CYBERSECURITY

Sicuri ma non troppo

I recenti attacchi informatici e l'entrata in vigore del regolamento europeo sulla protezione dei dati alzano l'attenzione sulla cybersecurity degli studi. La risposta anche dalla governance

di **Roberto Molica**

NESSUNO È AL SICURO. COSÌ IN UN articolo di aprile TopLegal Review aveva messo in guardia dal rischio informatico per gli studi: il numero di attacchi informatici che si verifica quotidianamente dimostra che l'essere vittima di un cyber attacco non è un se, ma un quando. Una affermazione che è stata convalidata da un nuovo susseguirsi di attacchi hacker rivolti agli studi. Il 27 giugno è stato il turno dello studio **Dla Piper**, interessato dall'attacco del ransomware NotPetya che, diffusosi a partire dall'Ucraina, richiedeva un riscatto per recuperare l'accesso ai contenuti. E ancora, lo scorso ottobre è stata la volta dello studio di servizi offshore **Appleby**, caduto vittima di un data breach che ha generato lo scandalo Paradise Papers.

La questione culturale

«Nessuno può dirsi completamente al sicuro, le tec-

La sicurezza informatica è prima di tutto un problema di governance

niche di attacco evolvono in continuazione e con loro muta anche la superficie di attacco da presidiare – dice a TopLegal Stefano Buschi, partner e responsabile nazionale per i cyber risk e crisis management services di **Deloitte** – Gli studi legali, soprattutto quelli che non hanno una propria funzione Ict e un provider esterno dedicato, spesso faticano a identificare il perimetro da proteggere e le migliori pratiche per farlo».

Cosa fare per mettersi al riparo? Il primo modo per approcciare il problema è realizzare di essere potenziali vittime. I server degli studi detengono informazioni dal valore inestimabile: non c'è luogo migliore per un hacker nel quale ricercare dati sensibili. Si tratta di un tema ostico da trattare per le insegne: anche se la minaccia informatica è sempre dietro l'angolo, non sono tanti i professionisti realmente consci dell'importanza della questione. Eppure con la prossima entrata in vigore del regolamento europeo sulla protezione dei dati (*vedi l'approfondimento nel box*), al danno si aggiungerà la beffa con una sanzione per gli studi che potrà arrivare fino al 4% del fatturato annuo.

Se la risposta deve passare attraverso adeguati presidi tecnologici è però anche una questione formativa e di governance. Molto spesso le falle derivano da una non adeguata preparazione specifica dei professionisti, siano essi soci o semplici praticanti. «Soprattutto in Italia, dove solo ora si sta diffondendo una maggiore consapevolezza da parte degli utenti "medio-piccoli" sull'importanza della sicurezza informatica – spiega Buschi – spesso anche alcune pratiche basilari vengono sottovalutate, con effetti molto rivelanti. Ad esempio nel caso cui l'uso di dispositivi privati sia permesso in azienda - Bring your own device - (come lo smartphone personale che accede alla rete wireless dello studio), se le pratiche di sicurezza e di configurazione degli accessi alle reti aziendali non fossero correttamente configurate, si potrebbero evidenziare ampie vulnerabilità nel confronti di virus già presenti sui dispositivi "privati" di clienti, fornitori e tirocinanti presenti nello studio e che si potrebbero quindi diffondere su tutti gli apparecchi connessi alla stessa rete». Qui l'esempio recente è il ransomware Wannacry diffusosi a maggio 2017 sfruttando la vulnerabilità di dispositivi non aggiornati.

Data protection, cosa cambia

Il 25 maggio 2018 sarà applicabile il nuovo regolamento Ue in tutti gli Stati membri

L'applicazione riguarda anche le imprese situate fuori dalla Ue che offrono servizi nel territorio dell'Unione

Previste sanzioni fino al 4% del fatturato annuo mondiale dell'esercizio precedente

Lo studio ha 72 ore di tempo per comunicare a tutti i soggetti coinvolti l'eventuale violazione dei dati (*data breach*)

Fonte: Elaborazione a cura di TopLegal Review

A ognuno il suo rischio

Esistono chiaramente molteplici tipi di attacco e ognuno di essi porta con sé diversi tipi di minacce. I danni maggiori per uno studio sono però imputabili alla paralisi di alcune attività per giorni interni con il blocco che spesso interessa, in via precauzionale, i terminali ma anche i servizi di posta e i telefoni. In casi come questo, gli scenari per gli avvocati sono quasi apocalittici. Riportare lo studio alla normalità può comportare un costo immenso in termini di energie e tempo. Non solo. Per una insegna legale una minaccia come il ransomware non è neanche la tipologia di attacco informatico più pericolosa. È semplicemente il più visibile. «Sono molto evidenti gli attacchi di tipo ransomware – precisa Buschi – ma sono più dannosi gli attacchi silenti che passano

Due anni nel mirino
Gli attacchi informatici agli studi nel biennio 2016-2017

Studio target	Caso
Appleby	Lo scorso ottobre 13 milioni di documenti vengono sottratti allo studio di servizi offshore. Il caso ha preso il nome Paradise Papers
Cravath Swaine & Moore e Weil Gotshal & Manges	A marzo del 2016 il Wall Street Journal segnala che degli hacker non identificati avrebbero violato le reti di alcuni studi legali statunitensi
Deloitte	A settembre The Guardian rivela che la società di consulenza è stata oggetto di un attacco informatico
Dla Piper	Lo scorso luglio si trova interessato dall'attacco del ransomware NotPetya, diffusosi a partire dall'Ucraina
Mossack Fonseca	Nell'aprile 2016 scoppia il caso denominato Panama Papers, un data leak di 11 milioni di file sottratti allo studio legale panamense
Vari	Nel febbraio 2016 il Crain's Chicago Business riporta una elenco di 48 insegne Usa e Uk finite sotto la lente del cybercriminale russo Oleras

Fonte: Elaborazione a cura di TopLegal Review

inosservati e che permettono una continua fuoriuscita dei dati verso l'esterno, senza dare evidenza all'utente. In casi come questi le informazioni vengono sottratte continuativamente e possono passare anche diversi mesi prima che l'azienda, o lo studio in questo caso (o più spesso il provider di servizi Ict che ne gestisce rete e strumenti informatici) si accorga di una violazione dei propri sistemi. Si può stimare che molte società, tra cui studi legali, anche in questo momento abbiano in corso attacchi "persistenti" che durano da più mesi, e non se siano ancora accorte».

Il presidio della governance

Se lo studio legale custodisce informazioni relative a operazioni aziendali straordinarie o delicati processi giudiziari, un attacco informatico apre non solo questioni tecniche e di privacy ma anche e soprattutto interrogativi sulle conseguenze legate allo stesso mandato legale. «Una volta scoperta la vulnerabilità – dichiara Giovanni Casucci, partner di **Dentons** a capo della practice di intellectual property and technology – non si può ignorare l'accaduto e mantenere le strategie decise insieme ai nostri clienti prima dell'attacco, l'operatività va necessariamente adattata. Non vale la pena correre il rischio di mantenere la rotta operativa». Non bisogna pensare, dunque, che si tratti di questioni di competenza dei soli tecnici ed esperti informatici. Si tratta prima di tutto di un problema di governance. Ci si può dotare di tutti gli ultimi ritrovati tecnologici in tema di sicurezza ma il fattore umano resta fondamentale e gli errori di gestione si pagano. È necessario che la questione sia portata all'attenzione del management dello studio tenendo bene a mente che i danni derivanti da un attacco comportano costi molto maggiori rispetto a quelli dell'implementazione di sistemi di sicurezza.

Sono di questo avviso i professionisti di **BonelliErede** che, per affrontare il tema, hanno costituito un comitato It composto dai vertici dello studio: il managing partner Marcello Giustiniani (che ne è anche il coordinatore), quattro soci, il direttore generale e il direttore It che ha la funzione di elaborare e proporre al consiglio le strategie tecno-

I danni derivano spesso da una non adeguata preparazione dei professionisti

La sicurezza dello studio in quattro mosse

Analisi

Il primo passo è fare una valutazione della propria rete e dei sistemi di sicurezza appropriati alle esigenze dello studio. Rientrano in questo campo l'identificazione degli utenti, la gestione degli accessi, la crittografia dei dati, il controllo e la gestione delle terze parti

Governance

La sicurezza informatica deve essere presa in carico dai vertici dello studio, prevedendo comitati dedicati, policy di comportamento dei professionisti e sanzioni in caso di violazione delle stesse. La diffusione di una cultura della sicurezza è fondamentale per ridurre il rischio informatico

Monitoraggio

L'infrastruttura It deve essere costantemente monitorata e le anomalie vanno identificate e segnalate in tempo. Spesso la fuga dei dati avviene in maniera silente, senza che lo studio ne abbia contezza

Gestione dell'emergenza

Si deve disporre di piani e meccanismi per riportare la struttura alla normale attività nel tempo più breve possibile, prevedendo back up e piani di disaster recovery. Occorre mettere i professionisti di fronte a casi concreti per sapere come reagire a eventuali attacchi

Fonte: Elaborazione a cura di TopLegal Review

logiche dello studio. Oltre a questo gruppo di lavoro, lo studio si è dotato di un comitato compliance con la funzione di guidare e verificare il rispetto degli obblighi di legge applicabili allo studio nonché il compito di verificare la conformità normativa delle decisioni prese dal primo gruppo. Un doppio controllo che ha l'obiettivo di tutelare lo studio, nonché i suoi clienti, su tutti i fronti. I comitati sarebbero però di poco aiuto in assenza di strutture all'avanguardia: «Tutte le nostre sedi sono uniformate sia sulle policy operative ma soprattutto sui sistemi informatici – spiega il partner Tommaso Faelli – Disponiamo di una nostra rete di comunicazione criptata con connessioni ridondate per garantirci ampia disponibilità dei servizi. Abbiamo in essere un piano di disaster recovery e approvato un nuovo sistema di business continuity che ci permettono di rispondere in tempo reale alle emergenze». Precauzioni che vanno oltre la sicurezza informatica e che si sono rivelate utili anche in situazioni differenti, come i casi di calamità naturale: durante l'alluvione di Genova del 2014, che ha causato l'interruzione delle linee di telecomunicazione, la sede locale dello studio è riuscita a garantire la continuità dell'operatività delle proprie reti.

Soprattutto i grandi studi si stanno infatti sempre più attrezzando con policy e requisiti minimi di sicurezza che vengono a cascata imposti a tutte le sedi, le quali a loro volta possono, in autonomia, prevedere ulteriori precauzioni. Come spiega Francesca Gaudino di **Baker McKenzie**: «Le regole vengono stabilite a livello globale per tutte le sedi appartenenti al nostro network e vengono poi calate nelle realtà dei diversi Paesi. In Europa abbiamo necessità e obblighi diversi dagli Usa. Per una maggiore trasparenza e tracciabilità dei dati abbiamo ripensato la stessa organizzazione dei nostri server». Certo, la maggiore sicurezza potrebbe tradursi in alcuni casi in un appesantimento dell'operatività dello studio «Un sistema sicuro è lento e noioso – afferma Gaudino – Maggiori i muri di sicurezza innalzati, maggiori i tempi di gestione dei dati. E un semplice accesso può richiedere minuti e non secondi. È evidente a tutti

Il fattore Gdpr

UNA SPINTA DECISIVA PER L'IMPLEMENtazione di strumenti adeguati per la tutela da eventuali attacchi informatici proviene dall'ormai imminente entrata in vigore del General Data Protection Regulation (Gdpr), il nuovo regolamento europeo sulla protezione dei dati personali che mira ad adeguare la data protection di tutti i Paesi membri dell'Unione alla corrente evoluzione tecnologica. Entro maggio 2018 le società e, con loro, gli studi legali dovranno adeguarsi alla nuova normativa che impone criteri più restrittivi per il trattamento dei dati e che alza ulteriormente l'asticella degli standard minimi di sicurezza. La partner di **Baker McKenzie**, Francesca Gaudino, si concentra sul cambio di paradigma proposto dalla Gdpr che richiede un approccio preventivo ai problemi relativi alla sicurezza dei dati: «La Gdpr è un vero e proprio tsunami, che impone nuove regole, nuove procedure e nuove sanzioni. Il nuovo impianto normativo richiede più ragionamento rispetto a prima. Si tratta di un modo diverso di fare compliance. Più ragionato ma anche più sfidante». La transizione potrebbe essere più delicata per i grandi network internazionali in quanto il regolamento si applica anche alle imprese situate fuori dalla UE che offrono servizi a persone situate nel territorio dell'Unione. Più moderata l'opinione di Tommaso Faelli, partner di **BonelliErede** «Tutti gli studi più attenti stanno già lavorando in questo senso. Quasi nessuno ha già completato l'intero processo. Ma se si è conformi alla legge attuale, il passaggio al Gdpr non ha un impatto eccessivo». Non bisogna comunque dimenticare che le sanzioni previste in caso di violazioni posso arrivare fino al 4% del fatturato mondiale di una società. Al proposito Giovanni Casucci, partner di **Dentons**, sottolinea: «È vero che studi come il nostro hanno fatturati significativi. La sanzione del 4% non è ovviamente da trascurare ma non è la nostra principale preoccupazione. In caso di data breach, a prescindere dalle sanzioni, quello che conta è il tema della credibilità». Lo studio, entro 72 ore dall'evento di violazione dei dati personali, ha infatti l'obbligo di comunicazione all'Autorità Nazionale per la Protezione dei Dati Personali e a tutti i soggetti coinvolti. I suoi clienti.

che accedere liberamente alle banche dati con uno smartphone agevola e semplifica il lavoro, ma se questo espone maggiormente ad attacchi, allora il gioco non vale la candela».

Per gli studi si tratta quindi di riuscire nella non facile impresa di trovare il giusto equilibrio tra sicurezza del dato e operatività dei professionisti. Se Baker McKenzie chiede ai clienti di usare le sue piattaforme, Dentons per limitare gli accessi informatici e ridurre i rischi ha allo studio l'implementazione a livello internazionale di un approccio di *pessimistic security* il quale prevede l'autorizzazione di accesso ai dati laddove strettamente necessario.

Se gli studi cercano le soluzioni migliori per arginare le minacce, i clienti si stanno mostrando reattivi nell'adeguarsi a richieste legate alla sicurezza informatica. Le società infatti hanno già ben compreso il valore aggiunto di un solido presidio e soprattutto i gruppi di maggiori dimensioni già da anni operano controlli sui propri fornitori di servizi, tra cui anche gli studi legali. «Le grandi aziende scelgono i propri advisor anche in base alla loro sicurezza informatica – conferma Casucci di Dentons – Spesso la short list degli studi partecipanti a un pitch viene stilata in base alla loro affidabilità in termini di cybersecurity, la quale viene valutata prima della stessa fee». Una tendenza per ora principalmente anglosassone che qui in Italia non sembra essersi ancora imposta. Eppure, l'aumento del numero degli attacchi e la crescente spesa delle società in ambito sicurezza, dovrebbe far pensare che nel prossimo futuro la sicurezza informatica per gli studi sarà una discriminante sempre più importante anche per la stessa competitività dell'offerta legale.