ANALISI FORENSE: COSA ANALIZZARE

Il contesto

Prima di tutto è necessario capire quale è la problematica per la quale si è stati convocati. Può essere ad esempio un caso di spionaggio industriale, oppure sospetti di assenteismo da parte di alcuni dipendenti, oppure ancora sospetto di utilizzo prolungato degli strumenti informatici aziendali per fini personali, o altro ancora. Ogni problematica presenta peculiari interrogativi per capire come muoversi nel contesto.

Secondo, è importante capire alcuni aspetti della realtà aziendale nella quale ci si viene a trovare. Cosa produce, quali sono i beni informatici – intesi come dati – più importanti: nella fattispecie, per una azienda che produce macchinari saranno più importanti i progetti, mentre per una azienda di logistica saranno più importanti i report delle consegne effettuate. Vi sono poi dati importanti per chiunque, ad esempio le anagrafiche clienti e fornitori nonché i documenti amministrativi, ma di norma se qualcosa qui "scappa" la faccenda è meno tragica.
Poi è fondamentale l'organizzazione aziendale: quanti dipendenti vi sono, quante sedi o filiali, la gerarchia e l'organigramma. Questo per capire che ruolo hanno le persone sospettate, se si può coinvolgere qualcuno nell'indagine come collaboratore oltre alla direzione (ad esempio il responsabile informatico), ecc.
Tutto ciò può sembrare superfluo ma è fondamentale per potersi muovere con dimestichezza all'interno del nuovo ambiente nel quale si è chiamati a indagare, ottimizzare i tempi di esecuzione, risultare meno invasivi possibile e migliorare complessivamente il risultato – e quindi la soddisfazione del cliente.

Strumenti informatici

Non sempre è necessario analizzare ogni periferica informatica. E' invece necessario prendere di mira l'hardware che può potenzialmente contenere le informazioni che stiamo cercando, sulla base di una precedente analisi del contesto. Vediamo quindi caso per caso su che apparecchiature è necessario indagare nei differenti casi.

- **Computer fissi in uso all'azienda** (ivi inclusi i pc portatili utilizzati come postazioni fisse per necessità): vanno analizzati in caso:
  - si ricerchino dati informatici che l'utente può aver salvato sul computer stesso
  - se i documenti sono stati scritti, modificati o aperti con il computer
  - se la posta elettronica viene utilizzata in locale
  - se la posta elettronica è configurata su un programma e-mail come outlook
  - se l'utilizzo del pc non è limitato alla sola emulazione di terminale (client servizi terminal)
  - se si sospetta che un dipendente faccia uso del pc per fini non aziendali non autorizzati
  - se si teme che la problematica sia stata causata da accesso non autorizzato (hacker, virus, trojan, ecc)

- **Computer portatili in uso all'azienda** (ivi inclusi tablet pc e affini): vanno analizzati in caso:
  - Tutti i casi precedenti relativi ai computer fissi
  - Se si ritiene che il dipendente ne abbia fatto uso per travasare dati non aziendali collegandosi ad altra rete

- **Smartphone aziendali**
  - se lo smartphone ha potenziale accesso alla rete aziendale
  - se viene regolarmente utilizzato per accedere a dati aziendali
  - se si teme che la problematica sia stata causata da accesso non autorizzato (hacker, virus, trojan, ecc)

- **CDROM-DVDROM** di archiviazione dati:
  - Se i dati erano archiviati in tali dispositivi e in nessun altro luogo (per effettuare confronti)

- **Pendrive USB**:
  - Se i dati erano archiviati in tali dispositivi e in nessun altro luogo (per effettuare confronti)

- **Fotocamere digitali**:
  - Se si teme siano state effettuate fotografie per trafugare dati o per creare la problematica (per effettuare confronti, ricavare dati di utilizzo, ecc)

- **Server aziendali** (sia fisici che virtualizzati in hardware installati in locale):
  - si ricerchino dati informatici che l'utente può aver salvato su risorse condivise sul server
  - se si utilizza un sistema di condivisione dell'ambiente di lavoro, quale ad esempio il sistema terminal server;
  - se i documenti sono stati scritti, modificati o aperti da sessioni remote
  - se la posta elettronica viene utilizzata via web in una sessione remota
  - se si utilizza un server di posta locale (es. exchange, m-daemon, ecc)
  - se la posta elettronica è configurata su un programma e-mail come outlook in un ambiente terminal
  - se si teme che la problematica sia stata causata da accesso non autorizzato (hacker, virus, trojan, ecc)

  Va evidenziato, per tutto ciò che concerne i server, la necessità di identificare esattamente l'hardware in uso, il sistema operativo, la configurazione, la presenza di ambienti virtualizzati, ecc.

- **Aree in cloud**: vanno prese in esame qualora:
  - La posta elettronica sia ritenuta di interesse e sia in cloud
  - I documenti siano ritenuti di interesse e siano in cloud
  - L'intero ambiente di lavoro sia in cloud

  E' necessario tuttavia per analizzare un ambiente di questo tipo un accesso di tipo amministrativo o, in subordine, la collaborazione del gestore di tali spazi virtuali.

Va ricordato che vi sono dispositivi sui quali non è possibile, se non previa autorizzazione scritta, fare alcun esame, nella fattispecie tutti i dispositivi di proprietà personale delle persone e non aziendali. Allo stesso tempo, non è lecito forzare caselle email o altri spazi di memorizzazione personali senza esplicita autorizzazione scritta del proprietario o dell'autorità competente.

Analisi di un caso reale

Quella che segue è la disamina di un caso reale, nel quale si è verificato un caso di spionaggio industriale. E' stato necessario decidere cosa analizzare e cosa no, capire di che materiale informatico si stava effettuando la ricerca, e collaborare con CED e Direzione per acquisire i dati necessari.

Raccolta dati iniziale

- Quale è il motivo della chiamata? *Temiamo che un dipendente abbia trafugato dati aziendali riservati*
  - Cosa è uscito che non doveva uscire? *Alcuni disegni in cad sono finiti in mano a una azienda concorrente.*
  - Come lo avete scoperto? *Non ne siamo certi, ma parlando con un nostro cliente ci hanno riferito dettagli su un progetto di un macchinario che non avrebbero dovuto conoscere, a loro detta riferiti da una nostra concorrente.*
  - Sospettate di qualcuno in particolare? *Temiamo che sia coinvolto Pietro, la persona che ha supervisionato e personalmente sviluppato il progetto negli aspetti principali.*
  - Che altri soggetti possono essere coinvolti? *Forse nessuno, forse qualcun altro. Non lo sappiamo, ma a questo punto tutto è possibile, di Pietro noi ci fidavamo come di tutti gli altri.*
  - Che valore ha ciò che è uscito x l'azienda? *Inestimabile. E' un prodotto rivoluzionario che potrebbe sconvolgere il mercato a nostro favore.*
  - Che conseguenze vi possono essere? *Molto pesanti. Se aziende nostre rivali conoscessero i prodotti nei dettagli potrebbero rubarci tutti i clienti.*
  - Dove erano memorizzati i dati? *Nel server aziendale. Utilizziamo delle risorse condivise sul server ove sono conservati tutti i dati.*
  - Come ritenete siano usciti? *Non ne abbiamo idea! Forse tramite e-mail, oppure trafugati con chiavette USB...*

Ora, ottenute queste domande, abbiamo un primo contesto sul quale lavorare. Vediamo di completare l'analisi della situazione informandoci sul numero dipendenti, sulla gerarchia aziendale, sulle mansioni dei dipendenti, sulla situazione generale in essere compreso il clima aziendale.

Dobbiamo successivamente raccogliere informazioni sulla rete informatica aziendale, per capire 1) in che formato potrebbero essere i dati usciti dall'azienda, 2) quali possibilità di fuga possono essersi palesate.

La cosa migliore è coinvolgere l'amministratore del sistema informatico (sysadmin), se presente, o in subordine l'azienda responsabile della manutenzione della rete informatica.

Sulla base di ciò che abbiamo raccolto,cercheremo il file rubato o comunicazioni in merito in:

- Mail aziendali
- Mail personali
- Chiavette usb dell'ufficio

Mediante coinvolgimento dell'amministratore di sistema, si dovrà a questo punto capire:

- Come lavorano gli utenti?
  - In locale (pc)
  - In terminal (servizi terminal su windows server)
  - In altri ambienti terminal (citrix? Xterm?)
- Dove sono ospitate le mail aziendali? Che sistema si utilizza?
  - Exchange?
  - Configurate sui pc o su ambiente terminal?
  - In cloud?
- E' possibile connettersi dall'esterno? Come?
  - VPN
  - Mediante IP in servizi terminal
  - …

Ipotizziamo che dal confronto con il responsabile della rete informatica si ottengano queste informazioni:

- *Gli utenti lavorano in servizi terminal per usare word/excel/mail aziendale che è su exchange, chi disegna in cad lo fa in locale e poi i documenti vengono salvati in una cartella condivisa sul medesimo server. Non vi sono accessi possibili dall'esterno, abbiamo una normale ADSL. L'azienda non ha mai acquistato pendrive per uso aziendale, se vengono usate esse sono di proprietà dei singoli utilizzatori.*

Nel caso specifico quindi, si dovrà esaminare:

- Pc fisso del sospettato (1 HDD da 120GB, Windows 7): ricerchiamo artefatti dell'uso del documento diffuso illecitamente, della spedizione dello stesso o di parte dello stesso a terzi mediante e-mail in locale, e artefatti dell'uso di dispositivi USB; il tutto ipotizzando un determinato periodo di tempo nel quale si sospetta sia stato commesso l'illecito.
- Pc fisso di altri due potenziali sospettati (ognuno 1 HDD da 120GB, Windows 7): quanto sopra.
- Server terminal/exchange/archivio dati (3 HDD RAID5 SCSI 146GB, spazio 292GB, Windows 2003 server): analizziamo l'uso delle condivisioni, gli utenti che hanno avuto accesso a quel particolare documento, le mail contenute nel server exchange, artefatti di utilizzo di quel file nell'ambiente terminal, artefatti della spedizione dello stesso o di parte dello stesso a terzi mediante e-mail web in ambiente terminal.

Dovremo poi prendere in esame, collaborando con il responsabile della rete informatica, se sia possibile connettersi in wifi alla rete aziendale, e se siano presenti altre policy di sicurezza.

Per l'estrazione dati si sono ottenute le immagini dei 3 dischi dei pc fissi (3x120GB) e del server (3x146GB).

Nel caso specifico, i risultati sono stati:

- Si sono trovate nell'account terminal del sospettato due e-mail spedite a un amico, rivelatosi poi essere coinvolto nella situazione seppur in modo accidentale, contenenti un paio di file in formato CAD proprio con i disegni e le informazioni in possesso del cliente.
- Non sono stati trovati artefatti di alcun genere utili alla disamina della situazione nel pc fisso in uso al sospettato
- Non sono stati trovati artefatti di alcun genere utili alla disamina della situazione negli altri due pc esaminati

A seguito dell'indagine, vi è stato solamente un richiamo formale per l'incauto dipendente poiché, dopo una analisi attenta, il disegno è risultato essere un bozzetto incompleto e tra l'altro presentava errori che lo rendevano non funzionale, riducendo di molto il rischio di danno aziendale.