APPENDICE B

Principi legali di comportamento nella corretta acquisizione delle prove nel c.d. "incident response"

In questo documento si evidenziano in maniera molto sintetica alcuni principi basilari, più di buon senso che strettamente giuridici, che qualunque operatore del settore dovrebbe conoscere assolutamente a memoria.

1. Prove documentali:

Le prove acquisite nel corso delle analisi secondo il nostro diritto sono da considerarsi come prove documentali, e conseguentemente seguono il regime delle medesime per quanto concerne la valenza probatoria e l'acquisizione – eventuale – in un giudizio. Ovviamente nulla vieta che un "fatto", che verrebbe evidenziato da una analisi su macchine compromesse, non possa anche essere oggetto (sempre nei limiti di ammissibilità del mezzo istruttorio) di una prova testimoniale, ovvero il soggetto che abbia operato potrebbe essere chiamato a testimoniare sulle risultanze della propria attività.

2. Non alterabilità delle prove:

Nel documento sopra menzionato è stata ampiamente trattata la materia concernente la corretta acquisizione e manutenzione dei supporti contenenti sia direttamente le c.d. "evidenze informatiche", sia i supporti sui quali siano eventualmente state effettuate delle analisi. Il tecnico dovrà ragionare cercando sempre di attuare una sorta di "gioco delle parti"; dovrà essere sempre in grado di poter rispondere con certezza alla domanda che egli stesso (qualora fosse il tecnico di controparte) porrebbe al fine di insinuare il dubbio sistematico su quanto sia stato eventualmente eseguito. Esiste un altro modo di condurre la procedura? Se si per quale motivo è stata scelta una procedura piuttosto che un'altra? …

Inoltre occorrerà sempre tenere presente che – in caso di giudizio – l'attività dell'avvocato di controparte consisterà principalmente nel mettere sistematicamente in dubbio tutta l'attività svolta nel caso di un "incident response", per cui quanto appena scritto si rafforza ulteriormente.

In questo senso, suggerisco di seguire alcune semplici regole:

a. Non effettuare mai alcuna indagine sul supporto originario, ma sempre su una copia di "dump".
b. Non effettuare alcun intervento di analisi singolarmente, ma sempre in presenza di almeno un testimone qualificato, ovvero di un soggetto con adeguata formazione tecnica che possa testimoniare sulla esecuzione di determinate procedure.
c. Utilizzare per quanto possibile strumenti (tipicamente videocamere, ma non solamente) che registrino tutta l'attività, nessuna esclusa, eventualmente riprendendo l'attività medesima da più angolazioni.
d. Verbalizzare, al termine dell'attività, quanto si è compiuto, e sottoscrivere il documento insieme agli eventuali testimoni.

e. Conservare nella maniera più accurata possibile quanto appena descritto, curando in particolar modo che tali documenti non possano essere alterati nel tempo.

3. Liceità dell'acquisizione della prova.

Occorre tenere presente che nel processo civile e penale vigono regole diverse per quanto concerne la raccolta delle prove, per cui – semplificando di molto il discorso – nel processo penale le prove acquisite attraverso una attività che possa essere considerata come reato NON SONO ammissibili, mentre la medesima regola non vige nel processo civile.

Poiché è abbastanza facile che si possa compiere un reato (ovvero, più esattamente, che questa possa essere l'obiezione che si solleva, con conseguente assoluta inutilizzabilità delle prove raccolte qualora l'eccezione venisse accolta) ritengo che, prima di "esternare" qualunque risultanza della propria attività, si debba agire di concerto con il team legale, al fine di valutare con estrema attenzione cosa "evidenziare" all'esterno, previa accurata analisi del report effettuato.

Il rischio non è solamente quello di non vedere ammesse le prove raccolte, ma di essere incriminati per qualche reato commesso. Un esempio pratico può rendere meglio il concetto: non è lecito sottoporre a controllo l'apparecchio telefonico del coniuge anche se al fine di scoprire se il medesimo stia commettendo un adulterio.

Inoltre occorre ricordare che dal 2001 esiste in Italia una legge sulle c.d. "indagini difensive", che ammette lo svolgimento di indagini anche al fine di "prevenire" dei reati, quindi non solamente dopo che i reati siano stati commessi.

Però, in unione con il t.u. delle leggi di pubblica sicurezza, tale legge non ammette che vengano svolte investigazioni se non dall'avvocato nominato ovvero dall'investigatore privato nominato.

Ricordo inoltre che – sempre ai sensi del t.u. appena citato – è reato svolgere investigazioni senza essere – appunto – un investigatore privato. Un modo abbastanza semplice per ovviare alla situazione è farsi nominare coadiutore tecnico dell'investigatore medesimo, il quale sottoscriverà il rapporto, anche se questo sarà stato – di fatto – eseguito dal tecnico, sotto il diretto controllo dell'investigatore nominato (o dell'avvocato).

Al contrario, il medesimo principio di "divieto" non esiste nel processo civile, per cui – di volta in volta – occorrerà effettuare una scelta "strategica" per decidere attraverso quale strumento "legale" perseguire l'attacker.

L'attività di investigazione privata – Le c.d. indagini difensive – ecc.[1]

La prima cosa che viene in mente è l'investigazione privata, poiché l'attività che essi svolgono sembra essere in tutto e per tutto assimilabile a questa, quello che eventualmente risulta differente sono soltanto i mezzi utilizzati.
Bisogna quindi solamente vedere se tali soggetti possano rientrare nella categoria suddetta.
L'attività di investigazione privata, nel nostro ordinamento è disciplinata dalla legge di P.S. n. 773/31 e dal regolamento n. 365/40 che specificano soprattutto i limiti e gli adempimenti da porre in essere da parte di questi soggetti.[2]

[1] Le parti che seguono sono state tratte dal "Manuale di Security Management" di Dario Forte e Luca de Grazia
[2] Abbiamo trattato questa figura in maniera più ampia nel capitolo due.

In questa sede è importante avere solamente alcune nozioni di base, e quindi conoscere l'esatta portata, per esempio, dell'art. 134[3] del Testo Unico di P.S. n. 773/31, e la giurisprudenza in merito.

Il dettato della norma ci sembra abbastanza chiaro ed univoco: "… *è vietato eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati..*", e la giurisprudenza appare porsi nel medesimo solco abbastanza restrittivo.

Per fortuna da qualche tempo è stata introdotta anche nel nostro sistema giuridico la legge n.7 dicembre 2000, n. 397, c.d. sulle "investigazioni difensive", attraverso la quale la parte privata (in particolare sia l'imputato, sia il "possibile" imputato, sia la parte offesa (ovvero il soggetto giuridico che ha subito le conseguenze del reato) possono svolgere delle investigazioni per proprio conto e, quel che più conta, il risultato di tali investigazioni può essere utilizzato nel processo come fonte di prova, come per esempio dimostrato dall'articolo riportato in nota[4].

Di notevole importanza è poi l'articolo 391-nonies C.P.P.[5], che prevede la possibilità di svolgere attività investigativa da parte del soggetto privato *in via preventiva*, in altre parole senza che necessariamente sia avvenuto un reato.

Tale possibilità va ovviamente coordinata con quanto statuito dal TU PS sopra richiamato, per cui il discorso risultante dovrebbe essere quello della necessità per il Security Manager di poter fornire adeguato supporto tecnico al proprio avvocato o investigatore privato professionista che stiano – appunto – ricercando delle prove a favore del comune Cliente.

Il nocciolo del problema, rimane, a parere di chi scrive, comprendere da un punto di vista "legale" le attività svolte dal "tecnico", e viceversa, al fine di poter giungere ad un assetto del sistema informatico conforme ai criteri di sicurezza "tecnici" richiesti, ma altrettanto "compliant" con le

---

[3] Art. 134 TU n.773/1931.
Senza licenza del Prefetto è vietato ad enti o privati di prestare opere di vigilanza o custodia di proprietà mobiliari od immobiliari e di eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati.
Salvo il disposto dell'art. 11, la licenza non può essere conceduta alle persone che non abbiano la cittadinanza italiana ovvero di uno Stato membro dell'Unione europea o siano incapaci di obbligarsi o abbiano riportato condanna per delitto non colposo. (1)
I cittadini degli Stati membri dell'Unione europea possono conseguire la licenza per prestare opera di vigilanza o custodia di beni mobiliari o immobiliari alle stesse condizioni previste per i cittadini italiani. (2)
La licenza non può essere conceduta per operazioni che importano un esercizio di pubbliche funzioni o una menomazione della libertà individuale.
(1)Comma modificato dall'art. 33, l. 1° marzo 2002, n. 39.
(2) Comma aggiunto dall'art. 33, l. 1° marzo 2002, n. 39.

[4] *Art. 391-sexies* - Accesso ai luoghi e documentazione.
1. Quando effettuano un accesso per prendere visione dello stato dei luoghi e delle cose ovvero per procedere alla loro descrizione o per eseguire rilievi tecnici, grafici, planimetrici, fotografici o audiovisivi, il difensore, il sostituto e gli ausiliari indicati nell'articolo 391-bis possono redigere un verbale nel quale sono riportati:
la data ed il luogo dell'accesso;
le proprie generalità e quelle delle persone intervenute;
la descrizione dello stato dei luoghi e delle cose;
l'indicazione degli eventuali rilievi tecnici, grafici, planimetrici, fotografici o audiovisivi eseguiti, che fanno parte integrante dell'atto e sono allegati al medesimo. Il verbale è sottoscritto dalle persone intervenute.

[5] *Art. 391-nonies* Attività investigativa preventiva.
1. L'attività investigativa prevista dall'articolo 327-bis, con esclusione degli atti che richiedono l'autorizzazione o l'intervento dell'autorità giudiziaria, può essere svolta anche dal difensore che ha ricevuto apposito mandato per l'eventualità che si instauri un procedimento penale.
2. Il mandato è rilasciato con sottoscrizione autenticata e contiene la nomina del difensore e l'indicazione dei fatti ai quali si riferisce.

normative di tipo legale. Si tratta di un tema che probabilmente verrà approfondito in altra pubblicazione.

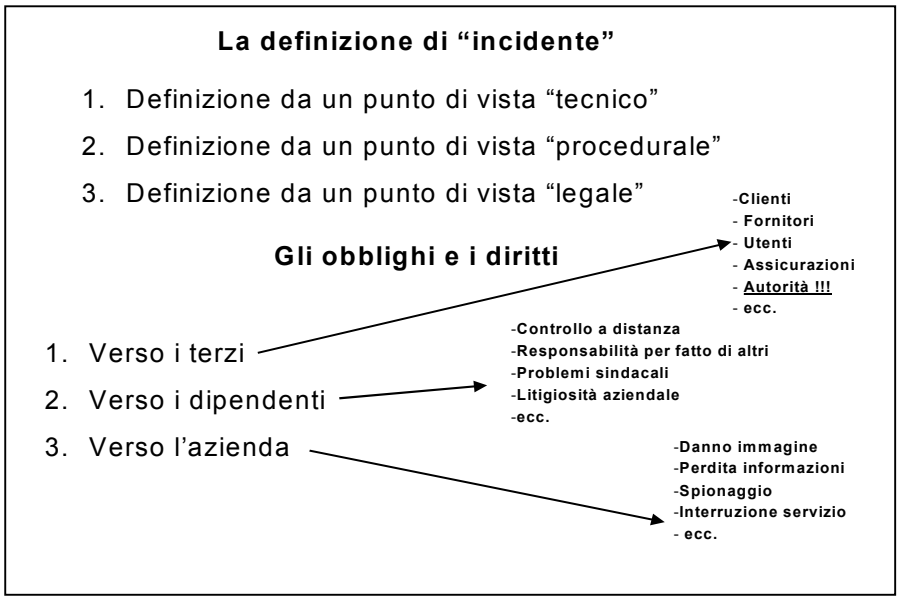
Cosa fare in caso di attacco ricevuto

E' sicuramente fondamentale che le procedure, come detto prima, siano state pianificate in precedenza e, ovviamente, "metabilizzate" mediante delle opportune esercitazioni, anche effettuate nell'ambito di una procedura di auditing. Di seguito alcuni consigli sulle operazioni piu' importanti da compiere:
Le procedure devono essere state approvate dal management. Ogni operazione effettuata deve riportare, anche in via riepilogativa, l'indicazione del manager che l'ha autorizzata; solitamente anche la modulistica viene approntata in via preventiva. Il formato elettronico della modulistica viene di solito memorizzato su Cd Rom[6], e tenuto pronto per qualsiasi evenienza.
Identificare *in tempo di pace* gli interlocutori di polizia a cui rivolgersi. Per identificazione intendiamo l'acquisizione di recapiti telefonici e fax dei vari uffici, con la loro ubicazione fisica per la successiva presentazione delle denuncie/querele.
Identificare in via prioritaria i consulenti/aziende esterne cui rivolgersi per eventuali forniture di servizi correlati alla pratica di incidente. Creazione immagini dischi, forensics iniziale, recovery dei dati, data collecting e quant'altro di correlato;
Identificare in via prioritaria, con controllo ciclico durante la procedura, i nominativi e le funzioni aziendali delle persone autorizzate a gestire l'incidente e le informazioni ad esso relative. Solo le persone autorizzate, che firmeranno il relativo *Non Disclosure Agreement*, potranno accedere alle informazioni concernenti l'attacco avvenuto e ai suoi sviluppi. In realta' la cosa migliore sarebbe creare un Incident Response Team, sottoporlo ad intense sedute di training e al quale dare l'incombenza di simulare ciclicamente un incidente, per verificare la congruita' delle procedure.
Pianificare *a priori* il piano di pubbliche relazioni. L'addetto alle PR o chi per lui, infatti, deve conoscere prima le informazioni che possono essere rilasciate e non. Questo e' un must per banche e istituzioni di tipo governativo.

Incident Handling – parte legale

In questa parte cercheremo di esaminare le linee guida che devono soccorrere l'ISM [7] nella gestione dei c.d. "incidenti informatici"; in primo luogo riteniamo sia necessario sia ogni soggetto provveda a redigere un elenco ed una catalogazione delle tipologie dei c.d. "incidenti informatici".
Infatti non sempre la concezione tecnico – informatica dell'incidente coincide con quella legale; in linea di massima si può affermare che il livello minimo di allerta viene sollecitato prima da un "incidente" di mero tipo legale, per i motivi che cercherò di spiegare nel prosieguo.
La schematizzazione riportata nell'immagine che segue probabilmente può essere utile a circoscrivere il problema.

[6] può anche costituire allegato alla policy di sicurezza a cui si riferisce.
[7] Acronimo per Information Security Manager



Riteniamo che sia importante chiarire che un "incidente informatico", che può assumere le più diverse forme (fermo macchina, sospensione e/o interruzione di un servizio, denial of service, diffusione di "virus", danneggiamento informatico, ecc. ecc.) è portatore di varie responsabilità da parte di chi lo subisce, nel senso che a seguito di tale incidente sorgono diritti e doveri nei confronti di vari soggetti, indicati in maniera esemplificativa nella diapositiva sopra riportata.
Cercando di andare più nel dettaglio, è opportuno tenere presente che in queste situazioni vanno a collidere due interessi che sembrano – a prima vista – completamente antitetici l'uno all'altro, in altre parole la necessità di intervenire il più presto possibile per ripristinare la situazione precedente all'incidente stesso, e la necessità di non prestare il fianco – manomettendo le evidenze informatiche che eventualmente abbiano subito un attacco da parte di terzi – a tutta la sequela di eccezioni che potrebbero essere sollevate (sempre da un punto di vista giuridico, che in questo caso non potrebbe non far leva su quelle che sono le risultanze di un'indagine sull'oggetto informatico compromesso) da parte del soggetto che si veda "imputato" dell'attacco stesso.
In altre parole, da una parte occorre "non toccare niente", mentre dall'altra è opportuno intervenire con la massima sollecitudine al fine di porre rimedio al "problema".
A prima vista questo potrebbe apparire un problema di poco conto, ma riteniamo che chiunque si sia trovato in una reale situazione di "allarme rosso" possa ben comprendere quanto le problematiche siano in linea di massima incompatibili.
Analizzando prima di tutto i rapporti con i terzi, si può citare – tra i tanti obblighi specificatamente imposti dalla legge – quello di avvisare l'assicuratore del sinistro entro un determinato termine [8] ovvero dalla possibilità che un qualunque incidente informatico possa

[8] Art. 1913 - Avviso all'assicuratore in caso di sinistro.
[I]. L'assicurato deve dare avviso del sinistro all'assicuratore o all'agente autorizzato a concludere il contratto, entro tre giorni da quello in cui il sinistro si e' verificato o l'assicurato ne ha avuto conoscenza. Non e' necessario l'avviso, se l'assicuratore o l'agente autorizzato alla conclusione del contratto interviene entro il detto termine alle operazioni di salvataggio o di constatazione del sinistro.
[II]. Nelle assicurazioni contro la mortalita' del bestiame l'avviso, salvo patto contrario, deve essere dato entro ventiquattro ore.

essere considerato come elemento fondamentale e costituente un aggravamento del rischio, con tutte ciò che ne può conseguire [9].

Cenni all'attività d'investigazione privata

La prima cosa che viene in mente è l'investigazione privata, poiché l'attività che essi svolgono sembra essere in tutto e per tutto assimilabile a questa, quello che eventualmente risulta differente sono soltanto i mezzi utilizzati.

Bisogna quindi solamente vedere se tali soggetti possano rientrare nella categoria suddetta.

L'attività d'investigazione privata, nel nostro ordinamento è disciplinata dalla legge di P.S. n. 773/31 e dal regolamento n. 365/40 che specificano soprattutto i limiti e gli adempimenti da porre in essere da parte di questi soggetti.

In Italia per svolgere tale attività è richiesta la preventiva licenza della competente Prefettura in cui ha sede l'Istituto d'investigazione, se questa è svolta professionalmente e in modo continuativo, e poi tutta una serie di requisiti che devono essere in possesso dei soggetti che materialmente operano, stabiliti dall'art. 134 del R.D. n. 773/31[10]:
Non essere sottoposto a sorveglianza speciale o misure di sicurezza
essere cittadino italiano
non aver riportato condanne penali per delitto non colposo
dimostrare di possedere la necessaria capacità tecnica
non aver subito con provvedimento definitivo l'applicazione di una misura di prevenzione
Dato importante è poi costituito dal fatto che nella domanda deve essere indicato il Comune o i Comuni nei quali si intende svolgere l'attività, in quanto la licenza è valida solo per questi, determinandosi al contrario l'esercizio di un'attività abusiva. La licenza è inoltre valida solo per un anno dovendosi poi rinnovarla con richiesta specifica.

---

[9] *Art. 1898* Aggravamento del rischio.
[I]. Il contraente ha l'obbligo di dare immediato avviso all'assicuratore dei mutamenti che aggravano il rischio in modo tale che, se il nuovo stato di cose fosse esistito e fosse stato conosciuto dall'assicuratore al momento della conclusione del contratto, l'assicuratore non avrebbe consentito l'assicurazione o l'avrebbe consentita per un premio piu' elevato.
[II]. L'assicuratore puo' recedere dal contratto, dandone comunicazione per iscritto all'assicurato entro un mese dal giorno in cui ha ricevuto l'avviso o ha avuto in altro modo conoscenza dell'aggravamento del rischio.
[III]. Il recesso dell'assicuratore ha effetto immediato se l'aggravamento e' tale che l'assicuratore non avrebbe consentito l'assicurazione; ha effetto dopo quindici giorni, se l'aggravamento del rischio e' tale che per l'assicurazione sarebbe stato richiesto un premio maggiore.
[IV]. Spettano all'assicuratore i premi relativi al periodo di assicurazione in corso al momento in cui e' comunicata la dichiarazione di recesso.
[V]. Se il sinistro si verifica prima che siano trascorsi i termini per la comunicazione e per l'efficacia del recesso, l'assicuratore non risponde qualora l'aggravamento del rischio sia tale che egli non avrebbe consentito la assicurazione se il nuovo stato di cose fosse esistito al momento del contratto; altrimenti, la somma dovuta e' ridotta, tenuto conto del rapporto tra il premio stabilito nel contratto e quello che sarebbe stato fissato se il maggiore rischio fosse esistito al tempo del contratto stesso.
[10] Art. n. 134 R.D. 773/31 - Senza licenza del Prefetto è vietato ad enti o privati di prestare opere di vigilanza o custodia di proprietà mobiliari od immobiliari e di eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati (114).
Salvo il disposto dell'art. 11, la licenza non può essere conceduta alle persone che non abbiano la cittadinanza italiana o siano incapaci di obbligarsi o abbiano riportato condanna per delitto non colposo.
La licenza non può essere conceduta per operazioni che importano un esercizio di pubbliche funzioni o una menomazione della libertà individuale

L'autorizzazione può essere richiesta sia da un privato sia da una società, in questo caso in persona del legale rappresentante che si assume la piena responsabilità in ordine all'attività esercitata.
Altri e più specifici obblighi di comportamento sono poi stabiliti dagli articoli seguenti del R.D. in ordine agli adempimenti, ai registri e alle cauzioni da versare[11].
Dell'attività d'investigazione privata svolta professionalmente si è anche occupato il legislatore per la necessità di coordinarla con la L. 675/96, con l'Autorizzazione n. 6/2000 al trattamento d'alcuni dati sensibili da parte degli investigatori privati, e questo soprattutto a seguito delle modifiche che sono intervenute nel codice penale che hanno riconosciuto un più largo campo d'azione a questi soggetti nella ricerca di fonti di prova atti a consolidare le tesi della difesa nel processo penale.
Il nocciolo della nuova disciplina risulta quindi essere questo:

quando l'investigatore privato svolge la sua opera professionalmente e al fine di acquisire informazioni utili per far valere o difendere un diritto in sede giudiziaria, dispone di una serie di deroghe alla legge n. 675/96;
mentre se le investigazioni sono svolte per fini diversi, ossia come reperimento di dati e notizie che non hanno un esplicito riferimento ad un'attività giudiziaria, al soggetto è applicata integralmente la disciplina dettata a tutela dell'altrui riservatezza della legge in questione.
Per quanto riguarda espressamente le deroghe alla 675/96 esse vertono in tema di notificazioni al Garante, autorizzazioni dello stesso, di consenso al trattamento dei dati personali da parte dell'interessato.
Per quanto riguarda, invece, l'attività d'investigazione per fini diversi da quelli sopra specificati, il trattamento dei dati raccolti durante detta attività sarà in tutto e per tutto soggetto alla normativa prevista dalla L. 675/96, e quindi l'investigatore privato potrà procedere al trattamento dei dati solo con il consenso scritto dell'interessato e se i dati sono sensibili, con l'autorizzazione del Garante.
Ora ritornando all'attività di qualsiasi soggetto che esegua un determinato tipo d'attività di "reperimento informazioni", sembra potersi affermare che qualora questi sia materialmente incaricato di verificare la sicurezza di un sistema informatico si comporti materialmente come un vero e proprio investigatore privato, solo che per farlo utilizza strumenti informatici.
Ci si pone quindi una domanda su quale sia la posizione e quali sono le regole che si devono rispettare nell'espletare tale attività e quali i limiti. Non essendo IRItaly un documento di mera impostazione legale, si rimanda eventualmente ad una trattazione abbastanza approfondita si trova nel Manuale[12] citato.

[11] Art. 137 R.D. 733/31 - Il rilascio della licenza è subordinato al versamento nella cassa depositi e prestiti di una cauzione nella misura da stabilirsi dal Prefetto.
La cauzione sta a garanzia di tutte le obbligazioni inerenti all'esercizio dell'ufficio e della osservanza delle condizioni imposte dalla licenza.
Il Prefetto, nel caso di inosservanza, dispone con decreto che la cauzione, in tutto o in parte, sia devoluta all'erario dello Stato.
Lo svincolo e la restituzione della cauzione non possono essere ordinati dal Prefetto, se non quando, decorsi almeno tre mesi dalla cessazione dell'esercizio, il concessionario abbia provato di non avere obbligazioni da adempiere in conseguenza del servizio al quale l'ufficio era autorizzato
[12] Manuale di Information Security Management