WWW.Criminologia.org
TELEMATIC JOURNAL OF CLINICAL CRIMINOLOGY
Telematic Journal of Clinical Criminology - www.criminologia.org International Crime Analysis Association

Il computer crime nelle organizzazioni: problematiche investigative

Di Marco Strano

Le tecniche investigative nei casi di computer crime

Spesso l'obiettivo principale di una investigazione nell'ambito del computer crime è quello di scoprire chi si è introdotto abusivamente in un sistema e come ciò sia avvenuto. In effetti la maggior parte dei computer crime vengono scoperti dalla vittima accidentalmente a distanza di tempo e poi verificati attraverso la laboriosa revisione di lunghissime liste di dati.
Talvolta è però possibile il monitoraggio di una intrusione in tempo reale (segnalata magari dai software di protezione). Una volta scoperto l'attacco al sistema informatico è fondamentale ridurre al minimo i rischi di ulteriori perdite e possibilmente cercare di acquisire elementi utili per la scoperta del colpevole. Queste due attività sono spesso in antagonismo logico tra loro. Il sistema migliore per interrompere un attacco è infatti spesso quello di spegnere il sistema e procedere al ricaricamento delle copie di sistema pulite e dei programmi applicativi. Tuttavia, tale operazione nella maggior parte delle volte riduce le possibilità di identificazione dell'intruso.
Quando inizia un'indagine su un crimine informatico all'interno di un'azienda l'elemento fondamentale da curare è rappresentato dall'assoluta riservatezza. Le strutture aziendali dovrebbero collaborare con gli organi investigativi ma le informazioni sull'investigazione in atto dovrebbero essere trasmesse al minor numero di persone possibili per limitare una fuga di notizie all'interno e all'esterno dell'organizzazione. Tali informazioni andrebbero quindi fornite solamente a chi ne debba per forza venire a conoscenza. Inoltre, tutte le comunicazioni collegate all'accadimento dovrebbero essere effettuate non utilizzando i sistemi informatici (email, intranet eccetera) al fine di evitare qualsivoglia intercettazione da parte dell'intruso.
L'intervento degli investigatori informatici, chiamati dall'azienda, inizia solitamente con un'indagine preliminare interna che tende in primo luogo ad accertare l'effettiva presenza di un crimine. Nel caso che ciò venga accertato, l'indagine cerca di stimarne tanto la natura quanto la gravità. L'investigatore deve infatti considerare che di fronte a un presunto attacco o a un'intrusione telematica non sempre si può parlare di crimine. Anche in presenza di elementi che lascino presagire l'espletamento di una condotta criminale ci si potrebbe infatti trovare davanti a un semplice errore. Le indagini preliminari di norma tendono quindi a riesaminare la denuncia iniziale del crimine e le varie testimonianze, a verificare il presunto danno o abuso e infine a controllare i filelog del sistema operativo. Qualora nella fase delle indagini preliminari si abbia la certezza di trovarsi in presenza di una presunta attività criminale, l'investigatore dovrebbe cercare di individuare gli elementi costitutivi del crimine in questione, onde poter delineare la fattispecie delittuosa presente. Nella prima fase, in caso di sospetti su possibili autori "insiders", né l'investigatore né tanto meno gli impiegati della società dovrebbero affrontare o parlare con tali sospetti per non dar loro modo di nascondere o cancellare le prove.
Dopo la fase preliminare, dopo che in pratica si è certi della presenza di un reato informatico e si sono raccolti i primi elementi, l'attività investigativa prosegue di solito con indagini convenzionali (interrogatori ed acquisizione di documenti cartacei) e con indagini telematiche, queste ultime talvolta in collaborazione con tecnici specializzati o programmatori informatici (anche dell'azienda vittima) che possono affiancare le forze di polizia durante gli interventi.

La determinazione investigativa primaria è quella che cerca di stabilire se un crimine informatico è opera di un insider o di un esterno o di entrambe le figure criminali[1]. E' importante che l'investigatore, qualora pensi di non avere la competenza necessaria per svolgere alcune delle operazioni si avvalga dell'intervento di un esperto prima di procedere.
Emerge quindi da questo quadro l'esigenza primaria di collaborazione da parte dell'organizzazione vittima di computer crime nel corso dello svolgimento dell'indagine al fine di facilitare l'identificazione e la descrizione delle eventuali prove rinvenute.

Le prove elettroniche
Le caratteristiche del cyberspazio implicano la necessità da parte degli investigatori e dei responsabili della sicurezza aziendale di prendere dimestichezza con una nuova filosofia dell'investigazione. Il "luogo del delitto", nei casi di computer crime è infatti costituito in parte da un ambiente elettronico e le prove di tali crimini sono costituite quindi da dati elettronici che dimostrano talune operazioni illegali avvenute all'interno di un computer. I dati elettronici comprendono tutti quei record, file, codici sorgente, programmi, altre tracce contenuti nel sistema di memoria del computer. Vista la diversificazione di impiego del computer nella società di oggi, le prove elettroniche arrivano ad assumere le forme più disparate. Possono essere sofisticati documenti di testo, database del personale, liste clienti, informazioni finanziarie, e-mail inviate tramite Internet e messaggi di Intranet locali, sistemi di pianificazione elettronica, file-log, trascrizioni di e-mail vocali eccetera.
I dati contenuti nelle memorie di un computer sono talvolta in grado di far accusare o prosciogliere un imputato e rappresentano quindi un elemento fondamentale nei casi di computer crime. Talvolta i dati che costituiscono una prova vengono cancellati in un computer (volutamente o inavvertitamente). Tuttavia il loro recupero è spesso possibile anche se tale operazione richiede abilità e competenza. Gli investigatori esperti possono infatti attualmente accedere con sicurezza a qualsiasi sistema informatico, rete o memoria per recuperare dati e determinare se siano stati manomessi, cancellati o danneggiati.
In alcuni casi gli investigatori hanno semplicemente bisogno di informazioni contenute sugli hardisk per le loro indagini, perciò non è necessario che sequestrino l'intero mezzo informatico. Una volta aver tracciato o fotografato lo schema del sistema, l'hardisk può essere rimosso e quindi trasportato in un laboratorio forense per essere copiato. Grazie all'uso di un *forensic software* si possono ottenere delle copie speculari del disco incriminato, una delle quali potrà poi essere restituita al presunto autore del crimine per permettergli di continuare a lavorare con il computer.
In altri casi, quando si raccolgono le prove in un computer crime, è invece necessario il sequestro degli apparati informatici e tale procedura di fatto impedisce al proprietario degli apparati qualsiasi utilizzo del sistema per un certo periodo, fino alla restituzione degli apparati.
Per le loro caratteristiche fisiche gli apparati che contengono le prove elettroniche nei casi di computer crime, necessitano di una particolare cura per il loro trasporto e la loro conservazione. Tutto il materiale dovrebbe essere impacchettato e conservato con delle tecniche specifiche per proteggerlo dal calore, dal freddo intenso, dall'umidità, dall'acqua, da campi magnetici e dalle vibrazioni affinché se ne possa disporre in futuro (anche per poterlo restituire al legittimo proprietario in condizioni accettabili). Qualora le prove non siano protette nel modo appropriato, le informazioni in esse contenute potrebbero divenire illeggibili. Documenti e dischi (quali hard disk, floppy e dischi a lettura ottica) dovrebbero essere infatti sequestrati e immagazzinati in container appositi per prevenirne il danneggiamento. Ad esempio, secondo quanto indicato dagli esperti statunitensi, gli hard disk dovrebbero essere impacchettati in una scatola anti-statica all'interno di una scatola di cartone rivestita di gommapiuma. Sarebbe meglio affidare queste operazioni di imballaggio a un addetto di sistema o a un consulente tecnico, soprattutto quando si tratta di mini-sistemi o elaboratori centrali. Infine, le prove dovrebbero essere trasportate in un luogo apposito, dedicato alla

[1] Quando ad esempio si ha il sospetto che un sistema informatico sia oggetto di un attacco da parte di un hacker esterno, il modo giusto per impedire a un operatore a distanza di cancellare i file di memoria non è quello di togliere l'alimentazione alla macchina, bensì di scollegare il modem. Scollegare la linea telefonica dal modem impedisce agli operatori a distanza di accedere al sistema, senza peraltro rischiare che i documenti aperti vadano perduti.

conservazione di materiale elettronico. Capita a volte che le apparecchiature informatiche risultino essere troppo ingombranti da poter essere trasportate, come nei casi di grandi elaboratori centralizzati. In questi casi, l'esame forense dovrà evidentemente avvenire sul luogo e tale operazione potrebbe comportare ulteriori problematiche tecnico-investigative. Ovviamente, per la peculiarità del luogo dove è avvenuto il crimine, sarebbe sempre auspicabile un aiuto dell'organizzazione vittima agli organi di Polizia che stanno operando.