojoj hipotezi u okviru nekog sudskog slučaja⁴.

Digitalni dokazi mogu biti bilo kakav niz bitova i bajtova na disku računara ili dugom memorijskom sistemu, i to su najčešće neki: **sistemske** (*swap* fajl, log fajl, konfiguracioni fajlovi i folderi...), **korisnički** (dokumenti i tekstualni fajlovi, tabele, slike, baze podataka, audio-video, arhivirani fajlovi, privremeni fajlovi, *backup*, sakriveni i šifrovani fajlovi, obrisani i preimenovani fajlovi ...) ili **Internet** (Internet adrese, *e-mail*, *cookies*, *bookmark*, *history*...).

Nauka o digitalnim dokazima je standardizovana u ISO/IEC 27037⁵ (prikupljanje i čuvanje digitalnih forenzičkih dokaza) i kroz: *SWGDE – Scientific Working Group on Digital Evidence* i *IOCE – International Organization on Computer Evidence*^{6 7}. U okviru njih su izdate preporuke za osnovne principe forenzičke analize digitalnih dokaza, kriterijumi, standardne radne procedure za: zaplenu računara, forenzičku akviziciju i analizu, čuvanje, kopiranje originalnih digitalnih dokaza, i dr.

Za dobijanje digitalnih dokaza u forenzičkom postupku postoji mnogo razvijenih **tehnika** i **alata** koji se danas koriste, a njihov prevelik značaj povezan je sa činjenicom „da danas preko 90 posto svih novih informacija je proizvedeno u digitalnom obliku^{8 9}“, i da se takvo bogatstvo mora na adekvatan način kontrolisati, nadgledati i čuvati.

Razvoj forenzičkih alata usavršavao se kroz tri generacije. Prvu generaciju su sačinjavali razni alati za: slike, dokumenta, pretraživanje i oporavak sistema; drugu

³ Bequai A., *op.cit.*, str. 45-47; Sieber U., *THE INTERNATIONAL HAND-BOOK INCOMPUTER CRIME*, John Wiley&Sons, 1986, str. 139-142.

⁴ http://www.ecdlcentar.com/baza/ecdl_informacije/it-vestak-cd-2009/ZBORNIK%20RADOVA%20ZITEH%2006

⁵ <http://www.iso27001security.com/html/27037.html>

⁶ http://www.theiai.org/disciplines/digital_evidence/index.php

⁷ <http://www.albany.edu/crccp/resources.html>

⁸ http://www.paho.org/English/DPI/Number14_article4_5.htm

⁹ http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Computer_Forensics_Emerges_as_an_Integral_Component_of_an_Enterprise_Information_Assurance_Program.htm

generaciju su činili posebno dizajnirani i razvijeni profesionalni alati (*Encase, SANS, Helix* itd.), kao i veliki broj besplatnih alata otvorenog koda koji se mogu naći i preuzeti sa Interneta; treću generaciju čine inteligentni alati koji u realnom vremenu, bezbedno i efikasno nadgledaju celokupan mrežni saobraćaj.

Naravno, svi destruktivni korisnici pokušavaju da prikriju i uklone tragove, tako da su najkvalitetniji digitalni dokazi po pravilu uvek nevidljivi za standardne alate iz operativnog sistema.

Neki autori koriste model „ledenog brega“ (slika 1) kako bi prezentovali problem sadržaja digitalnog dokaza, pri čemu se u literaturi mogu sresti različite interpretacije, ali svi mali vidljivi vrh ledenog brega poistovećuju sa elementima koji se lako prepoznaju i otkrivaju na jednom računarskom sistemu uz standardne alate operativnog sistema, dok se ispod površine ili u „dubokoj vodi“ nalaze teško dostupni elementi i digitalni dokazi koji su skriveni u privremenim fajlovima/folderima, obrisanim particijama diska, obrisanim mejlovima itd.



Slika 1 – Ledeni breg - vidljivi i nevidljivi nivo DIGITALNIH DOKAZA

Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, je da bude sertifikovan i priznat od državnih sudskih organa, kako bi digitalni dokazi bili validni u sudskom procesu.

Preporuke **profesionalaca** je da se forenzički alati i tehnike ne primenjuju na „živim“ podacima, već da se naprave njihove kopije, i da nikad, baš nikad, ne eksperimentišu korisnici koji nisu za to obučeni, jer će skoro sigurno oštetiti ili izgubiti potrebne digitalne dokaze.

Interesantno je i to, da profesionalci koji se bave digitalnom forenzikom ljubomorno skrivaju tajne svog zanata, jer kad ne bi bilo tako, njihov posao bi bio kudikamo teži. Uspešnost forenzičara obrnuto je proporcionalna znanju korisnika koji je bio cilj njegovog istraživanja. Forenzičari za razliku od drugih ICT¹⁰ specijalista moraju poznavati i poštovati pravilnike i uredbe o veštačenju i moraju svaki svoj korak evidentirati kako bi se njihov rad mogao smatrati objektivnim i validnim za sudski proces.

¹⁰ Information and communication technologies

Digitalna forenzika

Digitalna forenzika je fascinantno polje, jer kako organizacije postaju složenije i imaju veliku razmenu podataka i informacija na mreži, tako se i visokotehnološki kriminal razvija, velikom brzinom i u stalnom je porastu. Digitalno doba je proizvelo mnogo novih zanimanja, a jedno od najneobičnijih je digitalna forenzika, jer se bavi primenom zakona u nauci. Iako je sličan drugim oblicima pravne forenzike, digitalni forenzički proces zahteva ogromno poznavanje hardvera i softvera kako bi se izbeglo slučajno uništavanje dokaza, kao i očuvanje dokaza za kasnije analize.[3]

Digitalna forenzika je nauka koja predstavlja spoj tehnologije i znanja sa ciljem utvrđivanja na koji način računarski sistemi učestvuju u određenim kriminalnim radnjama. Nauka o digitalnoj forenzici obuhvata poznavanje metoda i procedura koje se primenjuju u analizi i prikupljanju podataka (dokaza). Tehnologija s druge strane predstavlja razne alate koji omogućavaju primenu metoda i procedura digitalne forenzike.

Pod **digitalnom forenzikom** podrazumevaju se metode prikupljanja, zaštite, analize i prezentacije dokaza koji su prihvatljivi za Sud¹¹, a mogu se naći na svim nosiocima digitalnih podataka. Pri tom je važno napomenuti da sami mediji i podaci ne predstavljaju dokaz, nego su samo potencijalni izvor dokaza. Pojam digitalna forenzika odnosi se na kvalitet i originalnost sačuvanih i generisanih digitalnih dokaza, kao npr. digitalni audio i video, digitalna fotografija, digitalni tekstovi i sve druge digitalne podatke koji su smešteni na stabilnim i prenosnim računarima, serverima, prenosnim memorijskim uređajima i drugim medijima, kao i dokaze sa Interneta.

Informacioni sistemi sami za sebe, sadrže značajne količine podataka koji se mogu iskoristiti kao dokazni materijal. Uklanjanje takvih dokaza je takođe mnogo teže nego što se uobičajeno misli da jeste. Metodama i alatima digitalne forenzike mogu se pronaći i otkriti takvi dokazni materijali koji su obrisani ili izgubljeni, pa čak i ako su podaci namerno uništeni.

Uloga i doprinos digitalne forenzike je dvojak: prvo dokazni materijal se može iskoristiti za utvrđivanje i otkrivanje slabih mesta, kao i poboljšanje postojećih zaštitnih mera, a drugi, da po potrebi i odluci najvišeg rukovodstva organizacije, digitalni dokazi budu izneti pred Sud. Takođe, sve je više velikih, privatnih kompanija koje koriste digitalnu forenziku kao vid unutrašnje kontrole svojih zaposlenih, pravdajući to prevencijom.

Digitalna anti-forenzika

Ne postoji generalni okvir u kome se može analizirati anti-forenzička situacija, već se sagledava kroz prizmu različitih aspekata i brojnih definicija eminentnih naučnika i praktičnih iskustava forenzičkih istražitelja.

Jednu od najčešće navođenih i prihvaćenih definicija dao je *dr Marc Rogers* sa *Purdue Univerziteta*, koji koristi više tradicionalan pristup „mestu zločina“. Anti-forenzika predstavlja „pokušaj da se negativno utiče na postojanje, obim i/ili kvalitet dokaza na mestu zločina, ili da se oteža istraživanje i analiza dokaza, ili potpuno onemogući njihovo izvođenje“¹².

Scott Berinato smatra da je anti-forenzika više od tehnologije i daje nešto jednostavniju definiciju u svom članku „Uspon anti-forenzike“ u kome kaže da je anti-forenzika pristup hakerisanju koji bi se ukratko mogao opisati: „Otežajte im da vas nađu i

¹¹ <http://www.coventry.ac.uk/researchnet/safe/a/2572>

¹² http://en.wikipedia.org/wiki/Anti-computer_forensics

onemogućite im da dokažu da su vas našli“¹³. Interesantno je da ni ovaj autor ne uzima u obzir korišćenje anti-forenzičkih metoda u zaštiti privatnosti ličnih podataka.

Zatim, *Peron* i *Legary* smatraju da je anti-forenzika način da se „ograniči identifikacija, prikupljanje, upoređivanje i validnost elektronskih podataka...“, a *Grugq* iznosi da je anti-forenzika „pokušaj da se smanji broj i kvalitet forenzičkih dokaza“. *Ryan Harris* (2006.) daje definiciju zasnovanu na terminima „dokaz“ i „proces“ koja glasi: anti-forenzika je bilo koji pokušaj da se kompromituje dostupnost i korisnost dokaza u forenzičkom procesu.¹⁴

Na osnovu svega navedenog može se zaključiti da anti-forenzika predstavlja alate i metode koje se koriste za sprečavanje stručnih službi u sistemu krivičnog pravosuđa u izvođenju forenzičke istrage i primene nauke u dokazivanju i izvođenju validnih digitalnih dokaza.

U naučno-stručnim krugovima vlada kontraverzno mišljenje o ulozi i značaju anti-forenzike, pri čemu se sukobljavaju dva dominantna pristupa od kojih jedan ima isključivo negativnu konotaciju korišćenja anti-forenzičkih alata i smatra da su isključivo zlonamerno dizajnirani, dok suprotstavljeno mišljenje ima pozitivno gledište tj. da se ovi alati mogu iskoristiti u ilustraciji nedostataka u sudskim digitalnim procedurama, forenzičkim alatima, kao i nedostataka u obrazovanju forenzičkih istražitelja. Najveći zagovornici ovog stava su *James Foster* i *Vinnie Liu* (2005.) koji su izneli mišljenje da će ubuduće forenzičari morati da ulože više napora da bi dokazali da su prikupljeni dokazi i tačni i pouzdani. Oni takođe veruju da će ovo dovesti do boljih forenzičkih alata i unaprediti obrazovanje samih forenzičkih istražitelja.

Anti-forenzičke metode i tehnike

Sa razvojem znanja u oblasti digitalne forenzike rastu i znanja u oblasti anti-forenzike. Svakodnevno sve više softverskih proizvoda vide svetlost dana, što će svakako u mnogome uticati na učinak digitalne forenzičke istrage.

U literaturi su date različite kategorizaciji anti-forenzičkih metoda, a jedna od najcelishodnijih i najpoznatijih je *Rogers*-ova¹⁵:

- sakrivanje podataka (data hiding),
- uništavanje korisničkih objekata (artifact wiping),
- prikrivanje traga tj. putanje (trail obfuscation),
- delovanje protiv digitalnih forenzičkih procesa/alata (attacks against the CF process/tools).

Sakrivanje podataka je proces kojim se otežava pronalaženje podataka pri čemu ostaju dostupni za kasniju upotrebu. Neki od najčešćih oblika skrivanja podataka su: enkripcija (šifrovanje), steganografija i neki drugi hardversko-softverski oblici. Svaka od ovih metoda u mnogome otežava i usporava samu forenzičku istragu. Kombinovanjem više različitih metoda skrivanja podataka, čini forenzičku istragu skoro nemogućom.

- **Enkripcija** ili šifriranje je proces u kriptografiji kojim se vrši izmena podataka tako da se poruka odnosno informacija, učine nečitljivim za osobe koje ne poseduju određeno znanje (ključ)¹⁶, a takođe je jedna od najčešće korišćenih anti-forenzičkih tehnika, za koju *Paul Henry* kaže da predstavlja „noćnu moru“

¹³ *Berinato, S., The Rise of Anti Forensics, 2007.*

http://www.csoonline.com/article/221208/The_Rise_of_Anti_Forensics

¹⁴ <http://www.dfrws.org/2006/proceedings/6-Harris.pdf>

¹⁵ http://cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005.pdf

¹⁶ <http://bs.wikipedia.org/wiki/Enkripcija>

forenzičkih analitičara¹⁷. Većina javno dostupnih programa za šifriranje omogućava korisniku da napravi virtualne šifrirane diskove koji mogu biti otvoreni samo određenim ključem. Primenom savremenih algoritama za šifriranje i različite tehnike enkripcije ovih programa onemogućavaju čitanje podataka bez odgovarajućeg ključa. Enkripcija fajla podrazumeva samo šifriranje sadržaja, što ostavlja važne informacije kao što su ime fajla, veličina i vreme kreiranja, pristupa, modifikovanja i brisanja neenkriptovanog fajla. Delovi sadržaja ovog fajla mogu biti rekonstruisani sa drugih lokacija, kao što su privremeni fajlovi, *swap* fajlovi i obrisane, neenkriptovane kopije. Široka dostupnost i laka primena ovih softvera sve više otežava rad digitalne forenzike. Najčešće korišćeni alati su: *FreOTFE*, *TrueCrypt*, *Cryptainer LE*, *CryptoExpert Lite*, *CompuSec*, *E4M Disk Encryption*, *Scramdisk Encryption*;

- **Steganografija** je tehnika koja se bavi sakrivanjem i otkrivanja skrivenih informacija ili fajlova unutar drugih fajlova. U novije vreme, primenu je pronašla u Internet komunikacijama, kao način da se u video ili audio fajlove ugrade skrivene poruke. Za razliku od enkripcije, kod koje se šifrovana poruka vidi, ali može da bude pročitana samo uz pomoć odgovarajućeg ključa, steganografija omogućava da poruka bude u potpunosti sakrivena. Fajl u koji se poruka unosi izgleda kao i original, bez poruke. Na taj način, .bmp, .wav, .au, .gif ili .jpg fajl mogu da nose skriveno značenje, a da onaj ko gleda (sluša) ne primećuje ništa "sumnjivo". Ugrađivanje poruke moguće je zahvaljujući programima kakvi su "*Steghide*", "*Hide and Seek*" ili "*Snow*", koji daju proizvod sličan digitalnom vodenom žigu, koji se upotrebljava kod fajlova radi zaštite autorskih prava. Treba napomenuti da nisu svi digitalni fajlovi pogodni za skrivanje tajni. Na primer, u izvršnim verzijama programa važan je svaki bit pa promena samo jednog bita može izazvati neispravan rad programa.
- **Ostali oblici skrivanja podataka** podrazumevaju korišćenje alata i tehnika za skrivanje podataka na različitim lokacijama na računaru kao što su: memorija, skriveni folderi, alternativni tokovi podataka, *bad* sektori, skrivene particije, mrtvi prostor (*slack space*) itd. Jedan od najpoznatijih alata koji se koristi je *Slacker* (deo *Metasploit Framework*) koji deli fajlove i smešta svaki deo u mrtvi prostor drugih fajlova čime se oni skrivaju od softvera za forenzičku istragu. Sledeća tehnika za skrivanje podataka je korišćenje *bad* sektora. Korišćenje ove tehnike podrazumeva da korisnik promeni određeni sektor iz dobrog u loši a potom podatke smešta u taj klaster. Forenzički alati vide ove klasterne kao loše i nastavljaju bez ispitivanja njihovog sadržaja.

Uništavanje korisničkih objekata ovom metodom se trajno eliminišu određeni ili čitave grupe fajlova/foldera koje je korisnik kreirao u sistemu. To se postiže upotrebom različitih metoda koje uključuju programe za čišćenje diskova, namensko brisanje fajlova i tehnike za razmagnetisavanje tj. uništavanje diskova. Programi za **čišćenje diskova** koriste različite metode za prepisivanje preko postojećih fajlova. Programi za **brisanje fajlova** se koriste za uklanjanje fajlova iz samog operativnog sistema. Prednost ovih programa je da ostvaruju svoj zadatak za kraće vreme i pri tome ostavljaju mnogo manje tragova nego programi za čišćenje diskova. Mana ovih programa što ne mogu u potpunosti da obrišu kompletne informacije o fajlu. Najčešće korišćeni programi su *R-Wipe & Clean*, *Eraser*, *Aevita Wipe & Delete* i *Cyber Scrubs Privacy Suite*. Sledeća grupa su **destruktivne tehnike** za razmagnetisavanje tj. uništavanje diskova koje podrazumevaju izlaganje digitalnih uređaja (diskova) magnetnom polju čime se brišu u potpunosti svi podaci koji su

¹⁷ http://layerone.info/archives/2006/Anti-Forensics-LayerOne-Paul_Henry.pdf

bili na njima. Metoda koja se koristi nešto češće od prethodne, je fizičko uništavanje uređaja i to: spaljivanjem, sečenjem, topljenjem itd.

Prikrivanje putanje je metod čija je svrha je da zbuni, dezorijentiše i preusmeri proces forenzičke istrage. Prikrivanje putanje obuhvata razne tehnike i alate koji uključuju čišćenje logova, *Spoofing* (metoda za zamjenu IP adresa), zombi nalog (program koji potajno preuzima kontrolu nad drugim umreženim računarom), trojanske komande itd. Jedan od najpoznatijih alata je *Timestomp* (deo *Metasploit Framework*) koji daje mogućnost korisniku da menja fajlove sa meta podacima koji se odnose na pristup, kreiranje i modifikaciju vremena/datuma. Korišćenjem ovog programa korisnik može da renderuje bilo koji broj fajlova, čineći ih beskorisnim u pravnom smislu, jer se dovodi u pitanje njihov kredibilitet. Drugi dobro poznat program za prikrivanje tragova je *Transmogripy* (takođe, deo *Metasploit Framework-a*). Ovaj program ima mogućnost da promeni informaciju u zaglavlju fajla i tako prikrije njegov identitet. Na primer, *.jpg zaglavlje može da se promeni u *.doc, tako da će program za forenzičku istragu koji traže slike, ovakav fajl preskočiti.

Delovanje protiv digitalnih forenzičkih procesa/alata. Direktni napadi na proces digitalne forenzike su najnoviji tipovi anti-forenzike i potencijalno njihove najveće pretnje, a svoje uporište nalaze u dobro dokumentovanim procedurama forenzičke istrage i nadaleko poznatim forenzičkim alatima koji na taj način postaju ranjivi i otežavaju forenzičarima da se na njih oslone¹⁸.

Napredna digitalna anti-forenzika

Napredna digitalna anti-forenzika se zasniva na radu sa alatima i programima koji se podižu (butuju) sa *CD/DVD* medija ili *flash* memorijama, pri čemu se celokupan rad odvija u radnoj memoriji (*RAM-u*) računara i njegovim isključenjem se gubi svaki eventualni digitalni dokaz, čime se u potpunosti onemogućuje forenzička istraga. Najčešći predstavnici su *LiveCD* i *BartPe* koji na sebi imaju operativni sistem i niz korisničkih aplikacija sa kojima se može izvrši kriminalno delo, a da pritom ne ostave nikakav trag.

Suprotstavljanje anti-forenzici

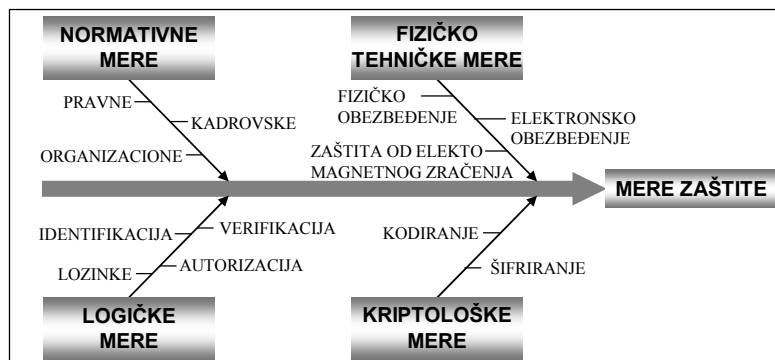
Zaštitne mere i rešenja koja će se primeniti u direktnoj su zavisnosti od stepena osetljivosti podataka i raspoloživosti finansijskih sredstava.

Zaštita računarskih sistema predstavlja izuzetno složen proces, koji se, posmatran u vremenu i prostoru, ni u jednom trenutku i ni u jednoj tački ne sme potceniti. Jer opasnosti koje, posredno ili neposredno, kontinuirano ili povremeno, ugrožavaju te procese, i u manjoj ili većoj meri predstavljaju pretnju sistemu i njegovim objektima, toliko su brojne, međusobno povezane i isprepletane da nad celim računarskim sistemom formiraju krajnje kompleksnu mrežu opasnosti. Upravo zbog toga potrebno je da se onemogućući svako slučajno ili namerno, iz bilo kojih neplaniranih i neočekivanih razloga, narušavanje, sužavanje ili sprečavanje funkcija računarskih sistema, odnosno otuđenje, uništenje, oštećenje, izmena ili neovlašćeno korišćenje informacionih resursa (hardvera, softvera, podataka itd.), i da se stvore svi neophodni uslovi, kako bi se funkcije odvijale, a podaci i informacije obrađivali i koristili na očekivan i unapred definisan način.

¹⁸ http://igneous.scis.ecu.edu.au/proceedings/2007/forensics/01_Kessler_Anti-Forensics.pdf

Protiv svih vidova anti-forenzike možemo se boriti primenom preventivnih mera zaštite, ali je neophodno dati što POTPUNIJE odgovore na sledeća „zlatna pitanja” o zaštiti računarskog sistema: ŠTA štititi? OD KOGA ili ČEGA štititi? ZBOG ČEGA štititi? ČIME štititi? KAKO štititi? [2]

Konkretan predlog zaštitnih mera, kao i pouzdan kriterijum njihovog izbora dat je na slici 2.



Slika 2 – „Riblja kost“ osnovnih mera zaštite [1]

Računarsko i mrežno okruženje unutar svake organizacije predstavlja komponentu koja povlači liniju između uspeha i neuspeha kompanije. Zato je važno znati da bezbednost predstavlja odgovornost svake osobe unutar organizacije čak i onih zaposlenih koji ne koriste računar u svom dnevnom poslu.

Zbog svega toga, jedan od prvih koraka i imperativ zaštite informacionih sistema je da svi korisnici i izvršioci svoju bezbednosnu kulturu i stručnost podignu na što viši nivo.

Zaključak

Ovaj rad je proistekao iz potrebe da se na jasan i transparentan način definiše veza i praktični koraci između zaštite informacionih sistema i anti-digitalne forenzike, kao i da se uoče njihove slabosti i promeni percepcija svih korisnika informacionih tehnologija, a sa ciljem unapređenja kvaliteta zaštite informacionih sistema i neometanog poslovnog procesa.

Ono što je sigurno, da će opseg i frekvencija računarskog kriminala biti u porastu, jer se povećava broj računara, automatizacija poslovnih aktivnosti i procesa, integracija računarskih mreža, kao i snižavanje praga znanja i stručnosti potrebnih za primenu ICT i širenja računarske pismenosti, koja već sada postaje glavna odrednica vremena u kome živimo.

Uspešne kompanije, nezavisno od strukture i veličine, u vremenu kada digitalni podaci i informacije imaju presudan značaj za uspeh i opstanak na tržištu, moraju sprovoditi edukaciju svojih kadrova, jer se protiv anti-forenzike ne mogu boriti neznanjem i nespremnošću. Ne treba se zavaravati, da ako do sada nisu imali problema sa kriminogenim ishodom, da ih neće ni biti. Ovde se ne postavlja pitanje da li će, nego kada će!?

Ne može se očekivati da se dobro i kvalitetno obavi današnji posao, sa jučerašnjim znanjima, i da se tako dočeka sutra.

Literatura

- [1] Milanović J. Zoran, Organizacija zaštite računarskih sistema, Magistarski rad, Mašinski fakultet – Beograd, 2006.
- [2] Petrović R. Slobodan, Kompjuterski kriminal, Ministarstvo unutrašnjih poslova Republike Srbije – Beograd, 2001.

- [3] Solomon M., Barrett D., Broom N., Computer Forensics Jumpstart, 2005.
- [4] Bequai A., op.cit., str. 45-47; Sieber U., THE INTERNATIONAL HAND-BOOK INCOMPUTER CRIME, John Wiley&Sons, 1986, str. 139-142.
- [5] http://www.ecdlcentar.com/baza/ecdl_informacije/it-vestak-cd-2009/ZBORNIK%20RADOVA%20ZITEH%2006
- [6] <http://www.iso27001security.com/html/27037.html>
- [7] http://www.theiai.org/disciplines/digital_evidence/index.php
- [8] <http://www.albany.edu/crcp/resources.html>
- [9] http://www.paho.org/English/DPI/Number14_article4_5.htm
- [10] http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Computer_Forensics_Emerges_as_an_Integral_Component_of_an_Enterprise_Information_Assurance_Program.htm
- [11] <http://www.coventry.ac.uk/researchnet/safe/a/2572>
- [12] http://en.wikipedia.org/wiki/Anti-computer_forensics
- [13] Berinato, S., The Rise of Anti Forensics, 2007.
http://www.csoonline.com/article/221208/The_Rise_of_Anti_Forensics
- [14] <http://www.dfrws.org/2006/proceedings/6-Harris.pdf>
- [15] http://cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005.pdf
- [16] <http://bs.wikipedia.org/wiki/Enkripcija>
- [17] http://layerone.info/archives/2006/Anti-Forensics-LayerOne-Paul_Henry.pdf
- [18] http://igneous.scis.ecu.edu.au/proceedings/2007/forensics/01_Kessler_Anti-Forensics.pdf