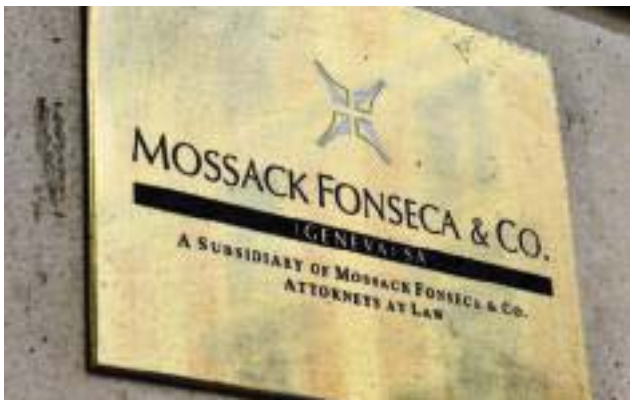
CYBERSECURITY

Studio sotto attacco

Anche gli avvocati si devono guardare le spalle dalle minacce della rete ma hanno l'opportunità di divenire uno dei primi presidi di sicurezza informatica per le aziende

di **Roberto Molica**



UNA RIDUZIONE DI 350 MILIONI DI dollari sul prezzo originariamente contrattato. Questo lo "sconto" di cui **Verizon** beneficerà nell'acquisizione delle attività core di **Yahoo**. Il motivo? Due attacchi informatici subiti dalla società di Sunnyvale che hanno riguardato più di un miliardo di account a cui sono stati sottratti dati sensibili come nomi, indirizzi email, numeri di telefono, password criptate e domande di sicurezza.

Si tratta forse del caso più eclatante in tema di sicurezza informatica ma rende chiari i rischi digitali per le società: nessuno è veramente al sicuro in rete. Neanche gli studi legali. Ne è un esempio l'attacco a **Mossack Fonseca** che ha portato allo scandalo denominato Panama Papers, con più di undici milioni di documenti contenenti informazioni finanziarie su società off-shore rese pubbliche. «Il numero di attacchi informatici che si verificano quotidianamente – afferma Giulio

Coraggio, partner responsabile del sector technology in Italia di **Dla Piper** – dimostra che l'essere vittima di un cyber attacco non è un se, ma un quando, e bisogna essere pronti a livello organizzativo e tecnico per minimizzare gli effetti negativi dell'attacco». Gli studi, soprattutto quelli più strutturati, hanno al loro interno informazioni di primaria importanza. Dati sensibili sul fronte giudiziario e commerciale che, se sottratti, possono essere rivenduti a soggetti terzi e utilizzati per trarne un vantaggio anticoncorrenziale. Non c'è da sorprendersi, dunque, che anche gli studi siano presi di mira da parte di chi fa del cybercrime il suo business, spesso per conto terzi. Si tratta di un trend messo in luce dal Dis, il Dipartimento delle informazioni per la sicurezza, che ha confermato «la progressiva saldatura tra le finalità economiche della cyber criminalità con quelle di comuni player di mercato, interessati a compromettere la competitività dei rispettivi concorrenti».

Se l'avversario si chiama ransomware

Una delle minacce più comuni è costituita dai cosiddetti ransomware, malware che criptano i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. Secondo Stefano Mele, of counsel di **Carnelutti**: «semplificando, si tratta dell'applicazione informatica del sequestro di persona ai dati degli utenti. Gli studi legali, infatti, sono vittime predilette di tali attacchi informatici in quanto soggetti paganti con grandi disponibilità economiche. Nel caso in cui lo studio legale non abbia un semplice backup aggiornato dei dati, cosa peraltro obbligatoria per la normativa in materia di protezione dei dati personali, deve decidere, inoltre, se perdere i dati o pagare il riscatto e rendersi "complice" di un reato. Un problema etico non indifferente». Per evitare di incorrere in tali situazioni, lo studio dovrà allora prevedere dei piani di *business continuity* e *disaster recovery*, processi gestionali che in caso di incidente informatico permettono di continuare l'attività e garantire l'erogazione dei servizi.

Non è solo un problema di interruzione di attività. Sul tavolo ci sono anche i rapporti con i clienti. Il Regolamento europeo sulla protezione dei dati personali di prossima applicazione prevede che, in caso di un'avvenuta violazione dei dati personali, il titolare del trattamento debba darne notifica all'autorità di controllo competente nonché a tutti i soggetti interessati. Per uno studio legale, e in generale per una qualsiasi società, si tratterebbe di un irreparabile danno sia d'immagine sia economico. Uno dei punti dolenti per gli studi professionali potrebbe dunque

Giulio Coraggio
Dla Piper

Stefano Mele
Carnelutti

Giuseppe Vaciago
R&p Legal

«Mappare i rischi è un lavoro di squadra tra consulenti legali e informatici»

essere la regolarizzazione con tale normativa. «Noi avvocati stiamo promuovendo servizi di assistenza per aziende in vista dell'entrata in vigore del Regolamento privacy – spiega Giuseppe Vaciago, partner di **R&p Legal** – ma per primi, vista la sensibilità dei nostri dati, dovremmo essere in regola da quel punto di vista. I vantaggi? Sarà più semplice capire le problematiche del cliente e, inoltre, sarà possibile raggiungere l'obiettivo di rendere più protetti i propri dati».

A fronte di una costante sofisticazione dei fenomeni di minaccia, non vi è però un'adeguata consapevolezza in merito ai rischi e al potenziamento dei presidi di sicurezza. Un problema culturale che sconta la forte disattenzione da parte degli alti livelli dirigenziali all'interno delle società. «Si tratta di temi di cui gli ingegneri informatici sono ben consci – dice Stefano Mele – ma che purtroppo non riescono ancora a essere recepiti come fondamentali nei Cda. Non si è capito, infatti, che essere in regola con la normativa non è solo un modo per evitare sanzioni in caso di controlli, ma oggigiorno significa soprattutto proteggere la propria azienda, il proprio business, le informazioni riservate e di valore e, di conseguenza, i posti di lavoro».

Lo stesso studio legale, allora, oltre che potenziale vittima di attacchi, ha l'opportunità di predisporre la propria struttura per diventare una delle armi a disposizione delle società per ridurre il rischio di attacchi e i relativi danni. La strada scelta dagli studi mira verso la prevenzione del rischio. «Veniamo coinvolti in decine di casi al mese per attacchi subiti dalle società – spiega Giuseppe Vaciago – ma l'intervento ex-post è complesso e non è in grado di soddisfare il cliente. L'unica risposta, anche se non si tratta mai di una soluzione assoluta, è data dall'intervento preventivo. Ma bisogna lavorare con gli informatici. Mappare i rischi dell'azienda per cercare di limitare i danni è un lavoro di squadra impensabile senza i consulenti informatici». Prevenire è meglio che curare, specie se in caso di violazione del nuovo regolamento sono previste sanzioni amministrative che arrivano fino al 4% del fatturato mondiale di una società. Al legale spetta dunque il compito di ampliare le proprie conoscenze. «Gli avvocati – spiega Giulio Coraggio – stanno diventando anche consulenti tecnici perché devono identificare le misure di sicurezza più idonee a garantire la conformità con la normativa e minimizzare i rischi di contestazione in caso di cyber attacco e gli effetti negativi dello stesso. Ci capita sempre più spesso di avere "accese" riunioni con i Cto (chief technology officer) o Ciso (chief information security officer) dei nostri clienti per trovare soluzioni che soddisfino le esigenze delle società e che allo stesso tempo non comportino costi eccessivi, non danneggino il business e ci permettano di sostenere davanti alle autorità che il cliente ha compiuto tutto quanto gli era richiesto dalla normativa».

Sono in aumento le società che mettono a disposizione software per la soluzione di questi problemi. Eppure, dal punto di vista del consulente legale, questi strumenti non devono essere considerati una panacea. È di questo avviso Stefano Mele: «Non è possibile mettere in sicurezza un'azienda attraverso strumenti tecnologici automatici né dal punto di vista tecnico/informatico, né tantomeno dal punto di vista della conformità legale. In ambiti così ampi, come sono la cybersecurity e la protezione dei dati personali, vi è bisogno della componente umana. C'è bisogno di veri esperti in grado di valutare i dati trattati e i relativi processi aziendali, e solo dopo le norme che li governano. Ciò, per raggiungere un adeguamento dei dati personali davvero tarato sull'esigenze di quella singola azienda e del suo business. Così come non esistono abiti su misura che vadano bene a tutti e per tutte le stagioni, non esiste e non può esistere un'attività legale che vada bene per ogni cliente, a maggior ragione nel settore della privacy e della protezione dei dati personali. Il nostro è un lavoro sartoriale che parte dalle esigenze del cliente e non dalle norme».