

Prefazione

Il punto di vista di CISO

La sicurezza dell'informazione oggi è un settore a rischio

Quando è stata pubblicata la prima edizione di questo libro, oltre dieci anni fa, la gestione dei rischi per la sicurezza era come un neonato, incapace di camminare, parlare o prendersi cura di sé stessa, e nemmeno di definire sé stessa. Abbiamo percorso un lungo viaggio da quei primi tempi in cui il termine “rischio” ricordava le tabelle delle assicurazioni, più che la sicurezza dei dati. Oggi non si può nemmeno cominciare a occuparsi di sicurezza senza pensare, considerare e includere il rischio in qualsiasi cosa si faccia. Ecco a voi l'evoluzione della sicurezza: il rischio.

Oggi la gestione dei rischi per la sicurezza, che nelle grandi aziende può essere affidata alla responsabilità dell'ufficio legale, amministrativo o di produzione, è un concetto entrato nell'uso corrente. Grazie a iniziative come il Sarbanes Oxley Act (SOX), il Payment Card Industry (PCI), l'Health Information Portability and Accountability Act (HIPAA), la legge SB1386 della California e altre, la sicurezza delle informazioni non è più relegata nelle retrovie delle funzioni IT “di back-end”, sommerse sotto strati di servizi IT concentrati sulla “disponibilità a ogni costo”, ma è considerata una responsabilità condivisa a livello organizzativo, strettamente integrata con tutti i tipi di rischi per la sicurezza presenti nell'ambiente.

Numerose minacce in rapida evoluzione sfidano le priorità e i processi utilizzati per proteggere le nostre imprese. Ogni giorno nuovi strumenti, tecniche, metodi, script e programmi malware a disposizione degli hacker attaccano il mondo con ferocia sempre crescente. Non riusciamo a stare al passo con le minacce e la vastità degli obiettivi che possono colpire nel nostro mondo. Tuttavia, nonostante il panorama delle minacce sia sempre in evoluzione, due elementi rimangono costanti. Il primo è vecchio come il mondo, e ci ricorda che il confine tra bene e male non è sempre così netto: “Per catturare un ladro, devi pensare come un ladro”. Gli americani condensano questo concetto in due parole: *think evil*. La seconda costante è che i professionisti della sicurezza devono avere una passione incrollabile e possedere grandi capacità per muoversi nei meandri tecnici della sicurezza dell'informazione. Senza entrambi questi elementi universali, il fallimento è inevitabile.

“Think evil” è al centro dell'approccio alla sicurezza, e molti del settore hanno scritto su questo argomento. In sostanza, significa che per avere successo nella difesa della sicurezza,

occorre avere la capacità di pensare come un aggressore creativo. Senza questa capacità di prevedere le minacce e difendersi in maniera proattiva, la sicurezza si ridurrà a una verifica meccanica di liste di controllo ricavate in base all'esperienza del passato. E sarete destinati a ripetere i fallimenti del passato.

Un altro imprescindibile requisito per essere in grado di garantire la sicurezza dell'informazione è il possesso di una miscela di varie capacità. Sviluppo di politiche, gestione di programmi, applicazione delle norme e così via sono tutte funzioni preziose e necessarie, ma al termine della giornata, spesso la differenza la fa il "saper mettere le mani sulla tastiera". Niente può sostituire l'esperienza e la conoscenza pratica di un solido professionista che ha partecipato alla guerra di trincea della sicurezza ed è sopravvissuto. Politiche e standard di sicurezza ben definiti, insieme a un forte programma di conformità sono necessari, ma una porta aperta è sempre una porta aperta e una vulnerabilità è un percorso di accesso ai dati. Per ottenere una solida sicurezza in qualsiasi ambiente, è essenziale sviluppare continuamente l'insieme delle conoscenze e capacità tecniche di coloro che hanno la passione di proteggere i nostri sistemi.

Questo libro è una delle fonti di informazioni che contribuiscono a soddisfare entrambi i requisiti per poter avere successo in questo campo. A prescindere dal livello in cui vi trovate nel ciclo vitale della sicurezza, e dal grado di conoscenze tecniche in vostro possesso, vi consiglio caldamente di leggere questo libro, così come lo consiglio a chiunque si occupi di sicurezza, anche il personale privo di conoscenze tecniche, affinché possa imparare a pensare come il nemico o almeno ad apprezzare la profondità e l'estensione delle conoscenze degli hacker. Quando avrete letto, assorbito e compreso a fondo gli argomenti trattati in questo libro, e avrete sviluppato il giusto atteggiamento nei confronti della sicurezza, potrete iniziare a occuparvi efficacemente di gestire la sicurezza in qualsiasi ambiente. Senza questi strumenti, finirete per girare a vuoto lamentandovi continuamente: "Perché la sicurezza è così difficile?".

– *Patrick Heim*
CISO, Kaiser Permanente