ItaliaOggi
www.italiaoggi.it
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO


La guerra al *cyber-crime* passa attraverso legali specializzati

Negli studi costituiti gruppi di esperti nella prevenzione e nella negoziazione con gli hacker

La guerra al *cyber-crime* passa attraverso legali specializzati

PAGINE A CURA DI ANTONIO RANALLI

Crescono i cyber-attacchi ad aziende e Pa e milioni di dati sensibili sono sempre più a rischio. Secondo il «*Threat Intelligence Report*» elaborato dall'Osservatorio Cybersecurity di Exprivia, che prende in considerazione 137 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media, tra luglio e settembre scorsi gli «incidenti in rete» a scapito di aziende, organizzazioni e persone sono raddoppiati. Secondo il rapporto stilato dal gruppo Ict, solo nei mesi estivi si sono registrati 602 casi tra attacchi, incidenti e violazioni della privacy, in calo del 10% rispetto al periodo precedente (672 fenomeni). Secondo il direttore Cybersecurity di Exprivia, **Domenico Raguseo** «questo dato è particolarmente preoccupante, soprattutto ai danni dei consumatori». Il settore maggiormente preso di mira dagli attaccanti è quello «Finance» (aziende finanziarie, istituti bancari o piattaforme di criptovalute), con oltre il 45% dei casi totali (280 su 602), seguito dal comparto «Software/Hardware» con 110 attacchi, e, infine, il settore «Pubblica amministrazione», che tra aprile e giugno ha segnato 84 casi. Mantiene il primato tra le principali tipologie di danni causati dagli hacker il furto dei dati con il 54% dei fenomeni totali (326), in leggera flessione rispetto al trimestre precedente.

L'attenzione delle istituzioni europee è alta sul fenomeno: è stato appena pubblicato il Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (si veda *ItaliaOggi* dell'11 gennaio 2024).

«La cybersecurity è un tema sempre più sentito sia dalle aziende che dai singoli individui», spiega l'avvocato **Stefano Tedeschi**, componente dell'ufficio di coordinamento dell'Organismo Congressuale Forense, che su questo tema ha dedicato un convegno che si è tenuto al Senato. «Gli hacker diventano più ingegnosi ogni giorno che passa, ed è sempre più difficile riuscire a intercettarli e riparare i danni.

Per questo motivo, per esempio, alcuni studi legali, principalmente americani, stanno indirizzando la loro specializzazione, attraverso professionisti legali dedicati alla cybersecurity, proprio al fine di ridurre il rischio di attacchi informatici, che progettano un insieme tecnologie, processi e misure di protezione. Si sta quindi formando sempre più nelle aziende, la figura del *Cyber Security Analyst,* professionista che risponde a due esigenze fondamentali delle aziende: prevenire e, quando necessario, individuare le minacce che potrebbero compromettere una infrastruttura ed i dati gestiti attraverso di essa. Nella società digitale nella quale viviamo, l'impianto normativo nazionale ed europeo in materia di cybersecurity è ancora in costruzione e nuove disposizioni progressivamente si stratificano sulle precedenti contribuendo a realizzare e consolidare una complessiva architettura di sistema. Come noto, infatti, la trasformazione digitale è oggi un terreno fertile nel quale possono fiorire opportunità di sviluppo e occasioni di crescita ma la tecnologia può dar vita a nuovi cambiamenti e rivoluzionare la vita umana solo se viene assicurata la sicurezza delle reti e dei sistemi informatici su cui essa si basa. Del resto, l'applicazione degli istituti giuridici tradizionali potrebbe rivelarsi inadeguata rispetto alle richieste di sicurezza digitale, che, al di là della specificità della materia, si estendono non solo nella direzione della prevenzione dei cyber attacchi ma anche in quella successiva di intervento.

Per garantire la sicurezza digitale e assicurare il corretto funzionamento e l'efficienza delle infrastrutture sono quindi necessari dei professionisti specializzati principalmente in ambito legale, che non si limitano più a fornire solo una consulenza di base, ma, capaci di interpretare le disposizioni e i principi della *cybersecurity law,* sono coinvolti anche nelle strategie di mitigazione e difesa contro le minacce, sempre più frequenti, alla sicurezza aziendale. Si tratta, infatti, di un'assistenza legale fornita da professionisti che siano in grado di comprendere ed affrontare le problematiche connesse ai sistemi tecnologici anche da un punto di vista tecnico. Coniugando la conoscenza del

ItaliaOggi
www.italiaoggi.it
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO


La guerra al *cyber-crime* passa attraverso legali specializzati

diritto con quella più specifica in campo tecnologico, in ambito societario, in particolare, la figura più tradizionale dell'avvocato potrà essere arricchita da una componente specialistica più articolata, incidendo sulle caratteristiche base della professione forense per orientarla al soddisfacimento di esigenze digitali di grande attualità».

Molte aziende hanno trovato «modi creativi» assumendo «hacker etici» e altri candidati non tradizionali per i loro ruoli tecnologici di nicchia «L'hacking etico, noto anche come test di penetrazione o audit di sicurezza», spiega **Antonio Bana**, partner di **Bana Avvocati Associati**, «è il processo di test delle vulnerabilità dei sistemi informatici e delle reti di un'organizzazione. Questi test vengono eseguiti con il permesso dell'organizzazione sottoposta al test e con l'obiettivo di individuare e risolvere i problemi di sicurezza prima che possano essere sfruttati da hacker malintenzionati.

Ma vi è di più! La maggior parte degli studi legali oltre oceano si occupa di violazioni dei dati dopo il fatto avvenuto, perché molti studi legali non sono aggiornati sulla sicurezza informatica. Molti si preoccuperanno solo della sicurezza informatica fino a quando non sarà troppo tardi e il loro sistema non sarà stato violato. Una perdita di dati lascia lo studio legale esposto a una perdita di fiducia da parte di clienti e membri del personale; inoltre, i dati riservati detenuti dagli studi legali possono portare a furti di identità, frodi e altri rischi. Ecco allora all'orizzonte la figura degli hacker etici che trascorrono la giornata a sondare il sistema del tuo studio legale per le vulnerabilità, testando vari modi per entrare e ideare metodi per fermare e bloccare i tentativi in arrivo per violare il sistema.

Ci vuole un hacker etico per conoscere e identificare un altro hacker? Quando viene violato, uno studio legale di solito si chiamano esperti di sicurezza informatica per identificare da dove ha avuto origine la violazione, possibilmente scoprire chi ha sferrato l'attacco, cosa è stato rubato e/o distrutto o riscattato e installa modi per prevenire un altro attacco. Ci sono almeno 5 elementi di utilità: risparmio sui costi generali; risparmio sui costi legati alla violazione dei dati; la *gamification* migliora la produttività; maggiore sicurezza della rete; accesso a esperti di sicurezza informatica. È tempo che gli studi legali si impegnino nella costruzione e nell'aggiornamento della loro sicurezza dei dati. E una soluzione innovativa sta impiegando hacker etici per prevenire gli attacchi alla sicurezza informatica. Gli studi legali negli Usa sembrano aver intrapreso oramai da tempo questa strada, loro che sono così rigorosi sul valore etico hanno creato nuove figure contro i mercenari della Cyberspace rendendo tutto apparentemente trasparente! Sarà la giusta scelta .... etica?».

Per **Lorenzo Battarino**, counsel dello studio **Trevisan & Cuonzo** «con l'aumento esponenziale delle minacce informatiche negli ultimi anni, le aziende sono costantemente esposte al rischio di attacco da parte di criminali informatici. E quando un attacco va a segno, spesso si è disposti a tutto pur di ripristinare al più presto i propri dati e l'operatività aziendale, compreso cedere alle richieste dei criminali e pagare quanto richiesto. È nata così la figura professionale del negoziatore di ransomware, specializzata nel gestire i contatti con i cybercriminali e concludere una trattativa per «liberare» i dati aziendali.

Tuttavia, è sempre consigliabile non negoziare con i responsabili degli attacchi informatici: contrariamente a quanto accade in qualunque trattativa commerciale, infatti, l'azienda e i propri negoziatori non potranno certo fare affidamento sui principi di buona fede e di legalità che sono alla base di qualunque normale transazione. Il rischio, dunque, di ritrovarsi ad aver pagato il riscatto richiesto senza riottenere accesso ai propri dati, o ad essere nuovamente colpiti da un successivo attacco informatico da parte degli stessi criminali, è molto alto.

Le imprese dovrebbero invece agire soprattutto in via preventiva adottando una serie di stringenti misure, tra cui ad esempio: 1) formazione e consapevolezza interna, 2) adozione di dettagliate politiche sulla sicurezza delle informazioni, 3) monitoraggio continuo dei sistemi, adozione di antivirus e firewall, 4) backup completi e regolari, 5) assicurazione contro il rischio cyber. Solo così è possibile evitare attacchi che possono risultare devastanti per l'operatività o la reputazione aziendale, e proteggere il know-how aziendale, che può comprendere dati riservati, segreti commerciali, strategie di business, progetti di ricerca e sviluppo, nonché informazioni finanziarie e legali».

La Casa Bianca sta valutando la possibilità di vietare giuridicamente il pagamento di riscatti nel tentativo di combatterli. «Si tratta di un'inversione di rotta rispetto alla precedente posizione che prevedeva soltanto di incoraggiare fortemente le organizzazioni a non pagare i riscatti, ma non a vietarli del tutto», spiegano **Giorgio Martellino**, presidente di Aitra (Ass. Italiana Trasparenza e Anticorruzione) e **Gaetano Dambra**, Corporate legal counsel di Avio Spa, «La Casa Bianca è ancora nella fase iniziale di prendere in considerazione un divieto sul pagamento del riscatto e non è chiaro quando o se tale politica verrà implementata... E se questo «vento» arrivasse anche in Europa?

In Europa, la legalità del pagamento di un riscatto per un *ransomware* è più complessa. Alcuni paesi, come Francia e Germania, hanno esplicitamen-

ItaliaOggi
www.italiaoggi.it
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO


La guerra al *cyber-crime* passa attraverso legali specializzati

te vietato il pagamento di riscatti. Altri paesi, come il Regno Unito e i Paesi Bassi, non hanno esplicitamente vietato il pagamento del riscatto, ma hanno pubblicato linee guida che sconsigliano tale pagamento. In Italia non esiste una legge specifica che vieti il pagamento dei riscatti dei ransomware.

Tuttavia, la legge italiana vieta il pagamento di riscatti a organizzazioni terroristiche. Inoltre, il Garante italiano per la protezione dei dati personali ha avvertito che il pagamento di un riscatto potrebbe violare il Regolamento generale sulla protezione dei dati – Gdpr. Le organizzazioni hanno bisogno di modi più sofisticati per comprendere la propria sicurezza e per rispondere quando fallisce, non basterà una norma a risolvere tutto. I consigli di amministrazione e gli amministratori delegati devono disporre di processi più chiari che li aiutino a dare priorità alle spese per la sicurezza (su larga scala e in tempo reale) e a gestire prontamente gli incidenti. Ecco, quindi, come le aziende potrebbero prepararsi: dotarsi di una procedura Ransomware che, garantendo il presidio dell'area attraverso specifiche fasi, *Identify, Protect, Detect, Respond e Notification*, preveda un processo chiaro di gestione degli incidenti, con identificazione di ruoli e compiti, e sia allineata ad un business continuity plan; verificare regolarmente i processi interni e la formazione sulla sicurezza dei dipendenti per individuare le lacune nella preparazione informatica».

Secondo **Luca Tufarelli**, founding partner di **Restuccia Tufarelli & Partners** «nel corso di un attacco informatico ransomware o, comunque volto a rendere inservibile un sistema, tutto avviene repentinamente. La situazione è quella del pugile a terra: poca lucidità e solo voglia di rialzarsi prima del *knock out* finale. Spesso manca la lucidità e c'è lo sconforto di qualcosa che non t'aspetti mentre occorre freddezza, lucidità ed attivare subito i rimedi di allerta e di polizia giudiziaria. Non credo sia corretto trattare direttamente con gli hacker, come fu riscontrato al tempo dei rapimenti delle persone. Vanno contattate subito le Autorità nazionali (ACN) tramite il Csirt per segnalare l'incidente a maggior ragione e obbligatoriamente se si è ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica. Inoltre, il mio consiglio è di presentare sempre una denuncia alle strutture di polizia a ciò deputate (Cnaipic). L'obbligo di segnalazione al Csirt sarebbe a mio avviso sempre consigliabile attesa la criticità di sistemi oramai comunque interconnessi anche se non appartenenti al Psnc. Il rischio di creare problemi a un «servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato» è sempre possibile. Se le trattative devono esserci queste vanno condotte nell'ambito di una operazione di polizia giudiziaria o di intelligence. Quello che consiglio è peraltro il comportamento adottato negli Stati Uniti per il noto caso della Colonia Pipeline del maggio 2021 dove la collaborazione del privato con la Fbi ha consentito di recuperare parte del riscatto e di arrestare alcuni hacker autori del misfatto. L'idea di uno studio legale che tratta o addirittura stipula un accordo mi sembra del tutto fuori luogo».

È fondamentale che gli operatori del settore sviluppino ogni tipo di competenza per far fronte alle opportunità ed ai rischi delle nuove tecnologie ed investano in modo concreto su come programmare i servizi legali nel medio lungo termine. «I professionisti che si occupano di questa materia devono conoscere non solo le regole di diritto ma anche di funzionamento delle nuove tecnologie», dice **Giovanna Boschetti**, counsel dello studio legale e tributario **CBA** «L'offerta, da parte di uno studio legale, di un servizio di negoziato con i criminali digitali ha una portata fortemente innovativa, anche in termini di comunicazione. Si parla di uno Studio che non limita più la sua offerta ai tradizionali accordi commerciali, o che offre la prestazione di professionisti consolidati in diversi settori del diritto commerciale e del diritto dell'informatica con specifiche competenze. Si parla di uno Studio che offre la presenza di una squadra multidisciplinare in grado di mettere al servizio del cliente conoscenze anche nei settori della data protection e della cybersecurity e conoscenze tecniche organizzate e formate nel settore hi-tech, nell'applicazione del diritto delle nuove tecnologie e nella conoscenza dei nuovi sistemi. Ciò significa anche aver investito sul capitale umano per sviluppare, unitamente alle tradizionali competenze legali, quel valore aggiunto, riconosciuto dal mercato, delle soft skills, in un'ottica nuova, che l'interlocuzione con criminali richiede. Penso che, in fondo, questo sia l'aspetto di maggior trasformazione che l'avvento delle nuove tecnologie comporta sulla nostra professione: sviluppare nuove competenze in relazione a nuovi strumenti e cambiare il punto di vista per ridisegnare l'offerta dei servizi legali».

Rispetto agli anni precedenti, oggi si assiste a una diversificazione delle strategie di attacco verso le aziende, capaci di causare incidenti e violazioni di dati personali senza precedenti. «Le tecniche sono diversificate e le aziende si trovano nella necessità di ponderare non solo i rischi connessi alla perdita di riservatezza, integrità o disponibilità dei dati, ma anche l'impatto della violazione sulla continuità stessa dell'attività imprenditoriale», dice **Ivan Rotunno**, practice leader Cybersecurity & data protection di **Orrick Italia.** «Sempre più di frequente, a seguito di un attacco,

www.italiaoggi.it
ItaliaOggi
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO


La guerra al *cyber-crime* passa attraverso legali specializzati

il threat actor cerca di interagire con la vittima della sua condotta nel tentativo di ottenere il denaro per la restituzione delle informazioni esfiltrate o per non diffonderle. La gestione di questo tipo di richieste è sempre complessa e richiede la valutazione, da un lato, delle tipologie di informazioni coinvolte nell'incidente informatico e, dall'altro, del rischio conseguente a dare seguito alle eventuali richieste di pagamento.

Dal punto di vista delle responsabilità previste dal nostro ordinamento, il solo fatto di essersi relazionati con l'attaccante non implica una violazione normativa e non deve intendersi come forma di cooperazione o partecipazione ad attività criminose, né può rischiare di esporre l'impresa a illeciti sia di natura civile che penale. Negoziazione con gli hacker potrebbe apparire comunque come un compromesso dei valori legali fondamentali e una sfida all'integrità e, per questo motivo, appoggiarsi a uno studio legale può essere un supporto utile non solo nel momento «patologico» di gestione dell'incidente informatico e della trattativa con gli attaccanti, ma anche nella fase precedente orientata a prevenire questi eventi».

Per **Pietro Montella**, founding partner di **Montella Law**, «è importante evidenziare che questa pratica non è priva di rischi e complessità, e il suo successo dipende da vari fattori, tra cui la natura dell'attacco, la reputazione dell'hacker e il contesto legale in cui si opera. La negoziazione con criminali digitali è un terreno minato dal punto di vista etico e legale, e può sollevare preoccupazioni riguardo alla legittimità e alla conformità alle leggi vigenti. Nel contesto italiano, la prospettiva dei legali dovrebbe considerare innanzitutto il quadro normativo e giuridico locale. L'Unione europea ha leggi e regolamenti specifici che regolamentano la cybersecurity, la protezione dei dati personali e la gestione degli incidenti informatici. Pertanto, qualsiasi iniziativa di negoziazione con hacker dovrebbe rispettare scrupolosamente tali normative, altrimenti potrebbe comportare conseguenze legali per le aziende coinvolte. Tuttavia, ritengo che l'attenzione principale debba essere rivolta alla prevenzione. Investire in formazione per sensibilizzare il personale sull'importanza della sicurezza informatica e nell'implementazione di misure di sicurezza logiche per proteggere i sistemi e i dati aziendali è fondamentale. La resilienza informatica, intesa come la capacità di un'azienda di resistere agli attacchi e riprendersi rapidamente in caso di violazione, è un obiettivo da perseguire. La creazione di piani di *business continuity* e *disaster recovery* solidi è una parte integrante di questo processo, consentendo alle aziende di affrontare gli imprevisti e le minacce cibernetiche in modo efficace. In sintesi, mentre la negoziazione con gli hacker potrebbe essere un'opzione in determinate situazioni, non dovrebbe sostituire gli sforzi mirati a prevenire gli attacchi cibernetici».

Secondo **Maurizio Bortolotto**, socio fondatore dello **Studio Gebbia Bortolotto Penalisti Associati** «occorre lavorare anzitutto sulla prevenzione: dalla formazione dei dipendenti alle procedure di backup e di ripristino, sino all'adozione di procedure volte a pianificare la reazione al cyberattacco. Crediamo molto nella necessità di formalizzare procedure per la risposta a questi incidenti al fine di gestire aspetti IT e soprattutto i passaggi decisionali ed informativi all'interno della società: il coinvolgimento dell'amministratore delegato, la definizione dei ruoli delle strutture aziendali, anche in ragione della delicatezza di alcuni dati a rischio di esfiltrazione, e la tempestiva informativa agli Organi di controllo al fine di una regolare contabilizzazione nell'eventualità in cui l'Organizzazione aggredita intenda pagare il riscatto. Al proposito non va dimenticato che l'Agenzia delle Entrate, nella risposta all'interpello n. 149 del 24.01.2023, ha affrontato espressamente il profilo della deducibilità o meno del riscatto eventualmente pagato dalle aziende a seguito di cyberattacchi e che proprio le modalità in cui si contabilizza il pagamento del riscatto possono porgere il fianco a contestazioni per «falso in bilancio» ovvero nell'ambito della materia fiscale, tributaria e AML. La procedura dovrebbe poi considerare gli adempimenti normativi (anzitutto il data breach) e le azioni che la società può intraprendere a sua tutela con l'Autorità giudiziaria».

www.italiaoggi.it
ItaliaOggi
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO


La guerra al *cyber-crime* passa attraverso legali specializzati


Domenico Raguseo


Stefano Tedeschi


Antonio Bana


Lorenzo Battarino


Giorgio Martellino


Gaetano Dambra

I cyber-attacchi ransomware possono essere prevenuti


Luca Tufarelli


Giovanna Boschetti


Ivan Rotunno


Pietro Montella


Maurizio Bortolotto