FORENSIC

L’attività di Forensic Accounting

Relatore: Dott. Rudi Triban, Senior Manager IRM KPMG – Milano
Dott. Stefano Martinazzo, Manager KPMG Forensic Department – Milano

Roma, mercoledì 4 ottobre 2006

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Ambiti di intervento

Clientela:

- Privata
- Istituzioni pubbliche (Ministeri, Procure delle Repubblica, Istituti universitari, …)

Ambiti di intervento

- Investigazioni contabili e di natura societaria (*Corporate Intelligence*) su "sospette irregolarità o frodi"
- Individuazione dei soggetti (persone giuridiche e fisiche) coinvolti nella frode
- Determinazione del danno economico prodotto dalla frode
- Organizzazione e rappresentazione della "prova" nei procedimenti giudiziari e/o in sede di provvedimenti disciplinari
- Consulenze tecniche nei procedimenti arbitrali
- Progettazione ed analisi di procedure "anti-frode" anche relative a sistemi informatici

KPMG

Rilevanza del fenomeno

L'impatto delle frodi in Italia

(alcuni risultati delle più recenti ricerche ed esperienze professionali)

- Il 40% aziende italiane ritiene di averla subita nel corso del 2005…
- …di tale campione, il 20% lamenta una perdita superiore a $500.000
- La causa primaria per più del 50% delle frodi, è dovuta a carenze nei controlli interni
- Il 41% delle frodi è scoperta in via accidentale
- Nell'85% dei casi è una frode c.d. "frode interna" (commessa dai dipendenti)
- Il 65% delle frodi interne sono commesse da dirigenti e/o amministratori

Le tappe dell'intervento forensic

- Valutazioni preliminari e pianificazione (rischi, competenze, stima della mole di dati utili alle indagini, verifica del formato del dato elettronico, …)
- Raccolta delle evidenze (catalogazione, codificazione, backup dei sistemi informativi, sequestri di PC, HD, ricostruzione di dati digitali cancellati, …)
- Analisi delle informazioni raccolte (attraverso tecniche investigative e appropriati tools informatici, …)
- Relazione tecnica/Esposto

E' RICHIESTO L'INTERVENTO

DELL' *IT FORENSIC SPECIALIST*

Team di lavoro

L'attività investigativa è condotta da esperti appartenenti a settori differenti:

- ü Esperto tecnico-contabile (Forensic Accounting Department)
- ü Esperto IT Forensic
- ü Legale (penalista, civilista, esperto di diritti societario, …)
- ü Fiscalista
- ü Esperti specifici (periti appartenenti a diversi settori)
- ü Polizia giudiziaria

KPMG

Le maggiori problematiche riscontrate

- Necessità di reperire e analizzare una grande quantità di dati (cartacei e digitali) con l'obiettivo di descrivere con maggiore precisione i fenomeni illeciti
- Riconoscere con la dovuta accuratezza il giusto "valore probatorio" delle evidenze documentali e delle testimonianze raccolte
- Capacità tecniche di acquisire banche-dati di grandi dimensioni (in ambito giudiziario e non) in rispetto delle normative sul trattamento dei dati elettronici
- Competenze nella custodia fisica, classificazione, archiviazione di documenti coperti da riservatezza
- Difficoltà nella rappresentazione di operazioni molto complesse in termini comprensibili e senza ridurne il necessario grado di approfondimento tecnico
- Estrema attenzione nel supportare ogni descrizione, parere, giudizio formulato, in modo adeguato e completo

Aspetti legali

Frode informatica

Il nostro ordinamento, con la legge 23 dicembre 1997 n 547, ha inoltre introdotto una nuova fattispecie tipica di delitto enunciata all'art. 640-ter c.p. e rubricata "Frode informatica". Il succitato articolo definisce la frode informatica come segue:

Art. 640-ter c.p.

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Aspetti legali

Sequestro dei dati

Il sequestro dei dati in formato elettronico è ammesso negli stessi limiti in cui è ammesso il sequestro cautelare disciplinato dagli artt. 253 e ss. del c.p.p. Infatti, l'art. 253 c.p.p. ammette il sequestro del corpo del reato o delle cose pertinenti al reato. Si intendono per corpo del reato (dunque suscettibili di sequestro) "le cose con le quali o sulle quali è stato commesso il reato nonchè le cose che ne costituiscono il prodotto, il profitto o il prezzo" (art. 653, comma 2, c.p.p.). In tale accezione, molto ampia, rientrano sicuramente anche i dati in formato elettronico.

Discrezionalità nell'ammissione delle prove

Nella nostra legislazione, il giudice ha ampia discrezionalità nel ritenere ammissibile o meno una prova. In via di principio, le prove elettroniche sono ammissibili (nei limiti stabiliti caso per caso dal giudice competente) qualora esse abbiano valore legale, cioè se ne sia inoppugnabile la fonte e la veridicità (es. email con firma elettronica).

Il codice civile e il codice di procedura civile se ne occupano non sistematicamente ma in diversi punti e le loro rispettive trattazioni a seconda del tipo di prova (es. testimoniale, scritta, etc.) e del tipo di processo (es. cognizione, ingiunzione, etc.).

Metodologia ed obiettivi

Per far fronte alle succitate problematiche ed aspetti legali e come linea guida per lo svolgimento di ciascun incarico è quindi necessario disporre di una metodologia al fine di raggiungere e garantire i seguenti primari obiettivi:

- ü Identificare ogni possibile fonte di evidenze
- ü Preservare l'integrità dei dati in modo inoppugnabile
- ü Analizzare i dati ed individuare le evidenze
- ü Presentare le risultanze

Una metodologia consistente che copra i seguenti obiettivi è necessaria negli incarichi nazionali ma diviene indispensabile nel caso di incarichi a livello internazionale dove sia necessario coordinare il lavoro di numerosi team operanti in luoghi differenti.

Problematiche organizzative

Durante incarichi di Forensic Accounting dove sia necessario acquisire ed analizzare dati è possibile dover gestire alcune delle seguenti problematiche organizzative:

- Dispositivi aziendali utilizzati dai dipendenti non sono prontamente sottratti a questi ultimi
- Mancato tracciamento del possesso da parte dei dipendenti di supporti di memoria aziendali e personali
- Impiego di computer personali
- Mancanza di adeguate politiche che garantiscano la data retention per quanto riguarda comunicazioni avvenute tramite posta elettronica

Problematiche tecniche

Durante incarichi di Forensic Accounting dove sia necessario acquisire ed analizzare dati è possibile dover gestire alcune delle seguenti problematiche:

- Evidenze presenti in differenti tipologie di sistemi e dispositivi
    - Cellulari, smartphone, PDA, fotocamere, UMPC, notebook, desktop, server e dispositivi di rete
- Necessità di acquisire, analizzare ed archiviare dati di dimensioni sempre crescenti
- Analisi di banche dati
- Acquisizione di dati da sistemi dismessi
- Acquisizione di dati da backup preesistenti
- Dati non direttamente accessibili

E’ possibile dover acquisire documenti in formato cartaceo; quest’ultimi dovranno quindi essere soggetti ad acquisizione e relativa conversione in formato analizzabile.

Strumenti Hardware

Per supportare l'operato dei professionisti negli incarichi di Forensic Accounting sono stati sviluppati appositi strumenti che permettano di operare secondo una specifica metodologia e permettendo di raggiungere i suddetti obiettivi.

Acquisizione

- Dispositivi che consentano di leggere ed esaminare il contenuto di una unità di memoria impedendone ogni modifica anche accidentale
- Dispositivi di replicazione delle unità di memoria, hard disk, comunemente impiegate in computer di varie dimensioni ed altri dispositivi

Trasporto

§ Dispositivi di cifratura che prevengano accessi non autorizzati ai dati acquisiti

Strumenti Software

Attualmente sono impiegate suite di software che consentono di svolgere le attività necessarie impiegando un ristretto numero di strumenti. Infatti differenti funzionalità, che richiedevano in precedenza numerosi software, sono state ora integrate in un limitato numero di strumenti.

Le principali macro funzionalità sono le seguenti:

- Accesso ai dati e predisposizione di una o più copie
- Analisi dei dati acquisiti
- Predisposizione di report relativi alle evidenze rinvenute

I principali strumenti software utilizzati per questa tipologia di incarichi sono i seguenti:

- **EnCase Forensic Edition, Guidance Software**
- **FTK, Forensic Toolkit, AccessData**

Ulteriori Strumenti Software

Infine è possibile impiegare un insieme di strumenti software, generalmente utilizzati da professionisti IT, per svolgere specifiche attività quali ad esempio:

- Scannerizzazione e OCR
- Identificazione di un eventuale utilizzo di steganografia
- Conversione di file in differenti formati
- Rimozione di protezioni a livello applicativo
- Rinvenimento di password
- Cancellazione definitiva di dati da unità di memoria

Domande & quesiti

Riferimenti

Rudi Triban

Senior Manager

KPMG S.p.A.

Information Risk Management

Via Vittor Pisani, 25

20124 - Milano

rtriban@kpmg.it

Secretary +39 02 6763.2248

Stefano Martinazzo

Manager

KPMG Audit S.p.A.

Forensic Department

Via Vittor Pisani, 25

20124 – Milano

smartinazzo@kpmg.it

Secretary +39 02 6763.2652