Questo articolo è apparso sul Corriere del Ticino di lunedì, 10 maggio 2005 nella sezione Primo piano

Reati informatici e prove digitali

È in costante aumento il numero di delinquenti che operano soprattutto su Internet. La rete facilita sia i crimini tipici dell'ambiente tecnologico sia quelli più « classici »

Silvano Marioni **www.marioni.org**

Oggi in tutto il mondo è in costante aumento il numero dei reati informatici e questo indica che c'è un aumento dei delinquenti che hanno familiarità con le nuove tecnologie. In particolare questi tipi di reati stanno diventando sempre più frequenti su Internet dove si manifestano come crimini tipici dell'ambiente informatico quali l'accesso illecito a sistemi di computer, il cyberterrorismo, il furto di dati informatici, il deterioramento o il blocco di siti Internet, la diffusione di virus informatici, il sabotaggio delle infrastrutture critiche. Ma i reati informatici non hanno solo a che fare con il danneggiamenti dei sistemi informativi. Dallo spionaggio alle malversazioni finanziarie, dalla pornografia infantile ai vari tipi di truffa, siamo di fronte a crimini che esistevano anche prima della diffusione dei computer ma che oggi con l'aiuto di Internet possono essere compiuti su scala più ampia e con maggiore efficacia.

La pornografia infantile – per fare un esempio – era presente anche prima degli anni ' 90, ma con l'avvento di Internet si è diffusa presso fasce di persone sempre più vaste. Una recente statistica inglese indica come gli arresti per questo tipo di reato siano passati da 35 nel 1988 ad oltre 2' 000 del 2003 con un aumento del 6'500% dovuto principalmente all'utilizzo di Internet. Possiamo quindi affermare che anche nel caso di reati di tipo « tradizionale » il nuovo mezzo informatico ne modifica la natura rendendoli più immediati da commettere e più impegnativi da reprimere. Sta emergendo una nuova categoria di delinquenti che in solitudine di fronte al computer e forti della loro identità virtuale, commettono azioni delittuose che non avrebbero mai il coraggio di compiere al di fuori del cyberspazio. Lo schermo diventa una protezione che altera la percezione dell'illegalità del comportamento e del danno procurato alla vittima e accresce la sensazione di non essere scoperto. Esistono anche dei criminali che svolgono attività per puro fine di lucro con decisione e competenza tecnica. I loro reati si presentano come attività apparentemente innocue quali lo spamming, utilizzato per ingannare le persone con frodi e truffe, o la diffusione di virus, o ancora attacchi diretti finalizzati a ricatti e estorsioni nei confronti di persone o organizzazioni. Senza dimenticare le malversazioni finanziarie che ormai non possono più essere fatte senza coinvolgere almeno in parte i sistemi informatici delle aziende. Ma ogni reato informatico lascia delle tracce. Esse possono essere utilizzate nelle indagini e nel successivo dibattimento. Spesso queste prove possono essere raccolte facilmente soprattutto nel caso in cui chi ha compiuto un reato non ha molta familiarità con l'informatica e non conosce le caratteristiche dei documenti elettronici.
Al contrario dei documenti cartacei, che possono essere distrutti in modo diretto e visibile, i documenti elettronici hanno una loro natura più persistente. Ogni volta che un documento elettronico viene creato o consultato lascia delle tracce che non sono così semplici da fare scomparire.
Non è sufficiente cancellare un documento perchè questa azione cambia semplicemente lo stato del documento rendendolo invisibile al normale utilizzatore del computer ma lasciandolo perfettamente accessibile agli strumenti di indagine informatica.
Inoltre possono esistere più copie di un documento su differenti server, sui supporti di backup, sulla rete aziendale o addirittura sulla rete pubblica o su altre reti. La posta elettronica è un caso tipico dove spesso si lasciano tracce compromettenti anche senza rendersene conto.
È famoso il caso del messaggio inviato da Nancy Temple, avvocato dell'Arthur Andersen, ad un manager della Enron in cui suggeriva un comportamento illegale per evitare problemi con la Security and Exchange Commission e che è stato un elemento fondamentale utilizzato dai giudici per incriminare sia la Enron che l'Arthur Andersen.
Per investigare sui reati compiuti con l'utilizzo di strumenti tecnologici, sono richieste particolari metodologie di indagine. Sono necessarie nuove procedure per raccogliere e produrre le prove informatiche garantendo la «catena di custodia» a partire dalla vittima del reato, passando dalle autorità inquirenti e fino al giudice.
Questo perché le prove digitali sono dei dati e delle informazioni per loro natura estremamente fragili che esistono, vengono memorizzate, o sono trasmesse per il tramite delle

apparecchiature elettroniche.
Queste prove possono essere evidenziate solo attraverso opportuni programmi e se non sono trattate nel modo corretto possono essere danneggiate o distrutte. Questo mostra i rischi che esistono per garantire il loro valore probatorio e evidenzia quanto sia importante utilizzare tutte le precauzioni necessarie per raccoglierle, conservarle e presentarle davanti a un tribunale.
In definitiva di fronte ai reati informatici si presentano nuove problematiche che richiedono un comportamento più attento da parte di chi li subisce e una rinnovata capacità di analisi e valutazione da parte delle autorità inquirenti e giudiziarie.

Criminalità su Internet e indagini in Svizzera

Intervista con Olivier Ribaux, esperto di diritto delle nuove tecnologie all'UNI di Losanna

Quale è la situazione nelle indagini informatiche in Svizzera? Ne parliamo con Olivier Ribaux professore straordinario presso l'École des Sciences Criminelles dell'Università di Losanna dove si occupa di diritto delle nuove tecnologie e tratta il tema delle prove digitali e il loro utilizzo nell'investigazione criminale. Il professor Ribaux lavora inoltre come analista criminale presso la Polizia cantonale vodese per i cantoni della Svizzera romanda.

Non esiste da parte dell'opinione pubblica una chiara percezione dei reati informatici. Può darci un'idea di come essi stiano aumentando in Svizzera e nel mondo, in particolare i reati su Internet? Quali sono i reati più frequenti e quali, secondo lei, i più pericolosi.

« La percezione dei reati informatici e del loro impatto non è un argomento molto chiaro per il grande pubblico. Spesso si citano casi di aziende che avrebbero avuto perdite finanziarie astronomiche ma è difficile interpretare o approfondire queste cifre. Inoltre, dato che raramente le vittime sporgono denuncia, la polizia ha una visione molto limitata dell'ampiezza del fenomeno. I reati conosciuti possono solo darci un'idea approssimativa del problema.
In particolare, siamo stati tutti sorpresi dal numero di « consumatori » in materia di pedofilia coinvolti nell'affare GENESIS nel 2002, quando è stato possibile sorprendere diverse centinaia di « clienti » svizzeri. L'utilizzo fraudolento delle carte di credito su Internet sembra che abbia acquistato una certa importanza, ma va anche detto che questo può essere fatto anche in caso di semplici furti di portamonete nei quali i malfattori trovano le carte e spesso … il codice scritto sulla carta. In questo caso commettere un reato informatico non implica necessariamente l'utilizzo di grandi competenze tecnologiche!
Oggi si sta delineando una tendenza generale: l'informatica permette di diluire le attività criminali internazionali in una moltitudine di piccoli reati che passano inosservati o rappresentano un rischio trascurabile per gli autori. Per esempio, tutti noi riceviamo nella casella di posta elettronica messaggi che, con pretesti diversi (vincite alla lotteria, dittatore deposto che ci supplica di aiutarlo a far uscire i suoi « risparmi » dal suo paese, ecc), ci esortano a versare su un conto all'estero una piccola somma con la promessa di guadagni strabilianti. La moltiplicazione dell'invio di simili messaggi non costa niente e permette di raggiungere una grande quantità di vittime potenziali e ingenue che possono alimentare i conti bancari dei truffatori ».

Quali problemi si incontrano nella ricerca e nella repressione efficace dei reati informatici e come si differenziano le tecniche di indagine rispetto ai reati tradizionali. Nelle indagini informatiche esiste un rischio maggiore di interferire nella sfera privata di cittadini innocenti?

« Il modo di procedere di un'inchiesta su un reato informatico è molto più pluridisciplinare rispetto a quello su un reato tradizionale e implica sovente la collaborazione di organismi diversi. È necessario confrontare le varie competenze oltre i confini cantonali e nazionali per essere in grado di applicare le leggi, unitamente ai metodi di prevenzione e di repressione, in modo sufficientemente rapido. È questo appunto lo scopo del Master « DEA en droit, criminalité et sécurité des nouvelles technologies » che abbiamo sviluppato all'Università di Losanna.
Gli inquirenti in quasi tutte le polizie sono stati affiancati da specialisti per consolidare la

gestione delle informazioni individuali. Questo ricorso a dei professionisti offre alcune garanzie in materia di protezione della sfera privata perché anche se ci sono delle regole che delimitano l'uso delle informazioni, non è facile trovare l'equilibrio tra l'efficacia delle misure repressive e le restrizioni imposte dalla legge. Le imprese private o le amministrazioni potrebbero essere tentate di utilizzare i propri dati a fini di inchieste interne o allorquando l'organizzazione subisce un attacco informatico. Qui c'è un rischio di svolgere delle attività approssimative: infatti prelevare, archiviare e interpretare gli indizi in un contesto legale è una vera e propria professione.
Ci sono ancora da compiere dei progressi per sistematizzare gli scambi in un quadro giuridicamente accettabile ed efficace tra le autorità giudiziarie e le società dove vengono svolte le indagini ».

La natura extraterritoriale di Internet richiede delle soluzioni a livello internazionale.

Quali sono le risposte a questo problema e quanto sono efficaci. Quali sono i loro limiti nelle attività di indagine e di repressione della criminalità e del terrorismo informatico?

« In molti paesi ci sono ancora numerosi problemi legati all'impossibilità di condurre un'inchiesta in modo efficace o alla lentezza imposta dai processi di cooperazione. Tuttavia, chi avrebbe creduto che un'operazione come GENESIS, che ha dato un segno molto forte a persone che credevano di agire in tutta impunità, sarebbe stata un giorno possibile? Il dibattito giuridico è attualmente molto vivace e si stanno mettendo a punto con una certa efficacia nuovi metodi di collaborazione, soprattutto a livello di Unione europea. Anche la Svizzera, malgrado il suo statuto a volte precario, segue queste evoluzioni nei gruppi di lavoro ».