Fabio Di Nunno

Cybercrime: nuove sfide e minacce in evoluzione

La sicurezza informatica è ormai un elemento strategico per garantire la prosperità economica e sociale di un Paese. Infatti, lo sviluppo sempre più veloce ed intenso delle tecnologie dell'informazione e della comunicazione si accompagna alla diffusione altrettanto rapida ed estesa di nuove forme criminose, che è possibile raggruppare nella categoria della criminalità informatica, e che evolvono molto più speditamente rispetto alle soluzioni giuridiche necessarie per risolvere i problemi che si presentano. Basti pensare alle azioni condotte da gruppi terroristici sempre più basate sulle nuove tecnologie, allo sviluppo continuo di reti legate alla pornografia o alla pedofilia, ai traffici illeciti di armi, droga, esseri umani, denaro sporco. Oltre a questi problemi globali, più di un milione di individui, ogni giorno, sono vittime di crimini informatici. A ciò si aggiungono altre azioni che chiunque, anche inconsapevolmente, può oggi compiere.

Secondo alcuni dati forniti da Symantec, su un campione di 24 Paesi, il 44% degli adulti sono stati vittime di crimini online, rispetto al 15% degli adulti vittime di crimini offline, mentre in Italia la percentuale di vittime di cybercrime sale al 68%. Ciononostante, la criminalità informatica non consiste in una categoria definita giuridicamente, anche se compare in fonti europee e sovranazionali. Analogamente, non esiste una definizione internazionalmente riconosciuta di "computer crime" o "computer related crime" o "cybercrime". Però, è certo che esiste un cyberspace, cioè uno spazio virtuale che permette la *delocalizzazione* delle risorse e la loro raggiungibilità, da parte dell'utente, da ogni luogo e distanza, anche grazie alle nuova dimensione del *cloud computing*. Ciò si accompagna alla *detemporalizzazione* delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, senza che vi sia la necessità della sua presenza fisica al computer. Quindi, Internet e le nuove tecnologie della comunicazione e dell'informazione presentano potenzialità criminogene mentre il fenomeno della criminalità informatica risulta essere flessibile ed aperto a fatti criminosi che possono essere commessi attraverso la rete o nel cyberspace.

Rifacendosi alla dottrina americana, nella categoria del cybercrime possono essere incluse tre sub-categorie:

a) reati in cui il computer o il sistema informatico costituiscono l'obiettivo delle attività criminali;

b) reati in cui il computer, le nuove tecnologie ed Internet, rappresentano gli strumenti per commettere o preparare un reato;

c) reati in cui il sistema informatico e la rete costituiscono solo un "aspetto incidentale" nella commissione dell'illecito.

La Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001 ed entrata in vigore nel luglio 2004, è l'unico trattato internazionale vincolante esistente oggi su tale tema. Il trattato stabilisce le linee guida per tutti gli Stati che vogliano sviluppare una legislazione nazionale completa contro la criminalità informatica ed individua alcuni crimini informatici:

1. Accesso illegale ad un sistema informatico
2. Intercettazione abusiva
3. Attentato all'integrità dei dati
4. Attentato all'integrità di un sistema
5. Abuso di apparecchiature
6. Falsificazione informatica
7. Frode informatica
8. Reati relativi alla pornografia infantile
9. Reati contro la proprietà intellettuale

L'attenzione al fenomeno è in crescita e, in Europa, con l'entrata in vigore del Trattato di Lisbona la criminalità informatica è stata inserita, nell'art. 83 del Trattato sul Funzionamento dell'Unione Europea, fra i fenome-



ni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale. Oltre ai fenomeni ormai noti da anni, molteplici sono le minacce che si stanno sviluppando e rendendo più insidioso il fenomeno del crimine informatico. Infatti, lo sviluppo del mobile computing significa anche lo sviluppo del cybercrime *mobile*, che si traduce in un rischio per le transazioni e i pagamenti tramite dispositivi mobili, il phishing su dispositivi mobili (vishing e smishing) e mobile applications fraudolente. A ciò si aggiunge il crescente uso di sistemi personali per accedere a dati aziendali sensibili (*Byod - Bring Your Own Device*), che presenta rischi di violazione dei sistemi aziendali attraverso i dispositivi personali dei dipendenti. D'altronde le aziende saranno anche sottoposte sempre più ad attacchi al cloud o attraverso il cloud.
Ancora, indubbiamente persiste la creazione di financial bancking trojan e malware, dove però ai malware tradizionali vengono apportare delle aggiunte personali, con l'uso tipico dalla lingua inglese ma con incremento dell'uso della lingua russa. Poi, continua il furto di account e di cyberattaccchi condotti manualmente, ma ai tradizionali attacchi Trojan *man-in-the-browser* si affianca un crescente uso di attacchi Trojan *man-in-the-middle*, dove, cioè, vi è la presenza fisica di un operatore a condurre l'attacco informatico. Gli stessi attacchi informatici stanno migliorando la loro effettività grazie a data filtering e data charting e, quindi, lo sviluppo di modelli malware più sofisticati grazie a data analytics, mentre l'uso incrementale dei social network può essere un ulteriore vettore di attacchi informatici sempre più personalizzati (*social networking feeds*).
Oltre a tutto questo, cresce il fenomeno dell'hacktivism, cioè di attacchi informatici per ragioni ideologiche, sociali, politiche, ecc. Seppure viste come forme di protesta ideologica o di espressione pubblica di opinioni sociali e politiche controverse, il fenomeno presenta rischi crescenti dato l'avvento di gruppi di hacktivists e lo sviluppo di legami tra hacktivists e cybercriminali motivati da scopi economici. Infine, la nuova frontiera degli attacchi informatici arriva allo spazio e possono coinvolgere la Stazione Spaziale Internazionale, i satelliti ed altre infrastrutture spaziali che sono ormai indispensabili per la vita qutodiana, come le previsioni meteo, i canali televisivi satellitari, la sincronizzazione delle operazioni bancarie, la trasmissione delle operazioni di trading, la navigazione aerea, marittima e terrestre, il Gps delle operazioni militari. In considerazione della portata transanazionale del crimine informatico, si sono sviluppate varie forme di cooperazione formale ed informale tra Stati, attraverso dei meccanismi regionali (Convenzione del Consiglio d'Europa sulla criminalità informatica, Convenzione della Lega degli Stati Arabi, ecc.) e dei network (Interpol, Europol, G8, NATO Cooperative Cyber Defence Centre of Excellence, ecc.).
Comunque, al di là degli scenari delineati, il cybercrime è davvero molto vicino a ciascuno di noi: basta rammentare i reati contro la proprietà intellettuale che vengono compiuti ogni giorno da persone comuni, anche semplicemente scaricando dal web un film. Infatti, il 31 marzo 2014 l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) ha emanato un regolamento per il copyright online, prima iniziativa in Italia volta ad affrontare in via amministrativa la pirateria online (e radiotelevisiva) e contrastare la messa a disposizione in rete di opere digitali in violazione del diritto d'autore dei titolari. La procedura è semplice e si svolge completamente online, tramite il sito www.ddaonline.it. La nuova procedura permette all'AGCOM di ordinare la rimozione selettiva dei contenuti in violazione dei diritti d'autore e la disabilitazione dell'accesso ai suddetti contenuti. Chiaramente tutto ciò apre scenari che è difficile prevedere, soprattutto per quanto riguarda l'applicazione, da parte dell'AGCOM, dei principi di gradualità, proporzionalità e adeguatezza. Per esempio, essendo possibilie ricorrere ad una procedura d'urgenza abbreviata (grazie alla quale il procedimento si conclude in 12 giorni invece dei 35 altrimenti previsti dalla procedura standard), la violazione relativa a un film in proiezione in quel momento nelle sale potrebbe essere considerata degna di maggiore tutela rispetto alla violazione relativa ad un film di qualche tempo prima? Il quadro delienato finora non è certo esaustivo, eppure offre un panorama variegato delle minacce che il cybercrime pone a singoli individui, ad aziende e ad interi Paesi, facendo emergere al contempo la necessità di definire una strategia di cybersecurity (sicurezza informatica) che va anche al di là dei confini nazionali.

