

integrirana sigurnost



Računalna forenzika

Goran Oparnica, direktor

ICTI 2006, Plitvice, 26.10.2006

Agenda

- O INsig2
- Što je računalna forenzika
- Success stories
- Forenzički alati

2

INSIG2

Računalna forenzika

O nama

- Dio grupacije IN2
 - Firme u Hr, Slo, BiH, SCG
- Korporativna sigurnost
- Fokus: sigurnosni sustavi
- ICT tehnologije

- Funkcionira 2,5 godine
- Trenutno 14 zaposlenih
 - podrška IN2
- Vlastiti stručnjaci za pojedina područja

3

INSIG2

Računalna forenzika

Djelatnosti

- Integrirana sigurnost
- Planiranje neprekinutog poslovanja
- Računalna forenzika
- Sigurne sobe

4

INSIG2

Računalna forenzika

Što je to računalna forenzika?

5

“Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence.”


INSIG2

Računalna forenzika

Zašto računalna forenzika?

6

Digital v Non-Digital



Over 90 percent of all information produced was in digital format. (UC Berkeley Study)

INSIG2

Računalna forenzika

Zašto računalna forenzika ?

7

- Korištenje ICT tehnologija u kriminalne svrhe zahtijeva posebne metodologije za vođenje istraga
- Računalni dokazi su osjetljivi, lako se brišu, mijenjaju i time kompromitiraju
- Specijalni forenzički alati omogućavaju povrat i analizu i obrisanih, skrivenih i privremenih datoteka koje normalno nisu vidljive

Zašto koristiti forenzičke alate ?

8



Moguće otkriti "klasičnim alatima"
(kao npr. Windows Explorer i sl.)

Ostatak koji je moguće otkriti samo
posebnim alatima

(Deleted, renamed, hidden, difficult to
locate.)

Princip "ledenog brijega"

Što je potencijalni digitalni dokaz?

9

- | | |
|----------------------------|--------------------------------|
| • Address Books | • File system artifacts |
| • Email files | • Backup files |
| • Audio/Video files | • Log files |
| • Image/graphics files | • Configuration files |
| • Calendars | • Printer spool files |
| • Database files | • Cookies |
| • Spreadsheet files | • Swap files |
| • Compressed files | • Hidden files |
| • Misnamed Files | • System files |
| • Encrypted Files | • History files |
| • Hidden Files | • Temporary files |
| • Password Protected Files | • Documents and text files |
| | • Internet bookmarks/favorites |

Metodologija općenito

10

- Sačuvati originalni medij u najboljem mogućem stanju
- Forenzička analiza se uvijek obavlja na kopiji
- Analiza se nikada ne obavlja na živom sustavu pomoću alata OS-a (browsing folders, i sl.)
- Nikada se ne smiju koristiti aplikacije OS-a (netstat, i sl...)
- Dokumentirati sve obavljene korake

Primjeri – Vodafone

11

- Informacije o novom mobilnom telefonu "procurile" u javnost
- EEE – Putem LAN mreže otkrio krivca
- Utvrđeno:
 - S kojeg računala je poslan e-mail, kada i kome
 - Točan sadržaj e-maila
 - Osoba koje je poslala e-mail
 - Djelatnik je suspendiran
- Vodafone zadržao partnerstvo sa proizvođačem mobitela

Primjeri – Firma XY1

12

- Pikovi u downloadu s Interneta van radnog vremena
- EEE detektirao dva Linux servera na mreži
- Download divx, mp3 i pornografskog sadržaja
- Daljnja istraga otkrila i krivce

Razvoj forenzičkih alata

13

Prva generacija

- Razni alati za: Image, Document, Search, Recover, and Report

Druga generacija

- Posebni dizajnirani i razvijeni forenzički alati: EnCase® i drugi

Treća generacija

- Network Forensics: trenutna, sigurna, efikasna forenzika računala putem LAN-a

EnCase forenzički alat

14

- Izveštaji prihvaćeni od strane suda u EU i USA
 - Implicitno prihvaćen i na sudovima u Hrvatskoj
- Ne invazivni alat za forenzičke istrage
- Prilagođen za istrage na velikim količinama podataka
- Podrška za FAT, NTFS, Apple, UNIX i LINUX
- Omogućava obavljanje svih nužnih forenzičkih analiza i istraga
- Uključuje i programski jezik EnScript

EnCase mrežna verzija

15



- Instalacija putem mreže na određeno računalo
- Ispitivač se autentificira na SAFE
- SAFE dozvoljava spajanje na određeno računalo
- Ispitivač se spaja na određeno računalo. Podaci se mogu vidjeti, pregledavati, analizirati putem mreže
- Ispitivač generira izvještaj

INSig2 & računalna forenzika

16

- Partnerstvo sa firmom Guidance software
- EnCase linija proizvoda
 - Za poduzeća (Forensics i Enterprise Edition)
 - Za istražne organe (LE Edition)
- Vlastiti školovani stručnjaci
 - Implementacija EnCase sustava
 - Pružanje konzultantskih usluga

Pitanja

17

?