CYBERSECURITY TRA DUE DILIGENCE E SPA

Il 2023 si apre con un attacco informatico che, seppur causando lievi danni nel bel paese, ha smosso l'attenzione ancora una volta su tali fenomeni[1]. La sicurezza informatica e i rischi di hackeraggio sono diventati le principali preoccupazioni nel mondo digitale di oggi.

Check Point Research (CPR), una sezione di Check Point Software, azienda leader nel fornire soluzioni di sicurezza informatica a livello globale, ha recentemente calcolato che le tendenze degli attacchi informatici a livello globale nel 2022 sono cresciute del 38% rispetto all'anno precedente[2] e incentrati principalmente sui settori *Healthcare* e IT (ciò è in parte dovuto al perseverare della pandemia da Covid-19 e allo scoppio del conflitto Russo-Ucraino). Inoltre, nel medesimo *report,* CPR sottolinea come la corsa all'introduzione nelle aziende di sistemi di intelligenza artificiale (tra i tanti, ChatGPT), potrebbe causare un incremento del numero di attacchi nel 2023.

L'aumento di "cyberattacchi" ai danni delle imprese italiane ed europee è spesso tenuto in scarsa considerazione dagli avvocati e consulenti legali, ma può seriamente compromettere la profittabilità delle società stesse, specie in caso di prospettate operazioni straordinarie quali fusioni o acquisizioni.

A tale ultimo proposito, in termini generali, vale la pena tenere conto di quanto segue: di fatto, una fusione o acquisizione (M&A) può portare una serie di vantaggi, ma allo stesso tempo introdurre anche nuovi rischi per la sicurezza informatica. Le minacce informatiche derivanti da questo tipo di operazioni possono essere classificate in 3 aree principali:

- **Rischio IT**. Durante un processo di acquisizione, ed ancor più in corso di fusione, le risorse IT coinvolte sono spesso sovraccaricate nel tentativo di gestire un'integrazione fluida tra le società interessate dall'operazione fin dalla fase di *due diligence*, il che porta a lunghi periodi di vulnerabilità, lasciando ampio spazio di manovra per eventuali furti di dati.
- **Rischio di integrazione**. La "fusione" di due o più diversi sistemi IT, a seguito del perfezionamento di un'operazione di M&A, può comportare notevoli sfide di integrazione, le quali a loro volta possono esporre la società acquirente a nuovi rischi per la sicurezza. Tali rischi includono, ad esempio, la perdita di dati sensibili durante il processo di integrazione a causa di errori umani o una carenza di compatibilità dei programmi di sicurezza, spesso risultato di una tentata armonizzazione di un complesso mosaico di sistemi che possono contenere punti ciechi ed essere vulnerabili in caso di attacco. Inoltre, la società acquirente (o quella risultante da una fusione) può ereditare sistemi cd. *legacy*, i quali per definizione non sono più supportati o presentano già un certo livello di vulnerabilità, con conseguenti rischi di minacce informatiche e perdite finanziarie significative.

[1] Per un approfondimento A. Martin, I. Fisher, R. Gallagher and T. Ebhardt "Hackers Target Thousands of Computers Days After Ion Attack", febbraio 2023, qui disponibile: https://www.bloomberg.com/news/articles/2023-02-05/cyber-security-hacking-news-italy-says-systems-attacked

[2] Si veda "Check Point Software's 2023 Cyber Security Report", febbraio 2023, qui disponibile: https://pages.checkpoint.com/cyber-security-report-2023.html

- **Rischio "culturale"**. Società diverse possono avere culture di sicurezza informatica diverse e, contemporaneamente, non avere il medesimo livello di consapevolezza dei possibili rischi. Ciò può comportare strategie di sicurezza disallineate e produrre una carente comunicazione tra i *team* IT. Proprio a tal riguardo, la conclusione di un'operazione di M&A, può portare ad una difficile definizione di ruoli di responsabilità, modifiche del modello operativo, barriere linguistiche e cambiamenti di sede.

Per mitigare questi rischi, è importante innanzitutto svolgere una *due diligence* approfondita sulla sicurezza informatica prima di un'operazione di fusione o acquisizione. Ciò dovrebbe includere la preparazione di una *check-list* tecnica, una revisione della posizione di sicurezza della società *target*, una valutazione del rischio dei suoi sistemi e applicazioni e una revisione delle sue politiche e procedure di sicurezza.

Tuttavia, i *team* legali che si occupano di operazioni straordinarie, ad oggi, ancora trascurano l'importanza di uno studio approfondito dei *cyber risk* durante la fase di *due diligence* e tendono a mantenere un approccio meramente documentale senza alcuna analisi tecnica dello *status* dei sistemi informatici e la loro sicurezza.

Un ulteriore strumento utile nel mitigare i rischi di sicurezza informatica consiste nel prevedere, all'interno delle clausole di dichiarazioni e garanzie nei contratti di compravendita (SPA), la conformità ai principali standard dei sistemi informatici della società target e l'assenza di eventi che abbiano intaccato i sistemi stessi. Le dichiarazioni e garanzie sono previsioni legalmente vincolanti mediante le quali il socio/venditore garantisce all'acquirente alcuni aspetti ritenuti rilevanti per l'attività della società *target*. Includendo nelle predette clausole aspetti di sicurezza informatica e la gestione dei *cyber risk* fino al momento del cd. *closing*, l'acquirente è consapevole dei potenziali rischi e riceve un'ulteriore tutela in caso di violazioni.

Ciononostante, l'operazione di acquisizione di Starwood Hotels & Resorts da parte di Marriott International dimostra anche l'imperfezione di tale soluzione, se non strutturata adeguatamente. Infatti, come noto al grande pubblico, due anni dopo la cessione della catena, Marriott scoprì una serie di *data breach* a partire dal 2014, a danno del database delle prenotazioni degli ospiti di Starwood[3], le quali hanno esposto le informazioni personali di 500 milioni di clienti ed è costata a Marriott decine di milioni di dollari di danni, derivati anche dalle sanzioni delle autorità competenti alla vigilanza dei dati personali. A tale proposito, un esempio dell'attività sanzionatoria delle autorità si riscontra con l'introduzione del GDPR con il quale il legislatore europeo ha previsto nuove sanzioni in caso di mancata diligenza e conformità dei sistemi di sicurezza agli standard di riferimento, alle quali si aggiungono i costi di adeguatezza, i danni di immagine ecc.

A conclusione di quanto sopra, la necessità di svolgere una approfondita *Due Diligence* del settore IT, sia da un punto di vista tecnico che legale, e di includere i rischi di sicurezza informatica nelle cd. *representations & warranties*, sta crescendo man mano che l'uso delle nuove tecnologie diventa imprescindibile per le imprese e, seppur il mercato italiano non mostri ancora rilevanti criticità in tale ambito, in un futuro prossimo sarà necessario sviluppare e prevedere tali clausole nella maggior parte degli SPA.

[3]N. Perlroth, A. Tsang and A. Satariano, "Marriott Hacking Exposes Data of Up to 500 Million Guests", novembre 2018, qui disponibile: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html