Digital Investigations tra Cloud, Mobile e GDPR - intervista a Mattia Epifani

Date : 5 febbraio 2018

Lei opera nel settore delle *Digital Investigations* collaborando con tribunali, Forze dell'Ordine, studi legali e aziende nei settori della *digital forensics*, *data protection* e *incident response*. Nella sua esperienza professionale ha occasione di riscontrare differenze di approccio tra interlocutori pubblici e privati?

Ci sono sicuramente delle differenze. Spesso quando si lavora con un privato si cercano riscontri di comportamenti che non necessariamente implicano ipotesi di reato, poiché può trattarsi di dipendenti (o manager) infedeli ovvero di violazioni delle *policies* aziendali, che l'azienda ha interesse a svelare anche se prive di rilevanza penale. Quando lavoriamo con realtà imprenditoriali, tuttavia, verifichiamo sempre che queste ricerche restino nel solco della legittimità.

Quando invece operiamo a fianco delle autorità giudiziarie, disponiamo di poteri d'indagine più ampi: ad esempio l'analisi di un dispositivo, una volta autorizzata da un Pubblico Ministero, può essere a 360 gradi anche nel caso di utilizzo promiscuo del dispositivo, mentre un'indagine commissionata dal datore di lavoro dovrebbe avere cura di escludere ogni contenuto privato per concentrarsi esclusivamente su dati e attività relativi all'uso aziendale.

Anche il ricorso sempre più frequente ai sistemi Cloud da parte dei vari dispositivi (sia Android sia iOS) per l'archiviazione e la conservazione dei dati solleva importanti complicazioni di natura tecnica e giuridica: pensiamo alle questioni di giurisdizione, alla territorialità del dato, alla necessaria individuazione dell'autore materiale del fatto in caso di responsabilità penali. È possibile superare tali difficoltà nell'ambito investigativo e giudiziario?

Rispetto al Cloud e alle altre tecnologie che delocalizzano i dati indirizzandoli a *server farm* sparse per tutto il globo, il vero limite è rappresentato dalle questioni di territorialità. In generale, il dibattito giuridico si sta interessando alla questione; esistono già strumenti formali a disposizione degli inquirenti, un passo importante è stato rappresentato dallo *European Investigation Order* - ma la direzione in cui si sta cercando di lavorare è sempre più quella della cooperazione e della *voluntary disclosure* che, oltre ad abbreviare drasticamente i tempi,

consente di ottenere informazioni anche da *service provider* che abbiano sede in Paesi che non hanno sottoscritto accordi internazionali in materia. I meccanismi volontari, d'altro canto, rischiano di implicare logiche discriminatorie per gli utenti: a titolo di esempio, le *big corporations* statunitensi come Google, Apple o Microsoft tendono a tutelare maggiormente i dati in loro possesso quando questi appartengano a cittadini USA.

Per quanto riguarda la tecnologia *mobile* - ormai assolutamente prevalente per le comunicazioni interpersonali, ma in rapida espansione anche sul piano dei servizi e delle transazioni economiche - quali problemi si pongono in termini di privacy e sicurezza?

La crittografia *end-to-end* su cui si basano le principali applicazioni comunicative sul mercato rassicura i privati in termini di riservatezza, ma inevitabilmente solleva grossi problemi in fase d'indagine: non tutto è perduto perché le informazioni restano sugli *endpoint*, ma per avervi accesso serve un intervento diretto sul dispositivo che, quindi, deve essere individuato in via preventiva. Al riguardo uno strumento interessante è rappresentato da Trojan di Stato e software-spia, che leggono le comunicazioni prima dell'invio, aggirando i meccanismi di cifratura. Al riguardo però serve una certa attenzione, perché si garantisce la sicurezza a scapito della privacy degli utenti. Ricordo che una recente sentenza della Corte di Cassazione ha negato l'ammissibilità a fini probatori di un'indagine telematica condotta tramite trojan perché, accedendo al microfono del dispositivo, erano state effettuate intercettazioni ambientali che esulavano dalle autorizzazioni concesse. È un tema complesso. Collaborando con l'Europol posso testimoniare che sul tema sono attivi anche diversi tavoli di lavoro tra autorità investigative nazionali e fornitori di servizi, ma le soluzioni legislative scelte non possono che variare sensibilmente da Paese a Paese (ad esempio la Germania, in seguito agli attacchi subìti negli ultimi anni, ha scelto di adottare norme molto specifiche sull'uso dei Trojan di Stato nelle indagini antiterrorismo).

In che modo inciderà la prossima entrata in vigore del GDPR europeo sul contesto attuale? Ritiene che la figura del *Data Protection Officer* assumerà un ruolo significativo all'interno di aziende e pubbliche amministrazioni, o che all'adeguamento normativo non seguirà un autentico cambio di rotta?

Nell'immediato prevedo un approccio tipicamente italiano, di mero adeguamento alla normativa. Le grandi riforme richiedono tempi di adattamento, ma sul lungo periodo sono piuttosto ottimista: potrebbe essere l'occasione per le aziende italiane di investire finalmente sulla sicurezza informatica, in termini formativi (la formazione è necessaria per *tutti* i dipendenti) e comunicativi. La dimensione internazionale del regolamento, inoltre, significa che il problema di implementarlo ci imporrà di metterci a confronto con Paesi tradizionalmente più rigorosi sul tema della privacy, e questo potrebbe già essere uno stimolo positivo.

Quali considera i trend in crescita del crimine digitale, e quali gli strumenti imprescindibili per contrastarli?

Fra i principali trend contemporanei indubbiamente quelli legati alle criptovalute e alla tecnologia *mobile*. Ma in realtà, se quando ho iniziato a fare questo mestiere ciò con cui avevamo a che fare erano reati informatici "tipici" come il download illegale o le varie ipotesi di accesso

abusivo. Oggi le analisi su dispositivi e dati informatici vengono richieste anche rispetto a crimini che con l’informatica c’entrano poco o nulla. In termini investigativi, a venirci in aiuto nei casi di criminalità comune sono spesso gli errori umani dovuti a un uso scarsamente consapevole della tecnologia; altro è per il crimine specializzato, dove gli autori dispongono solitamente di una maggiore preparazione tecnica. Qui risultano più utili gli strumenti tecnici e la *open source intelligence*, basata su aggregatori di dati non riservati accessibili alle forze dell’ordine (pensiamo per l’Italia agli archivi del PRA, pubblico servizio automobilistico), molto usata ad esempio nel settore dell’antiterrorismo.

A cura della Redazione