Autore
*Barbara Klett, LL.M.**

Cybercrime: rischi e la loro gestione

La crescente digitalizzazione e la messa in rete del mondo di oggi porta ad un'intensificazione dei rischi informatici.

La criminalità informatica è uno dei rischi operativi di importanza cruciale per ogni impresa. I criminali informatici individuano il punto più debole di un sistema, che spesso risiede nel fattore umano, per rubare dati sensibili al fine di estorcere denaro, di renderli inutilizzabili o di utilizzarli in modo improprio.
Secondo uno studio svolto nel 2018 da KPMG (KPMG, *Clarity on Cyber Security, driving growth with confidence*, maggio 2018) tra le imprese che hanno subito un attacco informatico è risultato che il 42% ha lamentato una perdita economica (di queste società il 75% è attivo nel settore finanziario), il 33% ha sofferto della divulgazione di informazioni interne riservate e il 25% ha dovuto far fronte a danni di immagine. L'80% degli organi societari ha riconosciuto la criminalità informatica come un rischio operativo, tuttavia solo il 28% delle società beneficiava di una copertura assicurativa contro i rischi informatici.

Un attacco informatico può rapidamente diventare una minaccia per l'esistenza stessa dell'impresa, in particolare per le piccole medie imprese.

Cosa sono e quali sono i rischi legati al Cybercrime?
Non esiste una definizione ufficiale di rischi informatici, essi possono tuttavia essere così descritti: I rischi informatici sono minacce operative che derivano da informazioni contenute in dischi fissi e reti informatiche. In questo modo tutte le informazioni che non sono fisicamente disponibili, ossia tutti i dati disponibili elettronicamente, sono esposte al rischio di attacchi informatici.
I rischi associati alla criminalità informatica variano da settore a settore e devono essere analizzati tenendo conto del profilo di business, dell'orientamento strategico, del posizionamento e della situazione di mercato dell'impresa interessata. Tra i possibili rischi legati alla criminalità informatica si possono elencare:

- attacchi volti a spiare i dati dei clienti o a paralizzare i sistemi, ad esempio installando software maligni (malware, virus);
- manipolazione (cancellazione o modifica) di dati contabili e finanziari, ad esempio falsificazione di ordini di pagamento o altre forme di abuso di sistema per ottenere vantaggi finanziari illeciti;
- furto di dati e conseguente estorsione finanziaria, sotto la minaccia di svantaggi dovuti alla divulgazione di queste informazioni;
- sottrazione di dati e know-how, per replicarli o distruggerli;
- danni di immagine, ad esempio a causa del furto di dati sensibili di clienti e/o dell'impresa;
- avvio di disposizioni patrimoniali mediante frode, appropriazione indebita e altre infrazioni.

L'avverarsi di rischi cyber può paralizzare l'attività di un'impresa e/o creare enormi costi per riprendere l'attività operativa, recuperare i dati persi, risarcire eventuali danni a terzi e/o perseguire i potenziali responsabili. La prevenzione e l'allestimento di un ventaglio di misure da mettere in atto in caso di crisi sono dunque temi da cui può dipendere la sopravvivenza di un'impresa.

La lotta contro la cyber-criminalità
La lotta contro i reati informatici rappresenta una sfida sotto molti aspetti. Lo scambio di informazioni a livello nazionale e internazionale e la cooperazione tra attori privati e statali è dunque essenziale. Il Consiglio federale istituito a inizio 2019, in aggiunta alla esistente centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, un nuovo centro di competenza che fungerà da primo punto di contatto nazionale per la popolazione e il settore economico per le questioni relative ai rischi cyber (www.isb.admin.ch). La fedpol è l'interlocutrice per le segnalazioni di contenuti e comportamenti criminali in rete.
A livello europeo vi sono istituzioni che si occupano di lotta alla criminalità informatica, come la ENISA (European Network and Information Security Agency) o la EUROPOL. Inoltre è in vigore la convenzione del Consiglio d'Europa del 23 novembre 2001 sulla criminalità informatica che rappresenta il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche e che mira a una politica penale comune per la protezione contro la criminalità informatica promuovendo la cooperazione internazionale.

La prevenzione
La prevenzione gioca chiaramente un ruolo di fondamentale importanza nella sfida alla criminalità informatica. Essa richiede una struttura di gestione del rischio composta da più elementi.
In primo luogo è importante riconoscere i rischi all'interno della propria impresa per poter stabilire quali sono i margini di tolleranza del rischio sopportabili, al fine di sviluppare una strategia di gestione del rischio appropriata. Un altro importante fattore da considerare nel mondo globalizzato di oggi al fine di minimizzare i rischi è quello di effettuare un esame professionale approfondito dei partner commerciali (e dei dipendenti) prima della stipulazione di un contratto. Un ulteriore strumento di tutela consiste nel richiedere delle garanzie contrattuali da fornitori e prestatori di servizi, come ad esempio: clausole di responsabilità in caso di violazioni di compliance o sanzioni contrattuali in caso di violazione delle confidenzialità e degli accordi sulla protezione dei dati. In questo senso è essenziale esaminare le esigenze specifiche delle parti contraenti al fine di individuare i rischi e regolarne le conseguenze.
È dunque necessario adattare le proprie misure di compliance e attenervisi scupolosamente.
Infine, è auspicabile valutare una copertura assicurativa a tutela dei rischi legati alla criminalità informatica sulla base dei potenziali rischi della propria impresa. Tuttavia è bene tenere presente che una polizza assicurativa non può coprire tutti i rischi. Per questa ragione le imprese devono piuttosto coordinare e integrare la polizza assicurativa con le misure preventive all'interno dell'impresa.

Le responsabilità all'interno dell'azienda
Gli organi direttivi sono responsabili della definizione del panorama dei rischi e dell'implementazione di un sistema di gestione della sicurezza funzionante, che ovviamente include anche la sicurezza informatica. Un danno economico ai danni di un'impresa causato da un attacco informatico può implicare la responsabilità degli organi direttivi personale e illimitata, la quale interviene già in caso di negligenza lieve e non può dunque essere sottovalutata.

La copertura assicurativa dei rischi informatici
In Svizzera e in altri paesi europei, il mercato assicurativo è molto attivo in termini di copertura di rischi informatici. La copertura del rischio informatico è un prodotto nuovo e ancora in evoluzione. Stipulando questo genere di polizze assicurative speciali un'impresa può assicurarsi contro richieste di risarcimento danni da parte di terzi (derivanti dalla legge o dal contratto) e puntualmente anche contro danni propri. Una copertura efficace presuppone l'identificazione dei rischi concreti dell'azienda, determinati dall'attività, dall'organizzazione dell'azienda e dai suoi partner commerciali. La copertura assicurativa è spesso condizionata a degli obblighi di diligenza da parte dell'impresa assicurata. Può rendersi quindi necessario dimostrare di aver utilizzato sistemi di protezione informatica all'avanguardia e di aver adottato le necessarie precauzioni nella la gestione del rischio informatico.
Nel caso in cui la responsabilità cada sugli organi societari è necessario verificare anche una corrispondente copertura responsabilità civile per gli organi societari (Directors-and-Officers (D&O)).

Conclusione
Le cifre presentate dal recente studio di KPMG dimostrano che in generale le imprese sottovalutano i rischi connessi alla criminalità informatica presentando lacune a livello di organizzazione e gestione di tali rischi. Un approccio strutturato consente di identificare i rischi e di utilizzare le conoscenze come misura preventiva. Attraverso la sensibilizzazione e l'acquisizione di conoscenze sui possibili rischi si può reagire in modo veloce e adeguato, garantendo un'efficacie capacità di azione a salvaguardia degli interessi dell'impresa.

**Avvocato specialista FSA responsabilità civile e diritto assicurativo*