La sicurezza informatica come priorità per consigli di amministrazione e CFO

Di Mark Hughes, DXC Technology

Per essere davvero efficaci, consigli di amministrazione e CFO devono conoscere a fondo i rischi e mettere la sicurezza informatica al primo posto in ogni attività: a partire dall'alto.

Sono un dirigente responsabile delle soluzioni di sicurezza per clienti internazionali e credo che la sicurezza informatica debba diventare la priorità di ogni consiglio di amministrazione. Nonostante i budget spesso limitati, **IDC** prevede una crescita annua dell'8,1% in tutto il mondo (pari a 174,7 miliardi di dollari nel 2024) per le spese di sicurezza.

E non è un caso. I furti di dati e gli attacchi ransomware possono causare disagi enormi (addirittura al pari di una catastrofe naturale) e portare le aziende alla paralisi, danneggiando il brand, la fiducia del cliente, le relazioni con i partner e non solo. È un dato sorprendente, ma il costo stimato dei crimini informatici (6.000 miliardi di dollari nel 2021) rappresenta "il più grande trasferimento di ricchezza economica della storia" secondo Cybersecurity Ventures.

Il 2020 dovrebbe aver insegnato qualcosa a consigli di amministrazione e CFO: tutto può succedere. Ma per essere davvero efficaci, bisogna conoscere a fondo i rischi e mettere la sicurezza informatica al centro di ogni attività, a partire dall'alto.

Non solo un problema informatico

È importante sottolineare come ormai la sicurezza non debba proteggere soltanto i sistemi informatici, ma essere integrata in tutto l'ambiente operativo.

Lo scorso giugno le reti interne di un grande produttore internazionale sono state vittima di un attacco ransomware che ha costretto l'azienda a chiudere gli impianti di produzione e a interrompere l'assistenza clienti e i servizi finanziari.

Inoltre, i rischi per le imprese di grandi dimensioni sono sempre più diversificati. Fattori sociali e tecnici relativi ad ambienti normativi, cambiamenti sociali e politici, cultura influiscono sulle possibili minacce.

Una comunicazione inadeguata delle policy aziendali può causare minacce interne e la diffusione di dati sensibili. Dall'introduzione di una nuova policy per il consiglio di amministrazione, di un'operazione di M&A o di un accordo di fornitura possono derivare sabotaggi al sito, alle pagine social o interruzione dei servizi attraverso attacchi DoS. Programmi di privacy troppo flessibili possono mettere in difficoltà le aziende in alcune regioni o non avere gravi conseguenze in altre.

Se è vero che molti consigli di amministrazione capiscono l'impatto che la sicurezza ha sul brand e sulla fiducia del cliente (e i CFO ne conoscono bene i costi), i chief information security officers (CISO) devono affrontare categorie di rischio in continua evoluzione.

La gestione di programmi di sicurezza e di sistemi contro gli attacchi dovrà sempre misurarsi con i rischi e i relativi costi, ma la posta in gioco è alta, per questo le decisioni di sicurezza devono essere prese in modo competente, strategico e collaborativo.

La sicurezza come priorità

Il nostro team ha l'obiettivo di spiegare i potenziali rischi ai dirigenti in termini per loro rilevanti. Sono numerose le best practice che contribuiscono a trasformare la sicurezza in una priorità assoluta per le organizzazioni.

Rischi e ROI al posto di minacce e vulnerabilità. Gli strumenti di monitoraggio informatico e di intelligence possono fornire un quadro preciso dell'incremento degli attacchi, ma non rispondono alla domanda più importante: quanto siamo sicuri?

Ai consigli di amministrazione servono dati per comprendere costi, affidabilità e rischi, ma i CISO devono fornire anche una panoramica "olistica" dell'esposizione al rischio.

Una cultura attenta agli attacchi informatici parte dall'alto. I team dirigenziali sono estremamente vulnerabili agli attacchi di spearphishing, sempre più sofisticati. I CFO cercano di valutare i rischi a fronte dei costi e della potenziale esposizione, così i CISO devono comunicare i ROI in modo chiaro: qual è l'impatto potenziale su quotazioni e valore azionario? Qual è il costo potenziale della vulnerabilità rispetto al costo della risoluzione del problema?

Rendere un sistema sicuro contro ogni minaccia potrebbe avere costi proibitivi, oltre a ostacolare l'innovazione e la crescita aziendale. Le decisioni sono frutto della collaborazione e devono garantire un equilibrio tra le priorità legate al rischio e l'efficienza dei controlli.

Individuare un "security champion". Negli ultimi anni i team dirigenziali hanno tentato di diversificare i ruoli al loro interno. In questo modo i consigli di amministrazione non traggono vantaggio solo da storie e prospettive diverse, ma da competenze rilevanti come gestione degli investimenti, informatica, risorse umane e gestione del rischio.

Inserire un esperto di sicurezza informatica all'interno del consiglio, soprattutto nei settori più esposti come quello bancario, commerciale, sanitario o pubblico potrebbe essere una buona idea. Con un "security champion" sarebbe più facile tenere la sicurezza al centro delle priorità. Un membro del consiglio esperto di sicurezza o capace di gestire le violazioni più gravi aiuterebbe i membri meno esperti a capire meglio i rischi in continuo cambiamento.

Non affidarsi solo all'assicurazione informatica. L'assicurazione informatica è uno strumento piuttosto recente per limitare i rischi e che generalmente copre i danni relativi alla violazione dei dati, inclusi costi legali, notifiche ai clienti, recupero dei dati e riparazione dei sistemi informatici coinvolti. Tuttavia non considera le perdite di valore legate al furto di proprietà intellettuale o i costi dell'aggiornamento software e hardware necessari per prevenire attacchi futuri.

CFO e chief risk officers devono valutare attentamente i vantaggi di un'assicurazione informatica rispetto alle opzioni di autoassicurazione. Nel 2018 la città di Atlanta ha speso **2,7 milioni di dollari a seguito di un attacco informatico** pur non pagando i 50.000 dollari di riscatto. La somma ha coperto in larga parte l'aggiornamento di sistemi ormai obsoleti. L'assicurazione informatica ha permesso al CFO di non pagare il riscatto, ma non ha evitato il danno d'immagine. Prevenzione, risposta rapida e capacità di ripresa operativa restano le difese migliori.

Un processo di gestione agile. Le vulnerabilità sono sempre di più e le tattiche degli hacker sempre diverse, così i programmi di sicurezza necessitano di processi di gestione agili per rispondere in modo appropriato.

Le organizzazioni devono gestire la sicurezza in base alle best practice e ai piani di resilienza, mentre i sistemi core devono affrontare le emergenze tramite piani di ripristino e backup. Proprio come le aziende mirano a continui miglioramenti in ambito operativo o di assistenza tecnica, i consigli di amministrazione e i CFO devono esigere miglioramenti in termini di sicurezza.

La gestione di programmi di sicurezza e di sistemi contro gli attacchi dovrà sempre misurarsi con i rischi e i relativi costi, ma la posta in gioco è alta, per questo le decisioni di sicurezza devono essere prese in modo competente, strategico e collaborativo. Consigli di amministrazione e CFO devono partecipare alla discussione

e rimanere aggiornati sulle minacce più recenti. Iscrivetevi per ricevere il **Security Threat Intelligence Report di DXC**.

Informazioni sull'autore

Mark Hughes è Senior Vice President Offerings and Strategic Partners presso DXC Technology, è responsabile dell'organizzazione e delle offerte di sicurezza di DXC a livello globale, comprese difesa informatica, infrastruttura protetta, identità digitale e protezione dei dati. In precedenza ha ricoperto il ruolo di Chief Executive presso BT Security.