Città Di Castello, 17.06.2017

Alla luce delle recenti norme europee in tema di privacy (GDPR) e cybersecurity (Direttiva NIS), oltre che l'enfasi data di recente alle best practice di sicurezza, grazie anche alla pubblicazione del Framework italiano per la cybersecurity, qual è oggi il ruolo della Digital forensic in azienda?

Il ruolo della digital Forensics all'interno di una organizzazione, non solo aziendale, ma anche istituzionale e pubblica, che impieghi strumenti elettronici di elaborazione per il perseguimento delle sue finalità di istituto, in un contesto come è quello attuale, caratterizzato dal fenomeno della c.d. digitalizzazione dei beni e dei rapporti, è un ruolo fondamentale, direi primario se non esiziale.

Ciò, in considerazione del fatto che, se è vero, com'è vero, che nel nostro ordinamento vige il principio in base al quale *"chi vuol far valere un diritto in giudizio deve provarne i fatti che ne costituiscono il fondamento"*, deve essere altresì vero che un "fatto digitale", potrà, ed in alcuni caso dovrà, essere provato solo digitalmente, vale a dire, solo facendo ricorso a procedure, strumenti e tecniche di investigazione digitale.

Un esempio chiarirà quanto sopra esposto.

Si faccia mente locale, con riferimento alle norme in materia fascicolo sanitario elettronico, dossier sanitario, o più semplicemente a quelle in materia di amministratori di sistema, al fatto che vi è l'obbligo di assicurare, mediante la generazione di appositi file di log, il controllo degli accessi a determinati contenuti informativi.

Ed allora quale potrà essere, se non quella di fare ricorso a procedure interne ed a strumenti di copia forense, firma digitale e marca temporale, la metodologia da impiegare per documentare, a fronte di una ispezione o nel corso di un processo, l'assolvimento degli obblighi imposti?

Ed ancora, come è noto, sia la NIS Directive sia il Regolamento Comunitario in materia di protezione dei dati personali impongono obblighi circostanziati di notifica dei Data Breach, ed implicano che il soggetto, ad esempio il titolare del trattamento, che subisce una violazione di dati, debba notificarla, unitamente alle circostanze relative alla sua verificazione all'Autorità di controllo preposta, entro 72 ore.

Come agire, in questi casi, considerando il fatto che nell'assolvimento dell'obbligo di notificazione del data breach, si stanno fornendo prove ad una autorità, se non ricorrendo a metodologie che integrino, nelle procedure di risposta agli incidenti, elementi specifici di raccolta e conservazione di evidenze digitali?

Via S. Apollinare n. 1 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
E - mail: giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Chi deve essere responsabile dell'acquisizione di "prove digitali", o "Digital Evidence"?

Personalmente, ritengo che - *analogamente a quanto avviene (o meglio a quanto dovrebbe avvenire), con riferimento all'applicazione pratica, nelle realtà lavorative quotidiane, delle norme in materia di Data Protection* - pure nel contesto della verticalizzazione delle funzioni all'interno degli organigrammi aziendali, attraverso l'individuazione di procedure dedicate di svolgimento, delle specifiche singole operazioni, in capo a personale dotato delle necessarie competenze e conoscenze, la responsabilità di un sistema di Corporate Forensics non possa che essere sistemica, vale a dire condivisa, ai vari livelli, in ogni area implicata dai suoi esiti, dell'intero tessuto organizzativo.

Per semplificare, potrebbe occorrere che l'area Legal di una organizzazione possa e debba relazionarsi efficacemente, se del caso attraverso appositi strumenti autorizzativi, previsti per esempio dal codice di procedura penale, nel caso di reati, oltre che con l'area HR, con l'area IT per coordinarsi, nella qualificazione della fattispecie in base alla quale l'attività investigativa deve essere effettuata, in funzione della individuazione del quadro probatorio digitale da costruire o all'interno del quale agire, prima dello svolgimento delle concrete operazioni tecniche che realizzeranno l'evidenza o la fonte di prova.

Si tratta, sostanzialmente di un processo organizzativo primario, integrato con gli altri processi, che deve essere coordinato dal Top Management, al quale devono essere assegnati budget per strumenti e competenze del personale, che deve essere disciplinato nei suoi rapporti con le altre funzioni e che, per tali ragioni, non può che essere condiviso, nelle sue fasi costitutive e realizzative, dall'intera organizzazione.

- Quali sono le diverse fasi di un programma volto ad acquisire prove digitali, a supporto di un corretto piano di Incident Response? le tecnologie di solito utilizzate?

La materia della Digital Forensics, da un punto di vista anche teorico e dottrinale si è evoluta moltissimo nel recente passato, proporzionalmente con l'evoluzione dell'impiego di strumenti elettronici di elaborazione che ci portano a considerare, anche da un punto di vista giuridico, fenomeni nuovi quali l'IoT, le Smart Cities, il Cloud Computing, quindi anche gli approcci metodologici si sono diversificati tra loro contemplando, a seconda dei vari autori o dei vari enti che rilasciano metodologie standardizzate, più momenti funzionali.

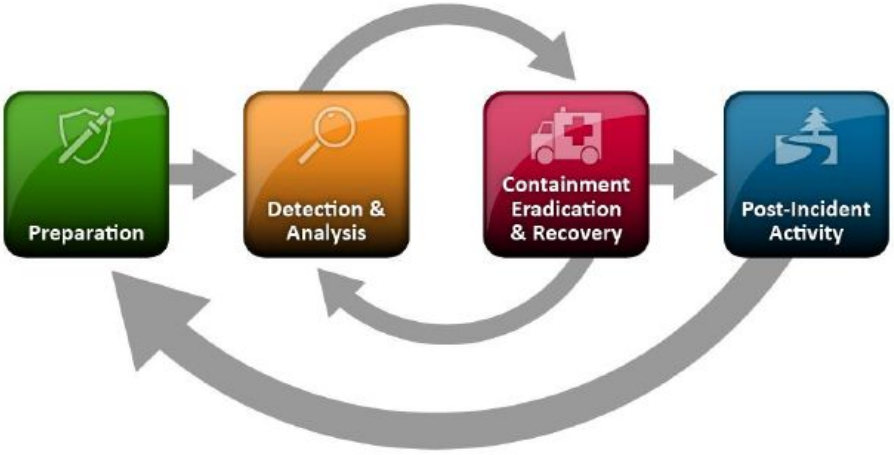
Personalmente penso che si possano individuare le fasi di individuazione, raccolta, analisi e presentazione, tuttavia, consiglio dal punto di vista dell'approfondimento scientifico, la lettura di una pubblicazione non più recentissima del National Insitute of Standards and Technology (NIST), la Special Publication 800-86, dal titolo: **"Guide to Integrating Forensics Techniques into Incident response"**.

Via S. Apollinare n. 1 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
E - mail: giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

In tale approccio sono indicate le fasi di Collection, Examination, Analysis e reporting.

Sempre da un punto di vista metodologico ritengo importante che accanto al documento appena ricordato si considerino con la dovuta attenzione i contenuti di un'altra pubblicazione, più recente, del 2012, anch'essa pubblicata dal National Insitute of Standards and Technology (NIST); la Special Publication 800-61 Revision 2 dal Titolo Computer Security Incident Handling Guide che, individua le fasi seguenti nel processo di risposta agli incidenti: Preparation, Detection & Analysis, Containment Eradication & Recovery, Post-Incident Recovery (Figura 1).

NIST 800-61 r2 - Incident Response Life Cycle.



Per quanto riguarda le soluzioni tecnologiche necessarie a condurre operazioni di digital forensics occorre, secondo me, preliminarmente considerare che una attività diretta a raccogliere evidenze digitali, relative ad un oggetto specifico di indagine, sarà tanto più fruttuosa, quanto più, al momento della configurazione del sistema che quell'oggetto ospita, ci si sia preoccupati di generare le evidenze stesse in modo tale che esse siano semplicemente raccolte in caso di necessità.

E quindi, si dovranno adeguatamente configurare i sistemi, per esempio, facendo ricorso a strumenti o a soluzioni di log generation, in modo tale da poter contare, alla bisogna, su una base probatoria predefinita e nota.

Nello specifico degli strumenti tecnici da impiegare, vale la pena sottolineare come siano disponibili sia soluzioni open source, per lo più basate su distribuzioni Linux gratuite, sia soluzioni proprietarie concesse in licenza d'uso.

Solo per citare alcune delle soluzioni si segnalano SANTOKU, DEFT e CAINE sul versante Open Source e OXYGEN Forensics, ENCASE e MAGNET FORENSICS sul versante proprietario.

Via S. Apollinare n. 1 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
E - mail: giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

- Qual è la situazione delle aziende italiane su questi temi?

In base a quella che è la mia esperienza ritengo che le aziende Italiane, dopo una stagione in cui poteva riscontrarsi una consapevolezza distribuita, per così dire, a macchia di leopardo, stiano iniziando ora ad approcciarsi in modo coerente e sistematico alle tematiche sopra illustrate.

Ciò deriva, dal mio punto di vista, da almeno due fattori principali, e cioè, da un lato, la spinta propulsiva all'approfondimento di queste tematiche, correlata all'emanazione di numerosi provvedimenti legislativi che hanno alzato il livello di attenzione alle implicazioni sottese al Cyber Risk, alla protezione dei dati personali, ed alla responsabilità d'impresa in materia di delitti informatici, e dall'altro, ad un incremento esponenziale di efficacia delle azioni condotte dai cyber criminali che hanno avuto come effetto, purtroppo, tardivo, quello di rendere, per ragioni assicurative o giudiziarie, necessario accertare lo svolgimento di determinati eventi digitali.

Si pensi, per fare un esempio conclusivo, alla necessità di documentare, in caso di copertura assicurativa per il rischio perdita di dati, le modalità attraverso le quali un ransomware abbia agito all'interno della rete aziendale ovvero abbia spiegato i suoi effetti su dati specifici oggetto della copertura stessa.

Avv. Giuseppe Serafini

Via S. Apollinare n. 1 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
E - mail: giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W