Il CISO come leader nella gestione del rischio informatico



Il rischio informatico è uno degli aspetti più critici della gestione aziendale moderna, soprattutto in un’epoca in cui la digitalizzazione e la trasformazione tecnologica sono al centro delle operazioni di ogni organizzazione. Per garantire la protezione dei dati aziendali, dei sistemi e delle informazioni sensibili, il **Chief Information Security Officer (CISO)** gioca un ruolo fondamentale. Tale figura è stata trattata seppur in maniera indiretta e più sintetica, in un altro elaborato realizzato in precedenza. Questo articolo esplorerà invece, in maniera più approfondita, il ruolo del CISO nella gestione del **cyber risk**, con particolare attenzione alla definizione e valutazione dei pericoli, alla mitigazione e all’integrazione del risk management nelle decisioni strategiche, nonché alla collaborazione con altri manager aziendali.

Definizione e valutazione dei rischi informatici nel contesto aziendale moderno

La gestione del Cyber risk inizia con una valutazione accurata dei rischi che un’azienda è chiamata a fronteggiare. Questo processo è cruciale, poiché solo identificando, comprendendo e misurando le minacce digitali, un’organizzazione può prendere decisioni informate per proteggere i propri asset. Il CISO, il cui ruolo ha assunto ulteriore rilevanza con l’entrata in vigore della direttiva **Nis2**, è il responsabile di questa fase, che coinvolge una serie di attività analitiche. In qualità di

leader nella gestione del rischio informatico, il CISO è responsabile della protezione delle risorse digitali aziendali contro minacce esterne ed interne.

Non è più solo un tecnico, ma un vero e proprio manager a tutto tondo.

CISO: da tecnico informatico a manager strategico della sicurezza aziendale

Il CISO deve saper interagire in modo efficace con diversi stakeholder, traducendo le complesse esigenze di sicurezza informatica in strategie aziendali chiare, operative e sicure. Per raggiungere questo obiettivo, è indispensabile non solo un'elevata competenza tecnica, ma anche doti di leadership, una profonda comprensione delle dinamiche aziendali e una solida capacità di gestione dell'Information security risk. Inoltre, eccellenti abilità comunicative sono essenziali per garantire una diffusione accurata delle informazioni, facilitando il processo decisionale strategico che spesso richiede il suo contributo.

È incaricato quindi di progettare e mettere in atto programmi completi per la sicurezza delle informazioni, proteggendo l'organizzazione dalle minacce informatiche. Inoltre, riveste un ruolo capillare nella formulazione di strategie solide che assicurano la riservatezza, l'integrità e la disponibilità dei dati, proteggendo le risorse e le infrastrutture aziendali. È anche responsabile della scelta di misure di sicurezza IT adeguate a migliorare la resilienza dell'organizzazione contro le minacce cyber in continua evoluzione.

La **prima fase** della gestione del rischio informatico consiste nell'identificare i vari tipi di potenziali pericoli che potrebbero minacciare l'integrità e la sicurezza delle risorse

aziendali.

Le recenti normative richiedono l'adozione **dell'Enterprise Risk Management (ERM)** per individuare e analizzare i diversi tipi di rischio a cui un'azienda è esposta. Questo processo prevede la valutazione della probabilità che essi si manifestino e la misurazione delle loro possibili conseguenze. Affinché un programma ERM sia realmente efficace, è fondamentale il coinvolgimento di tutti i team aziendali e l'implementazione di un ciclo continuo di gestione del rischio. In questo contesto, il Cyber risk rappresenta un elemento cruciale dell'ERM, assumendo un ruolo sempre più rilevante con l'avanzare della digitalizzazione.

La valutazione delle minacce per la sicurezza informatica è un processo sistematico che identifica, analizza e valuta le potenziali minacce informatiche che un'organizzazione potrebbe affrontare. Questo processo consente infatti al CISO di comprendere la portata e la gravità di essi, nonché di prendere decisioni informate su come mitigarli.

Le fasi principali nella valutazione dei pericoli per la sicurezza informatica sono:

Identificazione degli asset: il primo passo consiste nel mappare tutti gli asset IT dell'organizzazione, inclusi hardware, software, dati e reti.

Valutazione delle minacce: successivamente, è importante identificare le possibili minacce informatiche che potrebbero compromettere gli asset individuati. Questo include minacce interne ed esterne, come malware, attacchi di phishing, intrusioni e attacchi DDoS.

Analisi delle vulnerabilità: le vulnerabilità rappresentano le debolezze nei sistemi o nei processi che potrebbero essere sfruttate da attaccanti per eseguire un attacco. Il CISO ha il compito di individuare e analizzare queste vulnerabilità nei vari asset aziendali.

Valutazione dell'impatto: per ciascuna minaccia e vulnerabilità rilevata, è necessario esaminare l'impatto che un eventuale attacco potrebbe avere sull'organizzazione. Questo include l'analisi della perdita di dati, l'interruzione dei servizi, danni alla reputazione e le ripercussioni economiche.

Prioritizzazione dei rischi: in base alla valutazione dell'impatto, i rischi vengono classificati in ordine di priorità, considerando sia la gravità che la probabilità che si verifichino.

Trattamento dei rischi: una volta stabilita la priorità di essi, è necessario adottare misure per trattarli. Ciò può significare implementare soluzioni di sicurezza per ridurli, trasferirli a terze parti o accettarli quando non è possibile ridurli efficacemente.

Strumenti e metodologie per la valutazione dei rischi: esistono vari strumenti e approcci per aiutare il CISO nel processo di valutazione degli stessi per la sicurezza informatica. Tra i più comuni troviamo:

- **Questionari di valutazione dei rischi**: forniscono una struttura utile per una loro identificazione e valutazione.
- **Strumenti di scansione delle vulnerabilità**: utilizzati per analizzare i sistemi e le reti alla ricerca di vulnerabilità.
- **Software di valutazione del rischio basato su modelli**: strumenti che utilizzano modelli matematici per calcolare il rischio complessivo relativo alla sicurezza informatica dell'organizzazione.

Il ruolo del CISO nella valutazione dei rischi prevede una attività di supervisione e coordinamento dell'intero processo di valutazione di essi. Deve quindi garantire che la valutazione venga condotta in modo completo, accurato e

tempestivo. Inoltre, il CISO deve utilizzare i risultati della valutazione per prendere decisioni informate sulla gestione dei rischi e allocare le risorse di sicurezza in modo ottimale.

Tipologie principali di rischi informatici e loro implicazioni sulla sicurezza aziendale

Tra i principali pericoli vi sono:

- **Rischi legati alla protezione dei dati:** la violazione della privacy dei dati sensibili, come le informazioni finanziarie, sanitarie o personali dei clienti.
- **Rischi di accesso non autorizzato:** il pericolo che utenti esterni o interni non autorizzati possano accedere a sistemi o dati riservati.
- **Rischi legati a malware e attacchi informatici:** i malware, i ransomware e gli attacchi di phishing rappresentano minacce gravi che possono compromettere la sicurezza aziendale.
- **Rischi relativi alla sicurezza della rete:** vulnerabilità nella rete aziendale, che potrebbero consentire attacchi esterni attraverso reti non sicure.

Una volta identificati, il CISO, insieme al team di sicurezza informatica, deve valutare l’impatto e la probabilità di ciascun rischio. L’analisi di esso consente di determinare quali pericoli presentano la maggiore minaccia per l’organizzazione e le risorse aziendali. La valutazione è spesso supportata da strumenti di gestione del rischio e da metodologie come la **matrice di rischio**, che permette di classificare i pericoli in base alla gravità e alla probabilità che si verifichino.

Vantaggi della valutazione dei rischi per la sicurezza informatica: la valutazione dei rischi informatici porta

numerosi benefici e vantaggi alle aziende, tra cui:

- **Maggiore consapevolezza dei rischi**: aiuta il CISO a comprendere la natura e l'impatto a cui l'organizzazione è esposta.
- **Decisioni di sicurezza più informate**: permette di allocare meglio le risorse per implementare misure di mitigazione dei rischi.
- **Riduzione delle violazioni dei dati**: una gestione efficace dei rischi abbassa significativamente la probabilità di violazioni e i danni correlati.
- **Conformità alle normative**: facilita il rispetto di leggi come il GDPR, migliorando la protezione dei dati.
- **Aumento della fiducia dei clienti**: le aziende che gestiscono efficacemente la sicurezza informatica guadagnano maggiore fiducia da parte dei clienti.

Gestione delle identità e degli accessi (IAM): il CISO ha un ruolo cruciale nell'IAM, che include:

- **Definizione di politiche e procedure IAM**: stabilire autorizzazioni, privilegi e protocolli di autenticazione.
- **Implementazione di soluzioni IAM**: scegliere e configurare soluzioni adatte all'organizzazione, con attenzione alla scalabilità e all'integrazione.
- **Monitoraggio e gestione sicura delle identità**: gestire la creazione, l'aggiornamento e la disattivazione degli account, oltre alla protezione delle informazioni di autenticazione.
- **Conformità legale**: garantire il rispetto delle normative relative alla protezione dei dati e alla privacy.

Inoltre, il CISO deve essere aggiornato sulle tecnologie emergenti come l'autenticazione biometrica e la gestione degli accessi privilegiati, adattando le strategie di IAM alle nuove minacce. Il successo di un programma IAM dipende dalla collaborazione tra il CISO e gli altri stakeholder aziendali,

per rafforzare la sicurezza informatica e proteggere i dati aziendali sensibili.

Strategie di mitigazione dei rischi e compliance normativa nella cybersecurity

I CISO giocano un ruolo cruciale nel garantire il rispetto delle normative, il che comporta non solo assicurarsi che l'organizzazione aderisca alle leggi, ma anche comprendere come queste normative influenzano le operazioni quotidiane e le **strategie aziendali**. Infatti, i CISO devono prendere sempre più responsabilità nell'aggiornarsi costantemente sui cambiamenti normativi e tradurli in politiche pratiche per proteggere la privacy e l'integrità dei dati.

In questo contesto, i CISO devono interagire sempre di più con i dipartimenti legali e di compliance, affrontando la complessità dei requisiti imposti da **normative** come GDPR, DORA, NIS2, Cyber Resilience Act, AI Act e altre leggi pertinenti. Il loro compito principale è garantire che l'organizzazione rispetti queste normative e protegga i dati sensibili. Adottando un approccio proattivo alla compliance e utilizzando strumenti e tecnologie adeguate, i CISO possono ridurre il pericolo di violazioni dei dati.

Inoltre, i CISO sono responsabili di promuovere una cultura di conformità continua all'interno dell'organizzazione, realizzando audit regolari e implementando meccanismi per identificare e colmare eventuali lacune. Questo non solo aiuta a mitigare i rischi legali e finanziari, ma contribuisce anche a migliorare la reputazione dell'azienda, a rafforzare la fiducia degli stakeholder e a ottenere un vantaggio competitivo.

Una volta che le minacce o i pericoli sono stati identificati

e valutati, il CISO deve sviluppare strategie per mitigare o, almeno, ridurre l'impatto di essi. Le strategie di mitigazione sono fondamentali per prevenire gli attacchi informatici o per minimizzare i danni in caso di incidente. Tra le principali azioni che il CISO può intraprendere per ridurre le minacce segnaliamo:

- **Implementazione di soluzioni tecnologiche avanzate:** utilizzare strumenti di cybersecurity come firewall, sistemi di rilevamento delle intrusioni (IDS), antivirus e sistemi di prevenzione delle perdite di dati (DLP). Questi strumenti sono necessari per monitorare costantemente la rete aziendale e rilevare attività sospette.
- **Formazione del personale:** molte violazioni della sicurezza informatica avvengono a causa di errori umani, come cliccare su link di phishing o utilizzare password deboli. Il CISO deve organizzare programmi di formazione per sensibilizzare i dipendenti riguardo alle migliori pratiche di sicurezza e a come riconoscere e prevenire potenziali minacce.
- **Pianificazione della risposta agli incidenti:** è essenziale che il CISO sviluppi un piano di risposta agli incidenti chiaro e ben definito. In caso di attacco informatico, l'organizzazione deve essere pronta a rispondere rapidamente per contenere il danno e riprendersi dalla violazione. Un piano di risposta agli incidenti prevede attività come il recupero dei dati, l'analisi forense e la comunicazione con le autorità competenti.
- **Gestione delle vulnerabilità:** il CISO deve garantire che le vulnerabilità software vengano monitorate e corrette tempestivamente. L'adozione di pratiche come il **patch management** è necessaria per mantenere i sistemi protetti da eventuali falle di sicurezza.

Inoltre, è fondamentale che il CISO valuti continuamente

l’efficacia delle strategie di mitigazione implementate. In un ambiente di sicurezza in continua evoluzione, l’adeguamento continuo alle nuove minacce è cruciale per mantenere al sicuro l’organizzazione.

Integrazione del risk management nelle decisioni strategiche aziendali

Una delle sfide principali per un CISO è garantire che la gestione del Cyber risk venga integrata nelle decisioni strategiche aziendali. Questo richiede un cambiamento di mentalità: non è più sufficiente considerare la sicurezza informatica come un dipartimento separato o un costo da contenere. Molte imprese italiane vedono ancora il CISO come una figura puramente tecnica, relegata al reparto IT. Questo rallenta il passaggio verso una cybersecurity strategica, in cui la protezione dei dati è parte integrante della governance aziendale. Oggi, il Cyber risk deve essere trattato come una priorità strategica che influisce su tutte le aree dell’organizzazione.

Il CISO deve infatti lavorare a stretto contatto con il top management e con altri dirigenti aziendali per garantire che la gestione del rischio informatico sia un obiettivo condiviso. Ciò implica l’**integrazione** di esso nelle discussioni riguardanti la pianificazione strategica, la crescita aziendale, l’innovazione e la digitalizzazione. Ad esempio:

- **Decisioni su nuove tecnologie:** l’adozione di nuove tecnologie, come l’intelligenza artificiale, l’Internet delle cose (IoT) o il cloud computing, comporta nuove sfide in termini di Cyber risk. Il CISO deve partecipare attivamente alla valutazione dei rischi legati a queste tecnologie.

- **Sicurezza nelle acquisizioni e fusioni:** quando un’organizzazione acquisisce o si fonde con un’altra, il CISO deve valutare il Cyber risk associato alle infrastrutture IT, alle politiche di sicurezza e alla protezione dei dati. L’integrazione delle due aziende deve essere pianificata tenendo conto della sicurezza informatica come una priorità strategica.
- **Protezione della reputazione aziendale:** un attacco informatico o una violazione della privacy dei dati può danneggiare gravemente la reputazione dell’organizzazione. Il CISO deve garantire che la gestione dell’Information security risk sia una parte integrante della strategia di branding e della protezione della reputazione.

L’integrazione del risk management nelle decisioni aziendali implica anche la comunicazione regolare dei rischi e delle misure adottate a tutti i livelli dell’organizzazione. Questo approccio consente una maggiore consapevolezza della sicurezza in tutta l’azienda, dai dirigenti fino ai dipendenti, e facilita l’approvazione e l’attuazione di strategie di mitigazione.

Collaborazione con altri dirigenti per una gestione olistica del rischio informatico

Per una gestione efficace delle minacce informatiche, è fondamentale che il CISO collabori con altri dirigenti aziendali, come il **Chief Financial Officer** (**CFO**), il **Chief Operating Officer** (**COO**)**,** e il **Chief Legal Officer** (**CLO**). La sicurezza informatica non può più essere considerata solo un problema del reparto IT, ma deve essere trattata come una questione trasversale che coinvolge tutte le aree aziendali.

La cooperazione con il CFO è essenziale per garantire che le risorse finanziarie siano allocate correttamente per la

protezione dei dati e per l’adozione delle tecnologie necessarie. Il CISO deve anche lavorare a stretto contatto con il CLO per garantire che le politiche di sicurezza siano conformi alle leggi e ai regolamenti vigenti, come il GDPR, e per preparare l’azienda ad affrontare le possibili implicazioni legali in caso di violazioni della sicurezza.

Inoltre, il CISO deve stabilire una comunicazione chiara con il COO per garantire che le operazioni aziendali quotidiane siano supportate da una robusta infrastruttura di sicurezza. Questo include la gestione della continuità operativa, la protezione delle supply chain digitali e la pianificazione per il recupero dopo un disastro.

Un’adeguata sinergia tra il CISO e gli altri dirigenti consente di creare una **gestione olistica del rischio**, dove tutte le aree aziendali lavorano insieme per ridurre e gestire il Cyber risk in modo coerente ed efficace.

Conclusioni

In un contesto sempre più complesso e minaccioso, il CISO svolge un ruolo cruciale nella gestione del rischio informatico. Non solo il CISO è responsabile della protezione delle risorse aziendali e dei dati sensibili, ma è anche il leader che deve integrare la sicurezza nelle decisioni aziendali strategiche e collaborare con altri dirigenti per garantire una gestione di esso.

In qualità di membri attivi della **comunità della cybersecurity**, i CISO lavorano insieme non solo per difendere le proprie organizzazioni dalle minacce digitali, ma anche per sviluppare **strategie proattive** che siano in sintonia con gli obiettivi aziendali e ne favoriscano il raggiungimento.

La valutazione dei rischi, lo sviluppo di strategie di mitigazione e l’integrazione del risk management nella pianificazione strategica aziendale, sono attività

fondamentali per proteggere l’organizzazione dalle minacce informatiche e garantire una crescita sicura e sostenibile nel lungo periodo.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/ciso-gestione-rischio/