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

L'Italia è tra i primi 5 paesi del mondo con il maggior numero di aggressioni sulla rete

Cybersecurity, uno scudo contro gli attacchi alle imprese

Pagine a cura
di Alberto Grifone

La difesa degli asset informatici delle imprese e delle società che erogano servizi fondamentali (come nella sanità) è un problema di crescente rilevanza per il Paese. Secondo l'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, a fronte di una crescita delle minacce (1053 incidenti gravi nel primo semestre del 2021, +15% rispetto al primo semestre 2020, dati Clusit), il 31% delle grandi imprese italiane rileva un ulteriore aumento degli attacchi informatici. Effetti riconducibili anche qui sia al nuovo modo di operare da remoto, causa Covid e, più di recente, alla guerra in corso in Ucraina.

Nei giorni scorsi il governo ha presentato il Governo Draghi la prima strategia 2022-2026 per la difesa del Paese contro gli attacchi di criminali e potenze straniere su internet, assegnando risorse pari all'1,2 per cento degli investimenti lordi del Paese, con possibili sgravi fiscali per le aziende che investono in cyber security. Gli studi legali vengono sempre più spesso coinvolti e consultati dalle aziende per sviluppare servizi e consulenze preventive.

«L'assistenza nella gestione di cyberattacchi richiede un team multidisciplinare. A tal fine abbiamo creato in Italia e a livello internazionale una gruppo dedicato alla cybersecurity con competenze in materia di privacy, Innovation Technology, litigation, assicurativo e penale per poter fornire al cliente un'assistenza a tutto tondo sia rispetto alla compliance cyber che rispetto alla risposte ad eventuali situazioni di attacco informatico», spiega **Giulia Zappaterra**, senior lawyer nel dipartimento Intellectual property & technology di **Dla Piper**. «L'incarico più rilevante degli ultimi 6 mesi in materia di cybersecurity riguarda l'assistenza ad un cliente in un cyberattacco di tipo *ransomware* che ha impattato oltre 40 giurisdizioni con la conseguente necessità di procedere alle relative notifiche alle diverse autorità locali e comunicazioni agli interessati, alla gestione delle indagini interne, dei rapporti con i *threat actor* e richieste delle autorità. Con il network di Dla Piper e delle nostre best friend law firm siamo stati in grado di gestire la questione in modo efficiente fornendo assistenza in tempo reale al cliente in un momento di grande difficoltà operativa». Guardando ai prossimi mesi «prevediamo una forte crescita nella compliance cyber. Su questo infatti l'attività sta aumentando esponenzialmente rispetto agli scorsi anni, in quanto le imprese stanno prendendo coscienza del fatto che è necessario non solo adottare sistemi idonei a proteggersi da eventuali attacchi ma è altrettanto necessario adottare delle policy interne che tutelino l'azienda dai comportamenti interni (ad esempio anche dei propri dipendenti) e dimostrare di aver fatto quanto necessario attraverso procedure valide e applicabili. Si passa quindi da un contesto di pura sicurezza tecnica a quello di sicurezza anche documentale, volto a dimostrare le proprie buone pratiche e la prontezza nel reagire ai rischi di cybersecurity».

Per **Stefano Mele**, partner esperto in Cybersecurity del dipartimento Proprietà Intellettuale, Tmt e Cybersecurity dello studio legale **Gianni & Origoni,** oltre a quelle legate all'attuazione del reticolato normativo previsto dal Perimetro di sicurezza nazionale cibernetica, «le principali problematiche che stiamo gestendo sono legate al filone del supporto strategico e legale in caso di attacchi cyber di tipo ransomware o di operazioni cibernetiche dirette ad un possibile sabotaggio dei sistemi informatici o allo spionaggio e alla sottrazione di informazioni. Inol-

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile

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

tre, sempre più multinazionali nel settore tecnologico ci chiedono un supporto per valutare se i loro prodotti e servizi siamo o meno in linea con le normative europee e nazionali in materia di cybersecurity. Infine, se guardiamo alle attività un po' più «classiche» degli studi legali, c'è una richiesta sempre maggiore nelle operazioni di M&a di svolgere un'analisi legata anche al rischio cyber e, ovviamente, alla protezione dei dati personali». In ambito nazionale, insieme ai clienti, lo Studio guarda con interesse alle azioni che il governo italiano ha delineato all'interno del Piano nazionale ripresa resilienza (Pnrr) e i pilastri della ormai prossima nuova strategia nazionale in materia di sicurezza cibernetica, che inevitabilmente avranno numerose ricadute normative.

«A livello europeo siamo in attesa della cosiddetta «Direttiva Nis 2» (*Network and Information Security*), così come stiamo già analizzando le ricadute sul mercato dei nostri clienti del «Data Act» e della parte del «Cybersecurity Act» inerente alla creazione della prima certificazione europea sui livelli di cybersecurity dei prodotti, servizi e processi utilizzati all'interno dei confini dell'Ue. I continui e sostanziali interventi del legislatore europeo e nazionale nel settore della cybersecurity, che già oggi si delineano in maniera molto netta all'orizzonte, non potranno che far registrare un segno positivo nella crescita del mercato legale anche in questo 2022. Cosa che, peraltro, avviene in maniera costante dal 2018, ovvero a seguito dell'entrata in vigore della prima «Direttiva Nis». Mercato che, però, almeno a mio avviso, avrà una vera e propria esplosione dal 2023 in poi».

«Il team che si occupa delle problematiche della Cyber security è composto da tre professionisti esperti che forniscono consulenza a 360 gradi. In particolare, si occupano di fornire assistenza legale e tecnica già nella fase prodromica di progettazione ed implementazione degli asset informatici e supportano il cliente anche nell'eventuale e delicato momento conseguente ad un incidente informatico», spiega **Vincenzo Colarocco** responsabile del dipartimento privacy dello **Studio Previti**, fresco di nomina nella Commissione Protezione dati personali del Consiglio Nazionale Forense.

«L'attività di consulenza in ambito cyber, infatti, deve avere cura non solo di risolvere i problemi legati al concretizzarsi di un incidente informatico, ma soprattutto consigliare il cliente affinché svolga le proprie attività di business nel modo più sicuro possibile, adottando tutte le misure tecniche ed organizzative necessarie ed idonee a limitare enormemente il rischio per la sicurezza informatica».

Negli ultimi mesi lo studio ha assistito ad una evoluzione delle tecniche di *phishing* – tecniche informatiche fraudolente che, tramite l'invio di comunicazioni apparentemente affidabili, consentono di rubare informazioni personali delle vittime quali dati di accesso, indirizzi email, numeri della carta di credito. «I criminali informatici hanno sviluppato sistemi più evoluti di sfruttando altri strumenti di comunicazione quali Sms (il c.d. *Smishing*) e chiamate vocali (*Vishing*).

Quest'ultima modalità risulta particolarmente efficace in quanto la comunicazione vocale telefonica porta ad un coinvolgimento maggiore della vittima. Altri vettori recenti e particolarmente efficaci sono i Social Network e le piattaforme di Instant Message (oltre 2 miliardi di utenti attivi al mese) oppure le campagne pubblicitarie targhettizzate. In particolare, a seguito di un attacco di smishing, che aveva portato alla sottrazione di importanti somme di denaro, siamo intervenuti tempestivamente e grazie all'intervento delle forze dell'ordine la banda di hacker è stata arrestata e le somme connesse al reato sono state sequestrate» conclude.

Altro studio molto attivo è **Hogan Lovells**. «I nostri clienti ci coinvolgono sia nella fase patologica, quanto cioè un incidente è avvenuto e devono effettuare valutazioni di rischio e avviare processi di notifica, sia nella fase fisiologica, cioè nella preparazione delle procedure interne di adeguamento alla normativa e di incident response», spiega **Massimilano Masnada**, partner Hogan Lovells. «Abbiamo notato, inoltre, che la cybersecurity sta assumendo un ruolo di grande importanza anche in fase di negoziazione di contratti.

A parte le disposizioni del Gdpr sul data breach, sicuramente uno dei passaggi normativi più attesi è la Nuova direttiva Nis 2, attualmente in discussione, che dovrebbe allargare l'ambito applicativo dell'attuale Nis e apportare delle innovazioni interessanti, soprat-

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile

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

tutto affrontando il tema della sicurezza della supply chain e prevedendo un enforcement più stringente.

«Sempre a livello di Unione Europa, è bene ricordare che è in discussione anche la direttiva sulla *Digital operational resilience for the financial sector*. In ambito nazionale invece, siamo in attesa del completamento del processo che ha portato alla creazione dell'Agenzia Nazionale per la Cybersicurezza e ci aspettiamo un aggiornamento della disciplina in materia di sicurezza e incidenti nel settore delle telecomunicazioni, anche alla luce dell'entrata in vigore del nuovo codice delle comunicazioni elettroniche» aggiunge.

Le aziende sono molto preoccupate di proteggere i sistemi aziendali, dal punto di vista della compliance cui sono tenuti, a vari livelli, come anche per proteggere le loro informazioni riservate e i loro asset. «La clientela può essere adeguatamente preparata dal punto di vista tecnico e informatico, ma spesso non ha in essere adeguate protezioni anche di tipo giuridico, soprattutto contrattuale, per controllare al meglio le procedure interne e per minimizzare i rischi che potrebbero presentarsi attraverso violazioni da parte di dipendenti, collaboratori o fornitori, nei confronti dei quali si è generalmente più esposti.

Per questa ragione è spesso necessario integrare il livello di protezione tecnico con un adeguato sistema di policy interne e di contratti, oltre che con un training costante (tecnico e legale) dello staff del cliente» dice **Simona Lavagnini**, founding partner di **Lgv Avvocati**. «Si tratta di un ambito dinamico che è in continua evoluzione. A nostro modo di vedere un tema che ci pare cruciale è quello toccato dalle normative in materia di protezione dei dati personali, dell'intelligenza artificiale, nonché di servizi digitali in senso ampio.

Fra le iniziative legislative più importanti, da tenere in considerazione anche per i riflessi sulla cybersecurity, ci sono la proposta europea di regolamento sull'intelligenza artificiale e il Digital Service Act. Il settore è in forte crescita, sia per quanto riguarda la consulenza preventiva per fare in modo che i sistemi informatici interni delle aziende siano sufficientemente protetti, sia per quanto riguarda le azioni nel caso di violazione dei sistemi. La consulenza deve essere costante, dinamiche e interdisciplinare, oltre che tenere conto di aspetti di internazionalità (essendo spesso i temi crossborder). Per quanto riguarda invece la litigation, è cruciale partire da una buona base di descrizione tecnica dell'evento, che può derivare da sistemi di rilevazione ove inseriti a monte nelle strutture informatiche, ovvero anche tramite investigazioni ex post, che possono essere attuate attraverso esperti in analisi complessa dei sistemi informatici e del traffico di rete. Importante è anche affiancare le strategie di protezione, combinando a seconda delle esigenze del caso strumenti di difesa civile con strategie di tipo penale» chiosa.

Tavella Studio di Avvocati ha costituito un dipartimento data protection e cyber security coordinato da **Pierluigi Perri** of counsel, professore di Sicurezza informatica, privacy e protezione dei dati sensibili presso l'Univerisità degli Studi di Milano. In più, il team vede due risorse interne che hanno seguito un percorso di formazione specifico nel diritto IT e nella protezione dei dati. «Le principali operazioni che abbiamo seguito riguardavano la gestione di incidenti informatici sui sistemi dei clienti dovuti sia ad attacchi esterni dolosi che avevano compromesso la funzionalità del sistema e la disponibilità dei dati, sia ad azioni colpose svolte da personale interno o comunque da personale che aveva un accesso alle risorse informatiche dell'azienda», spiega Perri.

«È evidente che un attacco informatico genera una situazione di crisi che deve essere gestita, anche nell'ottica della tutela della reputazione dell'impresa. Possiamo distinguere due situazioni: una situazione di crisi e una di preparazione a possibili eventi indesiderati. Nella situazione di crisi, le principali richieste riguardano la corretta gestione della fase post-attacco, che riguarda soprattutto la presentazione di eventuali denunce, le operazioni di controllo del danno e tutela della proprietà intellettuale dell'azienda e dei dati dei clienti, nonché il rafforzamento del sistema sulla base dell'esperienza maturata a seguito dell'attacco. Nella fase di preparazione rispetto a possibili incidenti informatici, ci si concentra sulle operazioni di audit del sistema e di redazione e formazione dei dipendenti

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile

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

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile

sulle policy aziendali. E risaputo che il fattore umano rappresenta spesso l'elemento più debole della cyber security».

«Come da trend generale, la maggior parte delle operazioni seguite dal nostro studio ha riguardato analisi del livello di rischio di data breach legati ad attacchi informatici commessi tramite phishing o utilizzando malware di tipo ransomware cryptolocker», dice **Maria Livia Rizzo** dello **Studio Stefanelli&Stefanelli**. «Un caso particolare ha riguardato l'attacco a un indirizzo e-mail effettuato tramite una modifica delle impostazioni del relativo account, che inoltrava in automatico qualunque risposta alle mail che partivano da quell'indirizzo (contenenti liste operatorie) a un indirizzo mail terzo. Non mancano, ad ogni modo, clienti che in ottica di prevenzione ci chiedono un supporto specifico per individuare le misure di sicurezza, non solo tecniche ma anche organizzative, più idonee a contrastare le minacce IT». Il legislatore è particolarmente consapevole del fatto che, per rendere efficace la digitalizzazione, non è più possibile separare il concetto di tecnologia da quello di cyber security.

«Questo aspetto è reso evidente dall'incremento di norme volte a migliorare gli standard di sicurezza informatica che negli ultimi anni si sono susseguite sia a livello europeo che nazionale. Il prossimo passaggio normativo atteso riguarda le aziende che svolgono un ruolo chiave nella fornitura di servizi essenziali all'interno dell'Unione europea, o che operano in settori critici come quello dell'healthcare, ed è rappresentato dalla Direttiva Nis II, la cui proposta è stata pubblicata il 4 novembre 2021, e che andrà a sostituire la Direttiva Nis 1148/2016, recepita in Italia dal Decreto Nis del 2018. Dato il ruolo di primo piano svolto dal settore digitale nell'economia globale, un focus sulla sicurezza, resilienza e affidabilità dei sistemi Information Technology sarà necessariamente al centro delle strategie aziendali del prossimo futuro. Predisporre modalità di salvaguardia dei sistemi informatici e di protezione dei dati digitali diventerà sempre più importante» conclude.

Weigmann Studio Legale, grazie alla significativa esperienza, per il tramite di un team dedicato composto da **Fabrizio Tarocco**, equity partner e **Alessio Chiabotto**, Associate, offre servizi di consulenza ed assistenza legale tanto alle imprese che abbiano specifiche necessità in materia, quanto ai tecnici/esperti di compliance per coadiuvarli nel loro ruolo. «Registriamo un crescente interesse da parte delle imprese e, conseguentemente, un significativo incremento delle richieste di consulenza, sugli aspetti connessi all'emersione ed applicazione delle più recenti tecnologie al settore della sicurezza informatica, ad esempio valutazioni di compliance, rispetto alla legislazione in materia di protezione dei dati personali e di diritti di proprietà intellettuale, di sistemi di machine learning utilizzati con finalità di threat intelligence, consulenza su sistemi innovativi volti garantire l'integrità dei dati e a consentire la verifica delle identità digitali, consulenza su sistemi di mitigazione dei problemi di sicurezza attraverso sistemi automatizzati di analisi automatizzata del codice e consulenza sui sistemi di prevenzione in ambito aziendale dall'utilizzo da parte di dipendenti e collaboratori di prodotti software o contenuti digitali in violazione dei corrispondenti diritti d'autore di terzi».

«Siamo soliti assistere i nostri clienti nell'ambito dell'intero processo di adeguamento alla normativa privacy. Ci viene spesso richiesto supporto nella revisione e implementazione di misure tecniche e organizzative, nella gestione degli incidenti, nonché assistenza nella predisposizione di valutazioni di impatto per attività di trattamento che richiedono l'uso di nuove tecnologie. Seguiamo inoltre i nostri clienti nella redazione di policy, tra cui la documentazione di eventuali data breach e la predisposizione di linee guida sulla conservazione dei dati e sull'uso di strumenti informatici» spiega **Marta Minonne** di **Orsingher Ortu Avvocati Associati.**

Nell'ambito della strategia per il mercato unico digitale elaborata dalla Commissione Europea, vi è certamente l'entrata in vigore del nuovo Regolamento ePrivacy, che mira ad accrescere la fiducia nei servizi digitali e nella sicurezza degli stessi. «Di particolare interesse è anche la proposta per un Regolamento europeo volto a stabilire regole armonizzate in materia di intelligenza artificiale. Si tratta, infatti, di un settore tecnologico in grande espansione negli ultimi anni che, se da un lato consente di ot-

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

tenere benefici economici e sociali per le aziende, dall'altro porta con sé rischi connessi all'uso di tali tecnologie e possibili impatti negativi per gli individui.

È prevedibile che nel corso dell'anno si verifichi un incremento di incidenti e attacchi informatici con l'uso di nuovi e sempre più insidiosi malware, nonché di sofisticati sistemi di phishing. Essendo ormai confermato il trend che vede un numero crescente di aziende avvicinarsi al mondo dell'online e indirizzare verso tale settore le proprie attività lavorative, ci si aspetta un accrescimento degli investimenti sulle misure tecniche e organizzative volte a prevenire possibili attacchi e incidenti informatici» chiosa.

Studi in soccorso per aiutare le aziende a proteggere i dati

Maria Livia Rizzo

Fabrizio Tarocco

Marta Minonne

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile

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

Giulia Zappaterra

Stefano Mele

Vincenzo Colarocco

Massimilano Masnada

Simona Lavagnini

Pierluigi Perri

Ritaglio Stampa ad uso esclusivo del destinatario, Non riproducibile