COR.COM
IL QUOTIDIANO ON LINE DELL'ECONOMIA DIGITALE E DELL'INNOVAZIONE

Direttore Responsabile: Gildo Campesato
Condirettore: Mila Fiordalisi

L'ANALISI

M&A, il rischio cyber "entra" nella due diligence

Lo studio dei rischi legati alla sicurezza IT è diventato centrale nelle operazioni di acquisizione. Come dimostra il deal Verizon-Yahoo!. L'analisi dell'avvocato Alessandra Tarissi de Jacobis

di Alessandra Tarissi de Jacobis, partner dello studio De Berti Jacchia Franchini Forlani

La sicurezza informatica è ampiamente riconosciuta come una delle maggiori sfide per i governi di tutto il mondo che hanno posto la cyber-security come argomento prioritario all'interno della propria agenda politica; tutto ciò allo scopo di incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici.Tuttavia la cyber security non deve essere più considerata quale esclusivo appannaggio degli enti governativi, né può considerarsi riservata ai soli dipartimenti IT e ai professionisti della sicurezza informatica: è infatti innegabile che il cyber rischio non è un rischio tecnologico, ma un rischio strategico e aziendale da tenere in attenta considerazione anche da un punto di vista legale. Da qui l'esigenza di una cyber intelligence aziendale.Ciò posto, come qualsiasi rischio aziendale, il cyber rischio deve essere gestito in modo appropriato all'interno di un quadro generale di informazioni e di risk management.

Le operazioni di M&A rappresentano alcuni dei moment più importanti e vibranti della nostra economia: esse portano con se esperienze provenienti da una vasta gamma di professioni e contribuiscono a creare valore in molti settori.

Il valore di tali operazioni è rappresentato dal risultato sinergico di molteplici contributi, tra i quali meritano una speciale menzione la partecipazione attiva di vari professionisti del settore nonché numerosi flussi di informazioni e dati: tali sinergie se da un lato contribuiscono a creare un valore aggiunto, dall'altro creano altresì numerose vulnerabilità. che sono sempre più utilizzate da singoli e da gruppi per scopi criminali

Non è infatti difficile osservare come un'ampia condivisione di informazioni, soprattutto in sede di operazioni straordinarie, rappresenta una vera e propria sfida per gli operatori del settore:dati commerciali, informazioni IP e dati sensibili possono tutti essere coinvolti in minacce cyber.

Pertanto, chiunque sia coinvolto in operazioni di M&A deve considerare la sicurezza informatica come una delle maggiori priorità. Infatti, come sopra accennato, i grandi volumi di informazioni condivisi nel processo di completamento di una transazione – inclusi i dati strategici e finanziari - nonché il numero di persone coinvolte in ogni fase di un'operazione straordinaria sono assai più ampi rispetto a quelli nel corso di operazioni ordinarie. Questi fattori aumentano il rischio di attacchi cyber, la possibile compromissione delle reti, sistemi e dati aziendali. Le minacce nelle quali è possibile imbattersi hanno forme diverse e diversi scopi. Per questo motivo, data anche la pericolosità di alcuni dei soggetti che compongono la minaccia, la rete è oggi considerata un vero e proprio campo di battaglia, e come tale va difesa e protetta con strategie di intelligence

aziendale.Ma chi sono le potenziali vittime e i potenziali “nemici” e quale la possibile strategia al fine di evitare che la guerra cyber comprometta un’operazione straordinaria?

Sotto il profilo delle vittime potenziali, un rilievo particolare rivestono le imprese multinazionali, già più volte oggetto di crimini informatici dai quali sono derivati danni ingenti. Tuttavia, anche le imprese di piccole e medie dimensioni, che costituiscono il fulcro del tessuto economico italiano, costituiscono un potenziale bersaglio.Quanto ai nemici, si passa da piccoli criminali, a cyber-criminali professionisti freelance che vendono competenze e strumenti (malware, exploit zero-day,oaccesso abotnet), hacktivisti (guidati da supposti “principi” o scopi politici o morali) a cyber-organizzazioni criminali più sofisticate, spesso a servizio di società concorrenti. Tuttavia è anche necessario non sottovalutare che gli stessi dipendenti, collaboratori o fornitori di una delle aziende coinvolte in un’operazione straordinaria possono rappresentare un potenziale nemico.

Passando all’esame dei rischi e delle possibili strategie, occorre innanzitutto osservare che sebbene il rischio cyber possa a prima vista apparire come un rischio nuovo, le conseguenze di tale rischio sono ben note e consolidate: tra gli altri basta citare i danni all’immagine e alla reputazione, perdita di clienti, danni finanziari, turbativa di operazioni commerciali. Pertanto nessun soggetto operante nel campo di operazioni M&A, ivi inclusi i professionisti e le imprese, possono permettersi di ignorare tali minacce e rischi e devono acquisire consapevolezza con riferimento agli strumenti di protezione dei propri dati, clienti e reputazione nonché ai possibili relativi rimedi.

L'obiettivo di valutare la sicurezza informatica della società target dovrebbe essere introdotto sin dall’inizio di un’operazione straordinaria, già in sede di sottoscrizione di un eventuale lettera o Memorandum di intenti e ciò allo scopo di consentire al potenziale acquirente di essere a conoscenza della possibile esposizione e conseguenti responsabilità e rischi anche dopo la conclusione dell'operazione stessa. In tale scenario, la cyber due diligence sta divenendo sempre più una standard best practice nelle operazioni di M&A.

Come è noto l'obiettivo primario della due diligence è quello di ottenere una comprensione accurata della condizione finanziaria e legal, dei contratti, delle attività e delle passività della società target. **La cyber due diligence è quindi diventata una componente essenziale di tale processo di revisione ed indagine**, laddove avvocati e consulenti specializzati in cybersecurity rivestono un ruolo essenziale con riferimento alla valutazione del cyber-rischio. Tale due diligence dovrebbe comprendere una revisione e un'analisi delle politiche, dei programmi e sistemi informatici e della loro corretta configurazione nonché delle procedure di protezione dei dati, Inoltre essa dovrebbe avere ad oggetto non solo la società target ma anche terze parti, quali fornitori e dipendenti chiave, non dovrebbero essere trascurati.

I recenti noti avvenimenti relativi alla potenziale acquisizione di Yahoo da parte di Verizon e l’incidenza degli attacchi cyber subiti da Yahoo (e mai dichiarati né scoperti in sede di due diligence) sul prezzo finale di acquisto (sembra si tratti di oltre 350 milioni di dollari) ci devono insegnare l’importanza di un’attenta valutazione – legale ed economica - del rischio cyber, sin dalla fase iniziale del processo di acquisizione, non dimenticando peraltro che tale processo non può ritenersi ancora standardizzato ma in continua a evoluzione anche tenendo in considerazione i diversi settori in cui può operare la società target e la peculiarità finanziaria e legale di alcuni settori (si vedano tra gli altri sanità, comunicazioni, appalti pubblici). **Inoltre ad un’attenta due diligence dovrebbe anche seguire un’attenta redazione del contratto di acquisizione che contempli un attenta gestione del rischio**, astratto e concreto che sia, nonché delle conseguenze in termini di indennizzo e risarcimento dei danni nonché di eventuale aggiustamento del prezzo. In tale contesto non è neppure da sottovalutare l’importanza di eventuali polizze assicurative a copertura di tali possibili rischi.

26 Aprile 2017