
SN
IF


ORDINE DEGLI INGEGNERI
PROVINCIA DI UDINE


AICA

L'investigazione digitale

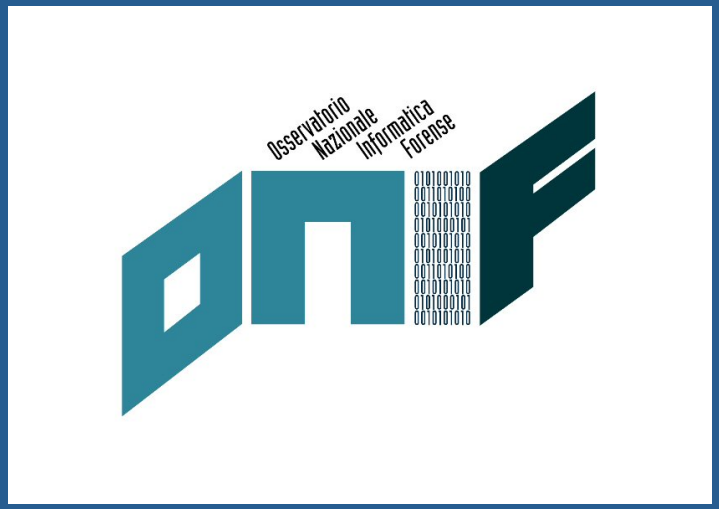
Metodologie di intervento nei casi di incidente informatico aziendale, come acquisire, preservare e documentare la fonte di prova.

Chi sono

- Digital Forensics Expert.
- Iscritto nell'albo dei consulenti tecnici e periti del Tribunale di Padova dal 2008, seguendo casi di cronaca di rilevanza nazionale.
- CTU e CTP dal 2006 per l'Informatica Forense
- Presidente della provincia di Padova di AIP-ITCS.
- Socio fondatore dell'Osservatorio Nazionale per l'Informatica Forense (http://www.onif.it)

Chi è ONIF

- l'Osservatorio Nazionale per l'Informatica Forense (http://www.onif.it) fondato nel 2015
- Diventare l'Associazione di riferimento per i professionisti dell'Informatica Forense
- Definire le professionalità, procedure operative, dati statistici e tariffari.



L'investigazione Digitale

L'investigazione digitale riveste un carattere di estrema importanza, nel periodo attuale, dove qualsiasi tipologia di informazione transita su reti telematiche e sistemi informatici.

L'evoluzione continua della tecnologia e gli scenari di crisi economica ampliano gli scenari di illeciti commessi per mezzo di sistemi tecnologici.

L’investigazione Digitale

L’investigazione digitale non si usa esclusivamente in scenari di violazione informatica commessa dall’esterno.

L’investigazione digitale affronta anche le tematiche di tutela del patrimonio aziendale, sia da attori esterni che interni dell’azienda.

L’investigazione Digitale

L’investigazione digitale segue delle metodologie scientifiche al fine di preservare inalterati i reperti e le fonti di prova.

L’inosservanza di una metodologia rigorosa potrebbe portare alla perdita di informazioni ed alla inutilizzabilità in sede giudiziaria.

L'investigazione Digitale: Gli step

1) Riconoscimento dell'incidente
2) Valutazione tecnica-investigativa-legale
3) Accertamenti tecnici
4) Documentazione e relazione

Riconoscere l'incidente

L'individuazione della fonte dell'incidente informatico è una delle fasi più complesse. La tempestività è determinante per delimitare lo scenario di intervento, limitare i danni, ripristinare l'operatività aziendale nel più breve tempo possibile.

Alcuni macro-scenari di incidente:

- Furto di dati od informazioni
- Alterazione fraudolenta di dati
- Diffusione all'esterno di informazioni riservate

Riconoscere l'incidente

Nel 90% l'incidente informatico non viene immediatamente riconosciuto.

Spesso nasce da una richiesta di assistenza tecnica o recupero dati da parte dei vertici aziendali ai responsabili o addetti IT.

Operazioni tecniche non professionali possono ridurre notevolmente il buon esito di un'indagine informatica.

Riconoscere l'incidente

Mancanza di tempestività e professionalità nell'intervenire possono causare:

1. Potenziale sovrascrittura di file di log di apparati e sistemi
2. Potenziale sovrascrittura dei cluster, di memorie informatiche, nel tentativo di recuperare dati cancellati
3. Alterazione e potenziale scomparsa di reperti utili ai fini dell'indagine (smartphone, backup, tablet, gps, chiavette etc.)

Valutazione Tecnica-Investigativa-Legale

Individuare l'obiettivo ultimo è di primaria importanza.

ESEMPIO

Agire in una fattispecie di furto di informazioni da parte di soggetti all'interno dell'azienda richiede competenze ed accortezze che nel 99,9% dei casi un tecnico informatico non può garantire.

Gli accertamenti tecnici

1. Corretta formalizzazione dell'incarico
2. Delimitare il perimetro «virtuale» delle indagini
3. Individuare ed Identificare i reperti
4. Acquisire con metodo scientifico
5. Mantenere la catena di custodia
6. Documentare tutte le fasi di acquisizione

Il metodo

Corretta Formalizzazione dell'atto di incarico

In relazione alla tipologia di illecito/incidente informatico si può agire differentemente:

- Verifica tecnica interna
- Verifica tecnica esterna
- Ausilio di legale (giuslavorista o penalista)

OGNI CASO VA VALUTATO IN CONCRETO.

Il metodo

Delimitare il perimetro «virtuale» delle indagini

Al fine di evitare o limitare contaminazioni della «scena del crimine», è preferibile, se possibile, isolare il perimetro o adottare tecniche di contenimento.

Agire con tempestività può limitare l'azione di manipolazione sui dati della scena criminis, impedendo che il terzo cancelli le proprie tracce di attività.

Il metodo

Individuare ed Identificare i reperti

Durante un indagine si potrebbe trovare difronte a diverse decine di TeraByte di dati, se non PetaByte, da dover acquisire ed analizzare.

A tal fine è necessario saper individuare gli elementi da dover acquisire «necessariamente» e quali poter discriminare, per evitare l'oversizing dei dati.

Ricordatevi di acquisire le Time Machine!

Il metodo

Acquisire con metodo scientifico

Una volta individuati i reperti, che potranno essere di diversa natura, è indispensabile applicare un corretto metodo scientifico per l'acquisizione della memoria a garanzia dell'integrità dei dati.

L'elemento imprescindibile di un'acquisizione «forense» di una memoria è l'impronta digitale da esso generata, meglio conosciuta come HASH che è un calcolo matematico abbinando diversi algoritmi come MD5, SHA-1 o SHA-256, al fine di scongiurare eventuali situazioni di Hash collision.

L'Hash del clone generato dovrà essere necessariamente identico alla memoria sorgente per avere la sicurezza di avere una copia identica all'originale.

Il metodo

Mantenere la catena di custodia dei reperti

E’ importante tracciare marche e seriali dei dispositivi di origine e di destinazione redigendo una catena di custodia con i soggetti che hanno maneggiato i reperti.

Il metodo

Documentare tutte le fasi di acquisizione

Un passo fondamentale è quello di documentare tutte le fasi tecniche dell'acquisizione, gli strumenti utilizzati, marche e seriali dei dispositivi di origine e destinazione, riportando l'impronta digitale (HASH) dei supporti.

I vari settori

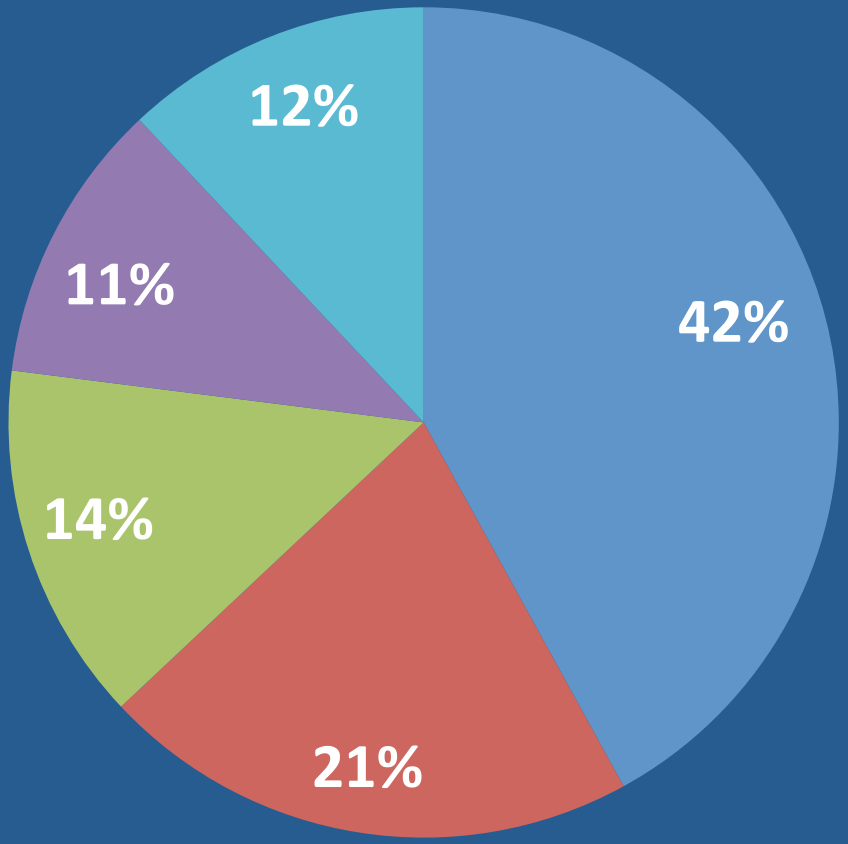
L'indagine digitale si può effettuare con l'ausilio multidisciplinare di attività informatico-forensi quali:

1. Computer Forensics
2. Mobile Forensics
3. Network Forensics
4. Video Forensics
5. Audio Forensics
6. Chip-Off Forensics

L’investigazione Digitale

L’investigazione digitale oltre all’esame delle evidenze raccolte dai reperti diventa efficace con l’ausilio di strumenti di Intelligence e l’incrocio di dati OSINT (Open Source INTelligence) o da fonti informative provenienti da altre banche dati.

Le frodi interne



Casi risolti con Investigazione Digitale

- Accertare commercio illecito di farmaci (File excel cancellati e recuperati da webmail)
- Passaggio di «progetti» alla concorrenza (email cancellata di 5 anni fa)
- Passaggio di ricette industriali (trasferimento di file Dropbox)
- Appropriazione indebita di informazioni aziendali riservate (analisi di registri e memorie usb)

Luigi Nicotera

Digital Forensics Expert

luigi.nicotera@studionicotera.it

Cell.: 346.7238618

http://www.studionicotera.it