Budgeting per la sicurezza informatica: responsabilità del CISO



La sicurezza informatica è ormai una priorità imprescindibile per le aziende di tutte le dimensioni. Con l'evoluzione delle minacce cyber e l'aumento delle normative che richiedono una protezione più rigorosa dei dati aziendali e dei clienti, il **Chief Information Security Officer** (CISO) si trova al centro di un processo complesso: il **budgeting** per la sicurezza informatica.

Questo processo non solo è fondamentale per proteggere l'infrastruttura aziendale, ma riveste anche un ruolo cruciale nella giustificazione degli investimenti e nella gestione delle risorse economiche destinate a questa causa.

In un contesto di risorse limitate, il CISO deve essere in grado di giustificare e allocare correttamente i fondi, monitorando al contempo le spese e analizzando il ritorno sugli investimenti (ROI) per garantire che ogni euro speso contribuisca a una maggiore protezione. In questo articolo, esploreremo le diverse dimensioni del budgeting per la sicurezza informatica, con particolare attenzione alle responsabilità del CISO.

Giustificazione degli investimenti in Cybersecurity al top Management: il ruolo strategico del CISO

Una delle prime sfide che il CISO affronta quando si tratta di budgeting per la sicurezza informatica è la giustificazione degli investimenti al top management. I CISO stanno evolvendo,

passando da una visione improntata alla paura a un approccio focalizzato sulla crescita, cercando di allineare le strategie di sicurezza informatica con gli obiettivi aziendali.

Questa analisi non solo mette in evidenza le preoccupazioni riguardo al rallentamento economico e alle restrizioni di **budget**, ma dimostra anche come i CISO stiano acquisendo una maggiore consapevolezza del business, segnando un cambiamento importante dai ruoli tradizionali a quelli di veri e propri facilitatori strategici per l'azienda.

In molte organizzazioni, la cybersecurity è vista come una spesa necessaria ma non direttamente correlata ai profitti aziendali. Pertanto, il CISO deve dimostrare in modo convincente che l'investimento in cybersecurity non è solo un costo, ma una necessità strategica che protegge l'azienda da rischi ben superiori.

I **budget destinati alla cybersecurity** riportati nel "The CISO Report 2025" realizzato da Splunk in collaborazione con Oxford Economics, mostrano un supporto non coerente e disallineato: solo il 29% dei CISO dichiara di ricevere un budget adeguato alle iniziative di sicurezza informatica e il raggiungimento degli obiettivi di sicurezza, mentre il 41% dei membri del CDA ritiene che i budget per la sicurezza informatica siano sufficienti.

Il 64% dei CISO esprime preoccupazione per il fatto che il contesto normativo attuale e le minacce informatiche possano compromettere la propria capacità di operare efficacemente.

I CISO hanno inoltre segnalato una riduzione delle soluzioni e degli strumenti di sicurezza (50%), il blocco delle assunzioni nel settore della sicurezza (40%) e la diminuzione o l'eliminazione della formazione sulla sicurezza (36%) come principali misure adottate per il contenimento dei costi.

Il primo passo per giustificare i fondi per la sicurezza informatica è comprendere e comunicare i rischi aziendali

legati alla mancanza di protezione. Il CISO deve essere in grado di spiegare come le minacce cyber possono compromettere la reputazione dell'azienda, danneggiare la fiducia dei clienti e portare a sanzioni finanziarie legate a violazioni dei dati. Il CISO può presentare casi concreti di violazioni della sicurezza o attacchi informatici che hanno avuto impatti devastanti su altre aziende, per illustrare il rischio che l'organizzazione sta correndo.

Il problema per il management non riguarda tanto l'aspetto monetario o dei costi, in quanto il compito del management è proprio quello di allocare risorse e definire i costi. Ogni attività ha un costo: acquisire un nuovo cliente, migliorare la visibilità del brand, implementare misure di sicurezza informatica, e così via. La vera difficoltà per il management sta nella **comprensione**.

Il management desidera comprendere come e dove vengono destinati i fondi, e vuole assicurarsi che questi siano stati impiegati in modo efficace. La sicurezza informatica può risultare talvolta complessa, difficile da comprendere e troppo tecnica. L'uso di metriche e la loro rappresentazione grafica all'interno di una presentazione chiara e ben strutturata, ad esempio in un PowerPoint, rendono più semplice per il management capire l'efficacia e giustificare l'accettazione di tali voci di spesa.

Un'altra strategia efficace consiste nel quantificare il rischio e associare a ogni minaccia un valore economico. Attraverso modelli di rischio basati sul valore economico potenziale di un attacco informatico, è possibile mostrare al management quanto potrebbe costare un attacco in termini di danni diretti (come la perdita di dati o il fermo dei sistemi) e indiretti (come la perdita di clienti e la reputazione). Una chiara analisi di rischio aiuta il CISO a motivare l'allocazione di risorse per prevenire o mitigare questi danni.

Essere in grado di valutare l'efficacia delle misure di sicurezza è un ottimo modo per giustificare le scelte di spesa e per rivedere i futuri budget per la sicurezza informatica. Le metriche di sicurezza offrono informazioni sulla solidità della vostra postura di sicurezza, inclusa l'efficacia delle misure di conformità adottate. Queste metriche forniscono un metodo quantitativo per dimostrare al management e ai membri del consiglio come un programma di sicurezza dei dati stia performando. Inoltre, possono aiutare a documentare l'approccio dell'azienda alla protezione dei dati in conformità con le normative vigenti. L'analisi di **KPI** e indicatori di rischio chiave (KRI) fornisce una visione chiara dello stato della sicurezza e del team, permettendo di ottimizzare strategie e approcci.

Esistono diversi KPI che possono essere misurati. Ad esempio, tra le metriche relative alle minacce, ci sono:

- Incidenti di sicurezza;
- Tempo medio di rilevamento (MTTD);
- Tempo medio di risoluzione (MTTR).

Infine, è importante che il CISO lavori a stretto contatto con altre funzioni aziendali, come il dipartimento legale, quello delle risorse umane e delle operazioni, per evidenziare come la cybersecurity influisca su più aree dell'organizzazione e non sia solo una preoccupazione tecnica. Quando la cybersecurity viene vista come una responsabilità condivisa e non come una funzione isolata, il management è più propenso a riconoscere l'importanza degli investimenti in sicurezza.

Allocazione delle risorse per massimizzare la protezione

A causa del rallentamento dell'economia, i CISO si trovano sotto forte pressione per assicurare una protezione informatica adeguata senza compromettere le iniziative di

crescita dell'azienda. Le imprese stanno puntando a modernizzare le loro infrastrutture IT come parte della trasformazione digitale, il che evidenzia la necessità di strategie di sicurezza che favoriscano, piuttosto che ostacolare, il progresso.

Una volta che il budget per la sicurezza informatica è stato approvato, il CISO deve affrontare la complessa sfida dell'allocazione delle risorse. La sfida consiste nel rendere altrettanto trasparente all'interno dell'organizzazione il modo in cui viene distribuito il budget per la cybersecurity, in modo da giustificarne il costo. La differenza sta nel fatto che, rispetto a funzioni come marketing, vendite, progettazione e assistenza – dove il ritorno sugli investimenti può essere spiegato con maggiore facilità – la matematica del ROI della sicurezza informatica è più complessa. Un aspetto cruciale è determinare come distribuire il budget tra le **diverse** aree della cybersecurity, come la protezione dei dati, la gestione delle vulnerabilità, la formazione del personale e la protezione dalle minacce emergenti.

La protezione dei dati è uno degli aspetti principali in cui il CISO dovrà investire. Con l'aumento dei regolamenti sulla privacy come il GDPR e altre normative a livello mondiale, la protezione dei dati sensibili deve essere una priorità assoluta. Ciò significa allocare risorse significative per strumenti di cifratura, soluzioni di backup sicuro, e politiche di gestione degli accessi che garantiscano che solo le persone autorizzate possano accedere a informazioni riservate.

Esistono normative di conformità che guidano l'allocazione delle risorse per la cybersecurity. Nel settore sanitario, ad esempio, è fondamentale garantire specifici requisiti di privacy per proteggere le cartelle cliniche e altre informazioni sensibili relative alla salute delle persone. Per rispettare queste normative, evitando sanzioni significative,

i CISO sono costretti a investire in strumenti e tecnologie specializzate, come la classificazione dei dati e la crittografia.

Accanto alla protezione dei dati, è necessario anche investire nella gestione delle vulnerabilità. I sistemi informatici sono in continua evoluzione, e nuove vulnerabilità vengono scoperte regolarmente. Il CISO deve stabilire una strategia per monitorare e gestire queste vulnerabilità, assicurandosi che vengano applicate tempestivamente le patch e le correzioni necessarie. Questo tipo di investimento è essenziale per ridurre il rischio che un attacco informatico sfrutti una debolezza nel sistema.

Anche la formazione del personale è un'area chiave per l'allocazione delle risorse. Le statistiche mostrano che una delle principali cause di violazioni della sicurezza è l'errore umano, come cliccare su link dannosi o utilizzare password deboli. Investire in programmi di formazione continua per i dipendenti, sensibilizzandoli sui rischi informatici e sulle best practices da adottare, è una strategia fondamentale per rafforzare la difesa dell'organizzazione.

Infine, il CISO deve tenere conto delle minacce emergenti e destinare risorse per affrontarle. Le minacce informatiche evolvono rapidamente, quindi è fondamentale che il CISO allocchi parte del budget per soluzioni innovative che rispondano a minacce come l'intelligenza artificiale malevola, il ransomware avanzato e gli attacchi alle infrastrutture di rete. La continua evoluzione della tecnologia impone che il bilancio venga pianificato con una visione di lungo termine, pronta ad adattarsi alle nuove sfide.

La parte del budget destinata alla cybersecurity per ciascuna categoria dipende quindi da vari fattori. Ad esempio, nuovi obblighi di conformità potrebbero rendere necessario un incremento delle costi in questa area in un determinato periodo. Allo stesso modo, l'arrivo di un nuovo investitore o

CEO potrebbe comportare un cambiamento nelle priorità, portando a un aumento o a una riduzione complessiva dell'investimento in sicurezza, in base a una diversa tolleranza al rischio dell'organizzazione. Questo scenario potrebbe spingere il CISO a rivedere e riallocare le risorse tra le diverse categorie.

Monitoraggio delle spese e ritorno sugli investimenti (ROI)

Una volta allocato il budget per la sicurezza informatica, il CISO deve monitorare attentamente le spese per garantire che ogni risorsa sia utilizzata in modo efficace ed efficiente. Il monitoraggio dei costi in sicurezza informatica può essere complicato, in quanto i benefici di molte misure di protezione non sono sempre immediatamente visibili in termini di risparmio economico diretto. Tuttavia, è fondamentale che il CISO stabilisca parametri chiari per il controllo e la valutazione dell'efficacia degli investimenti.

Per calcolare il ritorno sugli investimenti (**ROI**), il CISO può adottare vari approcci. Uno dei più utilizzati è il modello del "costo per prevenire una violazione", che cerca di stabilire il risparmio derivante dall'evitare danni potenziali a causa di un attacco informatico. In questo modo, l'efficacia delle soluzioni di sicurezza può essere misurata in termini di costi evitati anziché in termini di spese dirette.

Un'altra metrica utile per monitorare le uscite alla voce sicurezza è il "tempo di risposta agli incidenti". Investire in soluzioni che riducono il tempo necessario per identificare e rispondere a un attacco può ridurre significativamente il danno causato da una violazione. Misurando i miglioramenti nelle capacità di risposta agli incidenti nel tempo, il CISO può giustificare gli investimenti in soluzioni più sofisticate.

Il CISO dovrebbe anche sfruttare le metriche di performance per monitorare i progressi della sicurezza aziendale. Queste metriche potrebbero includere il numero di vulnerabilità risolte, il numero di minacce rilevate, il livello di conformità alle normative e la percentuale di dipendenti formati sulla sicurezza. Questi indicatori aiutano a dimostrare che gli investimenti stanno portando risultati tangibili e misurabili.

Strategie per ottenere finanziamenti aggiuntivi per la sicurezza

Anche se il budget iniziale per la sicurezza informatica può essere approvato, spesso il CISO si trova a dover affrontare la necessità di risorse aggiuntive per affrontare minacce emergenti o per aggiornare le soluzioni di sicurezza obsolete. In questi casi, il CISO deve adottare strategie efficaci per ottenere il supporto finanziario necessario.

Una delle prime strategie consiste nel fornire dati e analisi più approfondite sugli impatti economici di un attacco informatico. Utilizzando modelli di calcolo dei costi legati a un'eventuale violazione della sicurezza, il CISO può presentare una solida giustificazione per l'incremento del bilancio. La simulazione di scenari di attacco può essere un modo convincente per mostrare al management l'importanza di un investimento continuo in cybersecurity.

Per ottenere aumenti di budget in modo strategico e mirato, è fondamentale adattare il proprio approccio comunicativo sulla sicurezza in base ai diversi interlocutori. Quando ci si rivolge a un consiglio di amministrazione composto da membri provenienti da settori differenti, è utile presentare a ciascuno una "storia" che risuoni con le sue specifiche preoccupazioni. Questo approccio facilita un dialogo

costruttivo, sia nel caso di dover spiegare violazioni della sicurezza, sia quando si richiedono investimenti per nuove iniziative di cybersecurity.

Un'altra strategia per ottenere risorse aggiuntive è quella di collaborare con altre aree dell'azienda per integrare la cybersecurity in progetti più ampi. Ad esempio, se l'azienda sta per lanciare un nuovo prodotto o servizio, il CISO può dimostrare che un adeguato investimento in sicurezza è essenziale per proteggere la reputazione del prodotto e la fiducia dei clienti. Presentare la cybersecurity come un elemento essenziale per il successo dell'intera azienda aumenta la possibilità di ottenere di ottenerne di nuovi.

Infine, il CISO può esplorare opzioni di finanziamento esterne, come sussidi governativi o incentivi fiscali, che supportano l'adozione di misure di sicurezza avanzate. Spesso, i governi offrono incentivi alle aziende che investono in protezione contro le minacce cyber, e il CISO può utilizzare queste opportunità per ottenere risorse aggiuntive senza gravare troppo sul budget aziendale.

Conclusioni

La gestione del budgeting per la sicurezza informatica è una delle principali responsabilità del CISO e rappresenta una sfida complessa ma fondamentale per garantire la protezione delle risorse aziendali. La giustificazione degli investimenti, l'allocazione ottimale delle risorse, il monitoraggio delle spese e la ricerca di finanziamenti aggiuntivi sono tutti passaggi cruciali per garantire che l'azienda rimanga protetta dalle minacce informatiche emergenti. Con un approccio strategico e una attenta gestione, il CISO può non solo migliorare la sicurezza, ma anche giustificare e ottimizzare gli investimenti in un'area fondamentale per il successo dell'organizzazione nel lungo termine.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/budgeting-ciso/