RESURSI ZA ISTRAGU KOMPJUTERSKOG KRIMINALA

Mr Miodrag Đorđević, dipl. inž.
Ministarstvo odbrane SCG

Kratak sadržaj

U radu su, na osnovu prakse razvijenih zemalja u informacionom pogledu, analizirani resursi neophodni za istragu kompjuterskog kriminala. Razmotreni su aspekti formiranja timova za korporacijsku i zvaničnu istragu kompjuterskog kriminala od strane nadležnih državnih organa. Dat je i pregled definicija krivičnih dela "protiv bezbednosti računarskih podataka" iz Krivičnog zakona Republike Srbije, što može poslužiti za analizu stanja u ovoj oblasti. Takodje, detaljno je razrađjena organizacija, metodologija rada i standardizacija procedura rada kibernetičkih interventnih timova za istragu kompjuterskog kriminala. Detaljno je obrađena obuka članova tima i dat je predlog programa tri teme za jednomesečnu obuku pojedinih specijalista za istragu kompjuterskog kriminala.

Ključne reči: ***kompjuterski kriminal, resursi za istragu, kibenetički interventni tim, kompjuterski incident, digitalni dokaz***

Abstract

In this paper, based on best practice in the ICT (Information Communication Technologies) developped countries, all necessery resources requested for computer crime investigation were analysed. Some relevant aspects of corporate CIRT (Computer Incident Response Team) establishing and law enforcement team for computer crime investigation were considered. A review of definitions of the criminal acts against computer's data security, from The Criminal Law of The Republic of Serbia was shawn and used for the present state cross-section analisis. Organization, metodology and standard operation procedure of the CIRT are analysed in details, too. Training program of the CIRT members and three four-weeks training caurses for computer crime investigation specialists were considered in particular.

Key words: ***computer crime, investigation resources, CERT, computer incident, digital evidence***

Uvod

Istragu događaja koji predstavljaju zloupotrebu u informacionim tehnologijama i kompjuterskog kriminala mogu efikasno vršiti samo visokospecijalizovani stručni kadrovi u interventnim timovima sa odgovarajućim resursima napadnute organizacije i nadležnih državnih organa. Takav pristup jedino omogućava valjanu istragu i način da se sakupe, sačuvaju i na sudu prezentiraju digitalni dokazi o izvršenom kompjuterskom incidentu kao dovoljna podloga za pravedno sankcionisanje učinjenog krivičnog dela u oblasti primene informacionih tehnologija. Uspešan i efikasan rad interventnih timova može se obezbediti samo odgovarajućom specijalističkom obukom visokostručnih kadrova-članova tima na nacionalnom i na nivou svake organizacije.

1. Interventni tim za korporacijsku istragu kompjuterskog kriminala

Prema iskustvima informatički razvijenih zemalja, treba izvršiti vlastitu inicijalnu istragu kompjuterskog incidenta na korporacijskom nivou organizacije, utvrditi karakter incidenta i, tek onda, doneti odluku o pozivanju zvaničnih organa istrage kompjuterskog kriminala.
Uloga korporacijskih organa (privatnih) za istragu zloupotreba u informacionim tehnologijama (IT) i kompjuterskog kriminala ograničena je zato što:

- većina organizacija nije opremljena odgovarajućom opremom za istragu i forenzičku analizu, i

- ovi organi istrage nemaju sva zakonska ovlašćenja da otkrivaju trag do napadača i zaplenjuju računarski sistem napadača kao dokazni materijal.

Dobro rešenje je angažovanje stručnog konsultanta za inicijalnu istragu, akviziciju i forenzičku analizu digitalnih dokaza, vlastitim snagama, najmanje do trenutka utvrđivanja prirode incidenta i donošenja odluke o (ne)uključivanju zvaničnih istražnih organa, što se najčešće čini. Nalaženje stručnog konsultanta za bezbednost IS nije lak zadatak (jer su takvi kadrovi malobrojni gotovo u svim zemljama sveta) i treba ga obaviti pre prvog slučaja kompjuterskog incidenta. Organizacija, može formirati svoj interventni tim za brzo reagovanje i istragu kompjuterskog incidenta, a prazninu u stalnom timu popuniti pridruženim kadrovima - stručnim konsultantom, najčešće tehničkim ekspertom u oblasti zaštite informacionog sistema (IS) ili nadzora sistema zaštite. Naravno, konsultant može biti i privatna informatička firma sa znanjem i iskustvom u ovoj oblasti, kadrovski i materijalno opremljena i osposobljena za istragu i forenzičku analizu digitalnih dokaza.

2. Interventni tim za zvaničnu istragu kompjuterskog kriminala

Uloga zvaničnih, po zakonu nadležnih, organa u istrazi kompjuterskog kriminala varira od države do države, a zavisi od osposobljenosti policijskih i istražnih organa za ovaj posao. Između brojnih razloga da organizacije ne pozivaju zvanične organe istrage, odmah po utvrđivanju informacije da se kompjuterski incident desio, navedimo:

1. Vrlo je verovatno da će događaj ubrzo postati javna informacija.
2. Zvanični istražni organi u toku istrage prekidaju sve komunikacije i onemogućavaju rad IS, nadzornih organa i personala zaštite IS, što je za mnoge organizacije neprihvatljivo.
3. Organizacije strahuju od gubljenja ugleda i poslovnog gubitka.
4. Opravdan je strah od kompromitacije kod hakera i ponavljanja napada, itd.

Glavna korist pozivanja i uključivanja zvaničnih organa u istragu je:

- korišćenje skupe tehnologije (tehnika i alata) za akviziciju i forenzičku analizu digitalnih dokaza,
- uključivanje stručnih i ekspertskih kadrova u istražni postupak, forenzičku analizu i sudsko veštačenje kriminala u IT.

3. Kratak prikaz dela protiv bezbednosti računarskih podataka u SCG

U cilju analiziranja stanja u svetu i u nas u DZ SCG, daje se ukratko pregled sa definicijom krivičnih dela protiv bezbednosti računarskih podataka [11]:

1. ***Neovlašćeno korišćenje računara i računarske mreže*** je oštećivanje, prikrivanje, brisanje, izmena ili neki drugi način kojim se učini neupotrebljivim računarski podatak ili program.
2. ***Računarska sabotaža*** je uništavanje, brisanje, izmena, oštećivanje, prikrivanje ili neki drugi način kojim se učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka koji je od značaja za državni organ, javnu službu, ustanovu, preduzeće ili drugu organizaciju.
3. ***Pravljenje i unošenje računarskih virusa*** može biti sa ili bez namere da se prouzrokuje šteta tuđem računaru ili računarskoj mreži.
4. ***Računarska prevara*** je unošenje netačnog podatka ili ne unošenje važnih podataka ili na drugi način prikrivanje podataka i uticanje na rezultat elektronske obrade i

prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu.

5. ***Ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže*** je neovlašćeni pristup elektronskoj obradi podataka ili računarskoj mreži i izazivanje zastoja i poremećaj funkcionisanja elektronske obrade i prenosa podataka ili mreže.
6. ***Neovlašćeni pristup zaštićenom računaru ili računarskoj mreži*** je svaki neovlašćeni pristup računaru ili mreži uz nepoštovanje ili kršenje fizičkih i / ili elektronskih mera njihove zaštite.
7. ***Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži*** je neovlašćeno sprečavanje korisnika ili ometanje njegovog pristupa javnoj računarskoj mreži od bilo kog ili službenog lica.

Iz navedenog uočava se nedostatak, u našoj praksi, pravnog sankcionisanja "*odbijanja saradnje i nedavanje dokaza*" istražnim organima u cilju sprovođenja efikasne istrage kompjuterskog incidenta.

4. Formiranje korporacijskog interventnog kibernetičkog tima

Pojam interventnog kibernetičkog tima odnosi se na CIRT (***C**omputer **I**ncident **R**esponse **T**eams*) ili ređe na CERT (***C**omputer **E**mergancy **R**esponse **T**eams*) tipove kombinovanih, stručnih timova koje treba formirati, obučiti i sa njima rukovoditi. Oni obavljaju planski, prema utvrđenoj politici zaštite, sve radnje opisane u slučaju kompjuterskog incidenta [5].

Za formiranje kibernetičkih interventnih CIRT timova treba definisati organizacione i tehničke standarde, radne procedure i standarde dobre prakse, i nabaviti opremu sa potrebnim tehnologijama (tehnikama i forenzičkim alatima).

4.1. Standardizacija kibernetičkih interventnih timova (CIRT)

Formiranje, organizaciju kao i radne procedure CIRT tima treba standardizovati na nacionalnom nivou i uskladiti sa međunarodnim preporukama [6]:

1. Cilj: Standard se odnosi na praksu CIRT tima u korporaciji, a obuhvata sve korisnike koji imaju pristup IS i podacima.
2. Sertifikat: Standard propisuje profil lica iz organizacije nadležnog za formiranje CIRT tima (tipa CIO- ***C**hieff **I**nformation **O**fficer*, tj.glavnog specijaliste za zaštitu informacija).
3. Namena CIRT: Istraživanje kompjuterskih incidenata (događaja) u IS organizacije.
4. Misija CIRT: Ispitivanje očiglednih i nesumnjivih pokušaja zloupotrebe i upada u IS. **5. Opis:** Uloga CIRT tima je urgentna istraga kompjuterskog incidenta. Rukovodilac CIRT tima je CIO, koji je nadležan i odgovoran za sve aktivnosti CIRT tima.
6. Zadaci CIRT tima:

- Identifikacija napadnutih kritičnih sistema.
- Intervencija na sve bezbednosne incidente ili sumnjive incidente koji uključuju IS kompanije, računarsku mrežu (RM) i objekte podataka.
- Uspostavljanje 24-časovne direktne telefonske linije za izveštavanje o bezbednosnim kompjuterskim incidentima.
- Sakupiti tim najkasnije 3 sata nakon prijema izveštaja o bezbednosnom kompjuterskom incidentu.
- Izvršiti klasifikaciju bezbednosnih kompjuterskih incidenata koji zahtevaju istragu.

- Istraga i izveštavanje o svim dokazima nadležnim organima (menadžmentu).
- Procena nanete štete i obima upada.
- Kontrola i sprečavanje ponavljanja upada.
- Sakupljanje i dokumentovanje svih dokaza koji se odnose na bezbednosni kompjuterski incident, u skladu sa uspostavljenom procedurom.
- Održavanje i čuvanje svih dokaza, u skladu sa uspostavljenom procedurom.
- Registrovati sve korisnike procedure da bi se obezbedila zaštita dokaza
- Registrovati sve potencijalne korisnike, da bi se sprečio bezbednosni kompjuterski incident.
- Koordinirati oslanjanje na slične incidente ili pogođene tehnologije.
- Izabrati pomoćne članove tima za podršku istrage, u slučaju potrebe.
- Pratiti uputstvo za zaštitu privatnosti, uspostavljeno politikom zaštite kompanije.
- Obezbediti stalnu vezu sa zvaničnim organima istrage kompjuterskog kriminala i pravosudnim organima.

4.2. Organizaciona struktura kibernetičkih interventnih timova

Sastav CIRT tima čine: stalni članovi – jezgro tima, i pridruženi članovi za podršku.
CIO – tj. glavni specijalista za zaštitu bira jezgro tima i imenuje lidera CIRT tima.

I. Jezgro CIRT tima treba da ima najmanje 4 člana, odgovorna za**:**

- Određivanje da li incident zahteva dalju istragu.
- Kategorizacija bezbednosnog incidenta.
- Dodavanje pridruženih članova istrazi, ako je potrebno.

1. Rukovodilac servisa za nadzor (A*uditing service*) IS je član jezgra **CIRT tima**, a njegove dužnosti su:

- Obezbeđuje da se primeni procedura najbolje prakse u istrazi.
- Obezbeđuje nadzor procesa istrage.
- Obezbeđuje da se procedura lanca menadžmenta dokaza korektno sprovodi.
- Održava sistem odgovornosti za sve sakupljene dokaze u toku istrage.
- Dokumentuje sve aktivnosti istrage.

2. Administrator zaštite ili poverljivi provajder zaštite je član jezgra **CIRT tima**, a ima zadatak da:

- Informiše sve korisnike pogođene kompjuterskim incidentom o potrebi preduzimanja neophodnih akcija za kontrolu incidenta.
- Izvršava odgovarajuća traganja za napadačkim računarom, forenzičku analizu, i druge tehničke zadatke koje zahteva istražni postupak.
- Obezbeđuje analizu incidenta.
- Priprema konačni izveštaj i preporuke CIRT tima.
- Obezbeđivanje IT veštaka.

3. Administrator zaštite IS korporacije odgovoran je za:

- Obezbeđivanje veze sa zvaničnim organima istrage.
- Obezbeđivanje sprovođenja standarda najbolje prakse istrage.
- Lokalizovanje incidenta, ako je moguće.
- Menadžment procesa ispitivanja svedoka i osumnjičenih.

4. Predstavnik zakona (pravnik) je član jezgra CIRT tima sa odgovornostima:

- Ukratko upoznaje stalne i pridružene članove o zakonskim propisima o zaštiti privatnosti, zaštiti intelektualne svojine, proceduri istrage i zaplene računara za dokaz i zakonskim pitanjima prisluškivanja telefona osumnjičenog.
- Obezbeđivanje adekvatne zaštite prava osumnjičenog.
- Predstavnik je tima za odnose sa javnošću.
- Pregleda svaki članak u pripremi, pre objavljivanja u medijima.
- Pregleda svaki izveštaj mendžmenta.
- Radi kao lice za vezu sa zakonskim i pravosudnim organima.

II: Članovi za podršku su pridruženi (povremeni) članovi CIRT tima, i uglavnom su poznati eksperti u IT ili IT sudski veštaci.

IT eksperti mogu biti:

Specijalisti za platforme sa zadacima:

- Pregled log datoteka za nadzor (audit) sa izveštavanjem svih neobičnih ili sumnjivih aktivnosti.
- Izveštavanje o svakom neobičnom ponašanju kritičnih sistema.
- Da budu spremni da ukratko upoznaju CIRT tim sa radnim procedurama.
- Zaštita digitalnih kompjuterskih dokaza o incidentu prema uputstvu (proceduri) I instrukcijama jezgra tima.
- Procena nanete štete sistemu i/ili podacima i podnošenje izveštaja jezgru CIRT tima.
- Davanje stručne pomoći u određivanju obima upada u IS.
- Davanje stručne pomoći u identifikaciji tačke upada u IS i/ili izvora upada.
- Preporučuje mere zatvaranja tačaka upada u IS.

Finansijski inspektor (revizor) sa zadacima:

- Da ukratko upozna tim sa finansijskom problematikom i procedurom istrage.
- Da bude spreman da izvrši finansijsku kontrolu (reviziju), ako jezgro tima smatra da je to potrebno za potrebe istrage.
- Da izveštava o svojim nalazima jezgro CIRT tima.
- Da sledi procedure istrage kako je određeno od strane jezgra CIRT tima.

Istraživač prevara (pronevera) sa zadacima:

- Pruža pomoć stalnim članovima CIRT tima u otkrivanju i prepoznavanju prevara i pronevera u IS.
- Sledi uputstva i procedure za zakonsku pretragu.
- Sledi politiku zaštite privatnosti i tajnosti podataka kompanije.
- Pruža pomoć u identifikaciji objekata i materijala koji su korišćeni za izvršavanje prevare.
- U skladu sa uputstvom jezgra CIRT tima, čuva od izmene svaki sakupljeni dokaz sve dok se ne dostavi jezgru CIRT tima.
- Dostavlja CIRT timu dokaze i čuva ih sve do odluke o istrazi**.**
- Izveštava o svojim nalazima jezgro CIRT tima.

Lice za kadrovsko obezbeđenje sa zadacima:

- Savetuje stalne članove CIRT tima o personalnoj politici i procedurama.
- Daje preporuke i informacije menadžmentu kompanije o zaposlenim.
- Stara se o drugim pitanjima, uključujući sindikalne i druge specijalne ugovore.

Lice za odnose sa javnošću sa zadacima:

- Jedini je odgovoran za kontakte sa javnošću (medijima).
- Prima pravne savete pre svakog intervjua, konferencije za štampu ili puštanja vesti u medijima.
- Obezbeđuje potvrdu od CIRT tima da svaki intervju ili puštanje vesti u medijima neće uticati na istragu.
- Obaveštava sve druge pogođene korisnike da mu proslede svaki zahtev medija za informacijama.

III. Rukovodilac CIRT tima

Rukovodioca CIRT tima imenuje CIO iz redova jezgra tima. Rukovodilac može biti stalna ili rotaciona funkcija što je diskreciono pravo CIO.

Zadaci rukovodioca CIRT tima su da:

- Zakazuje i vodi sastanke CIRT tima.
- Kontaktira lice za odnose sa javnošću (PR).
- Periodično izveštava nadležni organ (CIO) o statusu istrage.
- Vodi istragu i koordinira aktivnosti tima
- Preuzima odgovornost za verifikaciju čuvanja dokaza u celom lancu istrage.
- Zakazuje sastanke pomoćnim članovima, po potrebi, za specifične aspekte istrage.
- Prezentira nalaze menadžerskoj strukturi kompanije.
- Nadzire i kontroliše proces istrage.
- Po završetku istrage izvršava naknadnu analizu, a sa stečenim iskustvima u toku istrage izveštava nadležni organ (CIO).

CIRT timove pojedinih kompanija treba organizovati na teritorijalnom principu, a glavni CIRT tim na nacionalnom nivou treba da bude povezan sa sličnim CIRT timovima i raznim međunarodnim asocijacijama radi usklađivanja standarda za istragu kompjuterskog kriminala, metodologije rada interventnih timova, organizacije istrage, primenjenih forenzičkih alata i sl.

5. Metodologija rada kibernetičkih interventnih timova

U istražnom postupku CIRT tim koristi metodologiju kojom obezbeđuje sledeće:

- Zaštitu prava osumnjičenih do mere koju diktira tekuća politika organizacije.
- Propisno sakupljanje, čuvanje i dokumentovanje digitalnih dokaza.
- Donošenje zaključaka sa činjenicama i dokazima.
- Vođenje kompletne istrage bez izmene digitalnih dokaza i uticaja izvana.
- Zadržavanje odgovarajuće poverljivosti istrage.
- Odgovarajuće vođenje istrage da se zaštiti IS organizacije od ponovljenog izlaganja incidentu.
- Korišćenje standardizovane tehnike i alata za akviziciju (otkrivanje i sakupljanje), forenzičku analizu, skladištenje i čuvanje digitalnih kompjuterskih dokaza. Osnovni

alati su: portabl hardversko-softverski alat za bekapiranje i mirorisanje diskova, foto/digitalne kamere i softverski alati za forenzičku analizu.
- Sakupljanje, označavanje i čuvanje digitalnih dokaza u lancu istrage u skladu sa standardizovanom procedurom.
- Pripremu i izradu izveštaja za nadležne organe (CIO ili zvanični organ istrage) u skladu sa standardizovanom procedurom.

6. Dokumentacija kibernetičkih interventnih timova

Rukovodilac kibernetičkog interventnog tima odgovoran je za vođenje evidencije o svim kompjuterskim incidentima i dužan je da ih klasifikuje po značaju i težini posledica u tri grupe: Klasa 1, Klasa 2 i Specijalna klasa.

Primeri incidenata Klase 1 su:
- Identifikovani i lokalizovani virusni napadi.
- Zloupotreba Internet mreže.
- Incidenti koji vode do grešaka korisnika, ili padova sistema (bagova).
- Manji pokušaji upada, skeniranja ili kačenja na sistem.

Primeri incidenata Klase 2 su:
- Napad na mrežnu barijeru (firewall).
- Koordinirani, distribuirani napadi.
- Virusni napad na ceo informacioni sistem.
- Finansijska pronevera koja uključuje računar.
- Napadi na server datoteka ili host server.
- Krađa intelektualne svojine.
- Napad na osetljive resurse (ljudske, finansijske, informacije, itd.).

Kategoriju **specijalne klase** kompjuterskih incidenata odobrava CIO. Incidenti u praksi mogu, tokom istrage, eskalirati iz jedne u drugu klasu.

7. Obuka članova CIRT tima

Standardni program obuke treba da sadrži sledeća poglavlja: definicije termina, uputstvo, SRP (standardne radne procedure), garanciju kvaliteta. [7]:

Organizacije koje koriste digitalne dokaze, fotografije i tehnologije slikanja u pravosudnoj praksi treba da primenjuju programe kontrole kvaliteta kojima obezbeđuju da dostignuti rezultati u sakupljanju digitalnih dokaza budu ponovljivi i validni. Deo ovih programa, kontrola izvršavanja funkcija i korektivne akcije treba dokumentovati.

Obuka o svesti potrebe. Profesionalci u zvaničnim organima istrage treba da budu svesni potrebe striktnog sprovođenja propisanih procedura i standarda koje se koriste unutar zajednice. Takođe, treba da budu svesni i da prate razvoj novih tehnologija i alata iz oblasti digitalne forenzičke analize.

Organizacije i pojedinci treba da definišu i primenjuju program kontrole kvaliteta i da obezbede: pouzdan servis, implementaciju priznatih standarda za dobru praksu i korišćenje validnih i pouzdanih procedura odgovarajućih za zadatak Pojedinci moraju imati obuku iz sistema kvaliteta.

Tehnička obuka. Lica odgovorna za rad sa informacionom tehnologijom treba da budu obučena za rad sa ovim tehnologijama i osposobljena da objasne svoj rad na prikupljanju digitalnih dokaza poroti i pred sudom. Pojedinci moraju imati specijalističku obuku, zavisno od specifične aplikacije digitalnog podatka-dokaza:

a. Akvizicija i skladištenje digitalnog dokaza

- Uzimanje i forenzička akvizicija digitalnog dokaza
- Prenos i dostavljanje
- Skladištenje i čuvanje

b.Procesiranje i forenzička analiza digitalnog dokaza

- Privremeno skladištenje
- Procesi poboljšanja
- Specifični aplikacioni procesi

c.Priprema digitalnog dokaza za glavni pretres

- Printeri, papir, filmski snimak
- Video bim prezentacija i drugi uređaji i prenosni mediji.

Obuka krajnjih korisnika o svesti potrebe. Pojedinci i organizacije u pravosudnom sistemu koji koriste digitalne dokaze moraju biti svesni o mogućnostima i ograničenjima pojedinih raspoloživih tehnologija. Obuku iz pojedinih tehnologija treba da imaju: istražni organi, menadžeri **i** pravosudni organi

Članovi jezgra CIRT tima treba da imaju **regularnu obuku** iz sledećih oblasti:

- Pravnog aspekta, zaštite ličnih podataka i intelektualne svojine i zakonskog aspekta otkrivanja i zaplene računara za dokazni postupak.
- Politike zaštite i procedura zaštite kompanije.
- Procedura i procesa istrage.
- Skladištenja, čuvanja i dostavljanja dokaza u skladu sa standardnom procedurom.
- Obuka za rad i rukovanje sa svim tekućim sistemima za detekciju upada i alatima za istragu.
- Sakupljanja, čuvanja i forenzičke analize digitalnih dokaza o kompjuterskom incidentu.
- Procedura za koordinaciju sa sličnim, spoljnim organizacijama kao što su CIRT, CERT, FIRST, i organima za zvaničnu istragu kompjuterskog kriminala (npr. kod nas u Republici Srbiji: MUP, BIA, VBA).

Članovi jezgra CIRT tima treba da imaju **periodičnu** obuku iz:

- Upoznavanja najnovijih alata za istragu i tehnika istrage i forenzičke analize kompjuterskih dokaza.
- Upoznavanja najnovijih informacionih tehnologija.
- Upoznavanja najnovijih promena zakona, zakonske regulative i politike razvoja organizacije, koje mogu uticati na istragu.
- Periodične simulacione vežbe obuke u menadžmentu kompjuterskih incidenata (2 puta godišnje). Ovu vežbu CIO monitoriše.

Članovi za podršku CIRT tima treba da imaju **regularnu obuku** iz sledećih oblasti:

- Pravnog aspekta, zaštite ličnih podataka i intelektualne svojine i zakonskog aspekta otkrivanja i zaplene računara za dokazni postupak.
- Politike zaštite i procedura zaštite kompanije.
- Procedura i procesa istrage.
- Skladištenja i transporta dokaza u skladu sa standardnom procedurom.
- Tehničke obuke na svim platformama, operativnim sistemima (OS) i aplikacijama za koje su pomoćni članovi odgovorni. Ove platforme uključuju, ali nisu ograničene samo na sve OS i platforme koje se trenutno koriste u IS organizacije, telefonskim kompanijama i sistemu Internet provajdera.

Periodične simulacione treninge u kompjuterskim incidentima (2 puta godišnje) koje CIO monitoriše.

8. Predlog tema za obuku članova CIRT tima

TEMA I

OSNOVI ISTRAGE I FORENZIČKE ANALIZE RAČUNARA

(Program obuke za 4 sedmice, [4, 5])

1. Kompjuterski kriminal – pregled
2. Prezentacija scenarija slučajeva
    - Predstavi se slučaj koga slušaoci rešavaju u toku kursa
3. Sakupljanje digitalnih dokaza (zakonski i proceduralni aspekt)
4. Uvod u PC hardver
    - Procesori
    - Memorije
    - Glavne ploče
    - HD/FD/izmenjiv drajvovi
    - BIOS/CMOS
5. Kompjuterski podaci
    - Bitovi
    - Bajtovi
    - ASCII
    - Norton-ov disk editor & Drivespy softverski paket
6. Uzimanje miror slike medija-kopiranje HD, diskova, multimedijalnih kartica, itd.
7. Fizičke karakteristike HD i FD
- Adresiranje cilindera, glave, sektora (CHSA)
- Adresiranje logičkih blokova (LBA)
- Uputstvo za konfigurisanje IDE kanala
- Uputstvo za konfigurisanje SCSI kanala
8. Master boot record
    - Particije i sistem datoteka
    - Tabela particija
9. Logičke karakteristike HD i FD
    - Boot records
    - OS prema Sistemu datoteka
    - «3 pravila» pisanja drajva

- Pisanje drajva preko drajvera
- Pisanje drajva preko redirektora
- Skrivene particije

10. Sekvenca butiranja DOS baziranih računara
    - POST
    - BIOS
    - CMOS
    - OS
    - Upisivanje vremena i datuma (pristup, modifikacija, kreiranje)
    - Duga/kratka imena datoteka
11. Pregled MS-DOS komandnih linija
12. Razumevanje virusa
13. Oporavak izbrisanih datoteka
14. Traženje na osnovu ključne reči
15. Razumevanje tipa datoteka i hedera datoteka
16. Kompresija podataka
17. Šifrovanje podataka
18. Potencijalni dokazi u MS Windows OS
19. Kreiranje forenzičke FD za butiranje
20. Praktični rad/vežbe slušalaca

TEMA II.

OSNOVNA OBUKA ZA FOREZIČKU ANALIZU RAČUNARA
(Program obuke za 4 sedmice)

1. Uvod u PC hardver
    - Procesori
    - Memorije
    - Glavna ploča
    - Čvrsti disk/disketa/pokretni diskovi
    - BIOS/CMOS
2. Asembliranje forenzičkih alata za akviziciju i analizu
3. Prezentacija scenarija slučajeva iz prakse
    - Primer slučaja iz prakse se postavi i rešava do kraja kursa
4. Razmatranje zakonskih i regulativnih aspekata sakupljanja digitalnih dokaza
5. Kompjuterski podaci
    - Bitovi
    - Bajti
    - ASCII
    - Norton editor diska & *Drivespy* softverski paket
6. Uzimanje fizičke (miror) slike diskova, multimedijalnih kartica i.t.d.
7. Fizičke karakteristike čvrstih diskova i disketa.
    - Adresiranje cilindera, glave, sektora (CHSA)
    - Adresiranje logičkih blokova (LBA)
    - Uputstvo za konfigurisanje IDE kanala
    - Uputstvo za konfigurisanje SCSI kanala
8. Snimanje u master *boo-t*u (*master boot record*)
    - Particije i sistem datoteka

- Tabela particija

9. Logičke karakteristike drajvera čvrstih diskova i disketa
   - Butiranje (*Boot records*)
   - OS prema sistemu datoteka
   - «3 pravila» upisivaja drajva (*drive lettering*)
   - Pisanje drajva preko drajvera (hw)
   - Pisanje drajva preko redirektora
   - Skrivene particije
10. Sekvenca za butiranje DOS baziranih računara
   - POST
   - BIOS
   - CMOS
   - Operativni sistem
   - FAT-12/FAT-16/FAT-32
   - Vremenski upis i upis datuma (pristup, modifikacija, kreiranje)
   - Duga/kratka imena datoteka
11. Pregled MS-DOS komandnih linija
12. poznavanje i razumevanje virusa
13. Oporavak izbrisanih datoteka
14. Traženje prema ključnoj reči
15. Razumevanje tipova datoteka i hedera datoteka
16. Kompresija podataka
17. Šifrovanje podataka
18. Potencijalni dokazi u MS Windows sistemima
19. Kreiranje forenzičkog FD (diskete) za butiranje
20. Praktičan rad/vežbe slušalaca

TEMA III

FORENZIČKA ANALIZA KIBERNETIČKOG PROSTORA (RM)
(Program obuke za 4 sedmice)

1. Osnove o prenosu podataka i umrežavanju
   - OSI referentni model (*Open System Interconection*)
   - Fizički mediji/kabliranje, topologija mreža (OSI fizički sloj)
   - Protokoli veze podataka (OSI Data Link/Logical Link Layer)
   - Komunikacioni protokoli (Slojevi Sesija, Transporta i Mrežni)
   - TCP/IP Internet aplikativni protokoli (Aplikativni i Prezentacioni slojevi)
   - Komponente mreže (hardver)
   - Mrežni operativni sistemi (softver)
   - TCP/IP protokol adresiranja i sub-umrežavanja
2. Instaliranje mrežnih OS i konfigurisanje RM
   - Fizička konfiguracija RM (hands on)
   - Windows 2000 Professional

1. Instalacija i konfigurisanje osnovne radne stanice Windows 2000 Professional (praktična vežba)
2. *Peer-to-peer* (direktno, svako sa svakim povezani računari) umrežavanje sa Windows 2000 Professional

3. Windows NT/2000 security system
   - Uvod u Windows NT/2000 Professional radnu grupu, domene i bezbednost
   - Instalacija i konfirguracija osnovne radne stanice Win 2000 Professional (praktična vežba)
   - Vežba u umrežavanju klijent-server tipa Win NT/2000 Professional (praktična vežba)
4. UNIX/LINUX OS
   - Uvod u Unix/Linux OS
   - Instalacija i konfiguracija osnovne platforme radne stanice/servera Linux (praktična vežba)
   - Vežba umrežavanja UNIX/Linux OS (praktična vežba)
5. Netware OS
   - Uvod u Netware i Novell Directory servise
   - Instalacija i konfigurisanje osnovne platforme Netware 4.2. servera (praktična vežba)
   - Vežba umrežavanja Netware (praktična vežba)
6. Analiza saobraćaja računarske mreže
   - Analiza mrežnih paketa (praktična vežba)
7. Procesiranje mrežnih OS (sistemi datoteka i OS)
   - Isključivanje Windows NT/2000 i procesiranje (praktična vežba)
   - Isključivanje Linux i procesiranje (praktična vežba)
   - Isključivanje Netware i procesiranje (praktična vežba)
8. Dizajniranje i implementacija forenzičke računarske mreže
   - Izgrađivanje MS-DOS Netware i NT/2000 klijenata (praktična vežba)
   - Rad sa Windows «Super–klijentom» (praktična vežba)
9. Bezbednost mreže
   - Osnove bezbednosti RM

9. ZAKLJUČCI

1. Prema iskustvima iz prakse informatički razvijenih zemalja, treba izvršiti vlastitu inicijalnu istragu kompjuterskog incidenta na korporacijskom nivou, odnosno nivou IS organizacije, utvrditi karakter incidenta i, tek onda, doneti odluku o pozivanju zvaničnih organa istrage kompjuterskog kriminala.
2. Za formiranje kibernetičkih interventnih timova za brzo reagovanje na kompjuterske incidente treba definisati nacionalne organizacione i tehničke standarde, radne procedure i standarde dobre prakse i nabaviti opremu sa potrebnim forenzičkim alatima.
3. Uspešan i efikasan rad interventnih timova može se obezbediti samo odgovarajućom specijalističkom obukom visokostručnih multidisciplinarnih članova tima na nacionalnom nivou, kao i lokalne timove na nivou regija i gradova.

10. LITERATURA

1. (http://www.atstake.com).
2. (http://www.ensfi.org).
3. (http://www.ojp.usdoj.gov/nij/pubs.htm),

4. Carrier B., *Defining Digital Forensic Examination and Analysis Tools*, avgust 7, 2002, carrier&atstake.com
5. Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 1998.
6. *IOCE Princips & Definitions*, IOCE 2. Conference, 7.10.1999, Marriott Hotel, London
7. Pettinari D., *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000.
8. Pollit M., *Report on Digital Evidence,* (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001.
9. Rosenblatt, K. S., *High Technology Crime — Investigating Cases Involving Computers,* KSK Publications, San Jose, CA, 1995.
10. Whitcomb C. M., *A Historical perspective of Digital Evidence*: *A Forensic Scientist s View,* International Journal of Digital Evidence, proleće 2002, vol.1, issuue 1.
11. Zakon o izmenama i dopunama Krivičnog zakona Republike Srbije, «Službeni glasnik RS», broj 6 / 11.04.2003.