Il ruolo dei CISO nella sicurezza informatica aziendale

I CISO devono passare ad un approccio proattivo che metta il monitoraggio continuo, l'uso di strumenti basati sull'intelligenza artificiale, la threat intelligence e l'approccio zero trust al centro del loro modello di sicurezza.

A cura di Stefano Rossi, Territory Account Manager di Bitdefender

La pandemia e ora il conflitto Ucraina – Russia ha portato una maggiore esposizione agli attacchi informatici. I criminali informatici stanno diventando sempre più sofisticati e gli attacchi avanzati odierni sono sempre più complessi, costringendo le aziende a pensare a una protezione su misura.

La società di consulenza e servizi professionali KPMG ha pubblicato il suo report annuale che mette in evidenza otto aree a cui i leader dovrebbero dare priorità per mitigare e minimizzare l'impatto degli attacchi informatici, proteggendo i clienti, i dati e la sostenibilità in un mondo digitale.

Maggiore dialogo sulla sicurezza a livello strategico

La protezione delle risorse critiche, dei sistemi e dei dati sensibili proprietari e dei clienti non è più solo un problema dei professionisti della sicurezza e dell'IT. Gestire e mitigare il rischio per supportare la fattibilità relativa alla strategia e alla sostenibilità operativa aziendale deve essere una responsabilità condivisa che inizia dal business.

La gestione del rischio informatico per ottenere un vantaggio competitivo e un successo a lungo termine deve partire dal consiglio di amministrazione e dalla dirigenza aziendale. Le moderne soluzioni di sicurezza possono solo garantire la riduzione del rischio se gli obiettivi di business non prevedono una solida struttura di sicurezza.

I CISO e i loro team devono dialogare con i decisori aziendali in modo che la sicurezza informatica sia allineata con gli obiettivi strategici dell'azienda.

Il fattore X: colmare il gap tra le necessità delle aziende e i talenti disponibili

Ora che i CISO e i loro team comprendono e parlano la lingua del business, dovrebbero mettere in evidenza come il programma di sicurezza informatica dell'azienda sia fondamentale per la crescita del business.

Purtroppo continua ad esistere un importante gap tra le necessità delle aziende e i talenti disponibili in ambito cybersecurity. Non solo mancano figure con esperienza, ma le risorse tendono a spostarsi perché sono alla ricerca di esperienze diverse per rafforzare le loro competenze esistenti e acquisirne di nuove, come evidenziato da KPMG.

Nei prossimi anni, i team della sicurezza informatica potrebbero avere accesso a un pool di collaboratori esterni fidati, i cosiddetti "gig worker", a seconda dei carichi di lavoro e della capacità. Ciò consentirà ai CISO di avere team composto da un nucleo ridotto e strategico, per poi ampliarlo e ridurlo in base alle necessità.

Adattare la sicurezza al cloud

La sicurezza informatica e la sicurezza cloud stanno diventando sinonimi, come messo in luce dal report. Tutti i principi che si applicano alla sicurezza on-premise - protezione dei dati, gestione delle identità e degli accessi, infrastrutture e gestione delle vulnerabilità - sono applicabili al cloud.

I CISO e i loro team devono lavorare con partner aziendali strategici per garantire che tutti comprendano i requisiti di sicurezza specifici del cloud e per collaborare con i fornitori di servizi cloud per evitare configurazioni errate.

L'identità al centro dell'approccio zero trust

Con l'aumento esponenziale del telelavoro e dell'e-commerce derivante dalla pandemia, la protezione dei dati sensibili non è mai stata così ardua. Le aziende devono considerare l'adozione di un approccio e di un'architettura zero-trust, con la gestione delle identità e degli accessi (IAM) al cuore della strategia.

Il report mette in evidenza che gli attuali modelli IAM, originariamente creati per gestire le identità digitali e l'accesso degli utenti per le singole aziende, sono stati ripensati per offrire il giusto livello di resilienza e fornire funzionalità di autenticazione fondamentali adatte ad ambienti informatici federati, privati, pubblici o multicloud.

Come un approccio automatizzato che può aiutare a eliminare i costi e i processi manuali, ridurre la superficie di attacco e stabilire policy e principi di sicurezza informatica, il modello di sicurezza zero trust si sta affermando sempre più come approccio sostenibile.

Sfruttare l'automazione della sicurezza

Alcuni dei principali benefici potenziali dell'automazione si ottengono quando ci si concentra sulle implementazioni progettate per aiutare a risolvere problemi aziendali, afferma il report. Per esempio: accrescere le competenze dei collaboratori orchestrando in modo più efficiente le attività

ordinarie, ottenere un vantaggio competitivo in aree in cui la rapidità è importante e analizzare grandi set di dati, spesso non strutturati.

A fronte di un panorama delle minacce in costante crescita in termini di volumi e di complessità e la mancanza di disponibilità di talenti nella sicurezza informatica continua ad aumentare, le aziende si affideranno sempre più a processi di sicurezza automatizzati, per automatizzare le funzioni di sicurezza relative a compiti di routine e ripetitivi, liberando così le risorse.

Le funzioni che erano precedentemente eseguite da professionisti altamente specializzati come la scansione delle vulnerabilità, l'analisi dei log e la conformità possono essere ora standardizzate ed eseguite automaticamente. Questo può accelerare il rilevamento degli incidenti e i tempi di risposta e garantire scalabilità.

Proteggere la frontiera della privacy

In molte aziende, la sicurezza informatica e la privacy dei dati sono viste come discipline diverse che spesso operano separatamente. In un ambiente in cui vengono utilizzati una moltitudine di dati sensibili, la revisione di terze parti, nuovi sistemi e nuove applicazioni richiede un approccio multidisciplinare alla gestione del rischio legato alla privacy. Dovrebbe includere sia la privacy che la sicurezza dalla fase di progettazione fino alla gestione del cambiamento organizzativo.

Oggi, c'è più consapevolezza e riconoscimento dei diritti delle persone riguardo alle loro informazioni personali. Il crescente numero di normative sulla privacy dei dati, ha portato ha un maggiore focus sulla protezione della privacy e della sicurezza dei dati.

Con così tante normative diverse, il panorama normativo è diventato sempre più complesso da gestire, in particolare per le aziende che operano in più paesi. L'automazione è fondamentale per il successo, come rilevato dal report, soprattutto per le aziende che non dispongono delle risorse per gestire aree come la valutazione del rischio relativo alla privacy e al reporting.

Protezione oltre i confini

Aziende di ogni dimensione stanno cercando di trasformare digitalmente le loro operazioni, e questo comporta l'adozione di un approccio incentrato sui dati che vengono condivisi regolarmente in un ecosistema connesso di partner.

Ciò crea numerose opportunità per i criminali informatici di compromettere i sistemi e i dati, e i CISO devono proteggere le loro aziende e allo stesso tempo incoraggiare il più ampio ecosistema ad adottare soluzioni di sicurezza informatica.

Le aziende hanno bisogno di verificare adeguatamente le policy di sicurezza organizzativa dei potenziali vendor, così come la sicurezza per i prodotti e i servizi a cui accedere, come evidenzia il

report. Ciò richiede uno straordinario impegno in termini di due diligence da parte di ogni singolo partner dell'ecosistema. I CISO devono passare ad un approccio proattivo che metta il monitoraggio continuo, l'uso di strumenti basati sull'intelligenza artificiale, la threat intelligence e lo zero trust al centro del loro modello di sicurezza.

Resilienza informatica

Molte aziende oggi operano come imprese digitali e hanno bisogno di sapere quanto siano in grado di ripristinare le proprie attività in caso di un potenziale grave incidente informatico. Il report incoraggia i CISO e i loro team a mantenere una comunicazione costante con i dirigenti che partono dal presupposto che, in caso di un attacco informatico, l'azienda possa recuperare in pochi giorni.

Le aziende dovrebbero comprendere come poter garantire la continuità del business nel caso si verificasse un'interruzione per più settimane. Devono prendere in considerazione vari aspetti: come preparare l'azienda ad affrontare un'interruzione di quattro o sei settimane a causa di un attacco informatico; il possibile impatto di un'interruzione sul servizio clienti, sui call center e sui centri di distribuzione ma anche in termini di requisiti normativi e legali dell'azienda, ecc.

"La resilienza richiede una valutazione dei principali processi operativi aziendali e una strategia per proteggerli", afferma il report. "Nel mercato attuale, un attacco informatico è quasi inevitabile per la maggior parte delle aziende. Con questa premessa, pensando all'approccio in evoluzione dei professionisti della sicurezza, il focus per molti CISO oggi si divide, in parti uguali, tra la riduzione della probabilità di attacco e la gestione delle conseguenze".

Scopri di più su come la protezione dei carichi di lavoro in cloud può ottimizzare e migliorare gli ambienti cloud e ibridi.

Informazioni su Bitdefender

Bitdefender fornisce efficaci soluzioni di sicurezza informatica che garantiscono alte prestazioni e facilità d'uso alle PMI, alle medie aziende e ai consumatori. Con una vision incentrata sul fornire le soluzioni di sicurezza informatica più affidabili al mondo, la missione di Bitdefender è difendere le aziende e le persone in tutto il mondo dagli attacchi informatici per trasformare e migliorare la loro esperienza digitale. Per maggiori informazioni, è possibile visitare la pagina https://www.bitdefender.com

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it