Cyber Crime: Risk Management e metriche di valutazione degli investimenti in misure di contrasto (E-CRIME PROJECT)

Alessandra Zaccaria

ABSTRACT

Negli anni 70' la comunità internazionale di *hackers* esplorava sistemi operativi e architetture di rete eseguendo i primi *penetration test* per una mera sete di conoscenza. Difatti, l'intrusione dei sistemi informatici rappresentava l'unica possibilità per conoscerli dall'interno, individuare eventuali falle e in definitiva per testarne il grado di inviolabilità. Nel tempo, alla curiosità e alla volontà di scambiarsi gratuitamente conoscenze è subentrata la sete di denaro di individui che, noncuranti dell'*ethical hacking*, hanno intravisto l'opportunità di fare affari, vendendo nel *black market* informazioni dall'alto potenziale economico. Attraverso i mezzi informatici, i criminali hanno cominciato a fare incetta di identità, dati bancari, informazioni cliniche, credenziali di accesso e persino di brevetti industriali o altri dettagli utili a logiche di concorrenza sleale che possono minacciare la sopravvivenza o il valore di mercato dell'azienda stessa.

L'attitudine al rischio dell'azienda varia e, a seconda dei casi, esso può mitigarsi, ignorarsi o trasferirsi ad un ente assicuratore. Se però l'azienda decidesse di mitigare il rischio di subire un attacco cibernetico, la difesa del perimetro aziendale per mezzo solo di soluzioni tecnologiche avanzate e costose potrebbe tradursi in una moderna linea Maginot, nei fatti una difesa aggirabile. Risulta invece opportuno comprendere l'esposizione al rischio dell'azienda e definire un buon livello di sicurezza proporzionato al valore degli asset da proteggere, a partire dalla massimizzazione delle risorse esistenti. Solitamente l'investimento in sicurezza è avvertito come un costo certo a fronte di un ritorno incerto, una sorta di dazio tecnologico. Non si tratta di un investimento finanziario tradizionale che garantisce un ritorno economico, può ritenersi invece una spesa definita che eviterebbe costi molto probabili ed elevati, ma che intanto ha ricadute positive su tutti i vettori di business, in termini di razionalizzazione e ottimizzazione di risorse.

In questo elaborato, seguendo l'impostazione dell'attività di Risk Mangement si descrivono prima le minacce, le vulnerabilità e le conseguenze dei cyber attack, che risultano essenziali nel loro insieme alla comprensione del rischio del cyber crime. In seguito, si intende analizzare le possibili contromisure che un'azienda non appartenente al mondo ICT può adottare per contrastare il rischio

in esame, classificate secondo il Cybersecurity Framework del *National Institute of Standards and Technology*. In riferimento alle contromisure, ispirandosi al contributo al progetto europeo *E–Crime* della fondazione di ricerca Global Cyber Security - Poste Italiane, sono suggerite le metriche di valutazione in base alle quali l'azienda può elaborare un'analisi costi/benefici e allocare al meglio le proprie risorse. In questa maniera, il costo delle misure di sicurezza ritorna utile assieme alla valutazione del cambiamento dell'esposizione al rischio del cyber crime per il calcolo della redditività dell'investimento (ROSI). Alla luce di questi elementi, si descrive uno scenario di attacco cibernetico in cui per ogni fase di sviluppo, sono segnalate delle contromisure che possono risultare adeguate alla mitigazione del suo impatto, classificate secondo le indicazioni del NIST. In ultimo, un ragionamento controfattuale consente di comprendere i criteri di valutazione del ritorno in investimento richiesto per la messa in sicurezza dell'azienda colpita, di natura economica ma non solo. Investire in modo intelligente in cyber security può riservare un ritorno valutabile in termini di affidabilità e competitività, cardini di un'economia sempre più informatizzata.