

DIGITAL FORENSIC

L'analisi di un incidente o di una violazione alla sicurezza ad un sistema informatico viene spesso definita come Digital Forensic o forensic computer.

La Digital Forensic (DF) è costituita da un insieme di tecniche e metodologie di lavoro che permettono un'attenta e puntuale analisi della c.d. Computer Crime Scene alla ricerca delle prove.

Conoscerne i lineamenti è utile oltre che per gli investigatori anche per manager e responsabili della sicurezza IT che in caso di attacco inside dovrebbero collaborare il più possibile con gli inquirenti, conoscendo le loro procedure e le loro esigenze tecniche.

Le caratteristiche del cyberspazio implicano infatti la necessità da parte degli investigatori e dei responsabili della sicurezza aziendale di prendere dimestichezza con una nuova filosofia dell'investigazione.

Il "luogo del delitto", nei casi di computer crime è infatti costituito in parte da un ambiente elettronico e le prove di tali crimini sono costituite quindi da dati elettronici che dimostrano talune operazioni illegali avvenute all'interno di un computer.

I dati elettronici comprendono tutti quei record, file, codici sorgente, programmi, altre tracce contenuti nella memoria del computer.

Vista la diversificazione di impiego del computer nella società di oggi, le prove elettroniche arrivano ad assumere le forme più disparate.

Possono essere sofisticati documenti di testo, database del personale, liste clienti, informazioni finanziarie, e-mail inviate tramite Internet e messaggi di intranet locali, sistemi di pianificazione elettronica, file-log, trascrizioni di e-mail vocali eccetera.

Il primo e fondamentale passo nel Digital Forensic è determinare dove cercare la prova digitale nel senso di stabilire quale apparato è in grado, almeno teoricamente, di memorizzare informazioni digitali attendibili ed inerenti il caso in studio per poi capire in quale stato dovrebbe essere reperito^[1] e/o analizzato.

Gli obiettivi principali della Digital Forensic sono infatti la conservazione, l'identificazione, l'estrazione, la documentazione, e l'analisi delle informazioni relative ai dati della rete o dei sistemi informatici per:

1. determinare cosa è accaduto
2. comprendere il problema
3. identificare i responsabili

La documentazione prodotta dovrà prevedere informazioni complete in merito alla metodologia seguita per l'analisi dell'incidente.

Ogni fase del processo di investigazione dovrà essere dettagliatamente descritta, ivi comprese le operazioni effettuate sugli elementi di prova che dovranno essere mantenuti nel loro stato originale.

Errori comuni che possono verificarsi durante le operazioni di Digital Forensic riguardano:

1. l'alterazione della "prova" come, ad esempio, l'installazione di software sui supporti di prova acquisiti prima dell'analisi o l'utilizzo dei supporti di prova come aree di lavoro durante l'analisi;
2. l'uso di strumenti non idonei come, ad esempio, software non certificati o utility non verificate;
3. la mancanza di annotazioni relative alle operazioni effettuate;
4. errore nella gestione della data e dell'ora del sistema.

Le fasi seguenti illustrano la metodologia adottata dagli investigatori per eseguire correttamente una duplicazione di un supporto digitale ai fini investigativi:

rimozione del supporto digitale dal sistema compromesso e relativa installazione su di un sistema predisposto per l'analisi degli incidenti (Forensic Workstation);

esecuzione di una copia di tipo data stream del supporto digitale su un nuovo supporto da usare successivamente per le operazioni di indagine forense; alcuni tra i tool più utilizzati per eseguire questo tipo di operazioni sono: SafeBack (<http://www.forensics-intl.com/safeback.html>) e Encase (www.encase.com);

I software utilizzati per le indagini svolgono un'analisi dettagliata delle seguenti aree del supporto:

- Volatile data;
- Swap file;
- Logical files;
- Registry or configuration files;
- eMail;
- Application and Security Logs;
- Temporary Files;
- System Logs;
- Free space;
- Browser cache;
- History File;
- Slack Space;
- Deleted Files.

Sebbene molti pensino che la DF si limiti alla repertazione ed analisi dei personal computer, in realtà esso si estende ad una grande varietà di sistemi elettronici digitali.

La valutazione di quale tra i sistemi digitali presenti nell'area di competenza debba essere repertato per la successiva analisi non risulta immediata.

I dati contenuti in telefoni cellulari, organiser(s), smart-card(s), palmtop, intere reti di computer, etc. potrebbero in molti casi risultare utili all'indagine ed il riconoscimento del loro stato (attivi, spenti, batteria scarica, connessi, ecc.) sicuramente influisce sulla decisione di acquisirli e sulla modalità per farlo.

In alcune indagini sono state sequestrati e bloccati fisicamente interi apparati di ISP per ricercare informazioni utili (commettendo peraltro un ulteriore illecito) mentre il repertamento avrebbe dovuto limitarsi esclusivamente alle informazioni di interesse presenti nelle memorie di massa.

Tale esempio è uno dei più importanti riscontri dei problemi legati ad un errato processo di identificazione.

Gli analisti della Digital Forensic fanno quindi uso di sofisticate strumentazioni hardware e software (Forensic Toolkit) per cercare di ricostruire gli eventi che hanno generato la violazione e per produrre un'accurata documentazione valida soprattutto ai fini giudiziari; nonostante gli sforzi su alcuni siti internet dedicati alla sicurezza informatica iniziano ad essere già disponibili dei tools denominati "Anti-Forensic", specificamente creati per rendere più "difficile", se non impossibile, il lavoro degli investigatori.

Testo Tratto da Inside Attack, NSTecna Edizioni, Roma, 2005

[1] Il repertamento fisico è la fase nella quale l'apparato digitale viene sigillato per la successiva analisi di laboratorio.

Si noti la distinzione tra esso ed il repertamento dati che si riconduce sommariamente ad una copia certificata di dati di interesse.



Articoli specialistici sull'argomento sono disponibili per i soci ICAA all'interno dell'area a loro riservata. Per diventare soci dell'Associazione è sufficiente inviare un'email di richiesta a segreteria@icaa-italia.org. L'iscrizione è gratuita e consente di ricevere la tessera plastificata di socio che contiene la password personale di accesso.