Collaborazione tra il CISO e il team IT: la chiave per una sicurezza informatica efficace



Nel mondo digitale odierno, la cyber security non può più essere considerata un compartimento stagno. La collaborazione tra il **Chief Information Security Officer (CISO)** e il **team IT** è diventata un elemento imprescindibile per garantire la resilienza delle organizzazioni contro le minacce sempre più sofisticate. Non si tratta solo di implementare tecnologie avanzate, ma di costruire una sinergia continua che integri le best practice della cybersecurity all'interno delle operazioni quotidiane dell'IT.

La mancanza di una comunicazione efficace tra questi due attori può generare vulnerabilità significative, esponendo le imprese a rischi non necessari. Questo articolo esplora come una collaborazione strategica tra il CISO e il team IT possa rafforzare la postura di sicurezza di un'organizzazione, migliorando la gestione dei processi, la risposta alle minacce e l'integrazione delle politiche di sicurezza nelle operazioni tecnologiche quotidiane.

Sinergia tra CISO, Team IT e Operazioni di Sicurezza Informatica Quotidiane

Sinergia tra sicurezza informatica e operazioni IT quotidiane

Una delle principali sfide nella amministrazione della protezione informatica è far sì che le pratiche di sicurezza

diventino parte integrante delle attività quotidiane dell'IT, senza rallentare i processi o ostacolare l'innovazione. Tradizionalmente, i team IT si sono concentrati sull'efficienza operativa e sulla disponibilità dei sistemi, mentre il CISO si è focalizzato sulla protezione dei dati e sulla gestione del rischio. Tuttavia, in un ambiente sempre più interconnesso, questi obiettivi non possono più essere trattati separatamente.

Qualsiasi strategia di cybersecurity e protezione dati non può prescindere da solidi processi di collaborazione e comunicazione interna.

Costruire una sinergia tra il CISO e il team IT e non solo, significa innanzitutto promuovere una cultura condivisa della sicurezza. Il Chief information deve lavorare a stretto contatto con i responsabili IT per assicurarsi che le decisioni tecnologiche quotidiane, come la gestione delle infrastrutture, delle reti e dei sistemi cloud, siano allineate con i requisiti di protezione dell'organizzazione.

La formazione continua rappresenta un pilastro di questa integrazione. I membri del team IT devono essere formati non solo su come gestire tecnologie e sistemi, ma anche su come riconoscere e mitigare i rischi di protezione. Analogamente, il CISO deve comprendere le sfide operative che il team di tecnici informatici affrontano quotidianamente, in modo da proporre soluzioni di protezione che siano praticabili e non percepite come un ostacolo.

Le riunioni periodiche tra il CISO e il team IT sono fondamentali per mantenere una comunicazione aperta. In questi incontri si dovrebbero discutere non solo le nuove minacce emergenti, ma anche gli aggiornamenti sui progetti IT in corso, permettendo una valutazione continua dei rischi associati. Una collaborazione efficace consente di prevenire i problemi prima che diventino incidenti, creando un ambiente in cui sicurezza e operatività si rafforzano reciprocamente.

Per quanto concerne invece il rapporto tra CIO e CISO, possiamo definirla come una collaborazione imprescindibile. Sebbene i CIO siano responsabili della amministrazione dell'infrastruttura IT di un'azienda, i CISO spesso ricoprono un ruolo ancora più ampio, occupandosi anche della gestione del rischio aziendale, della governance e della conformità normativa. Tradizionalmente, questo è visto come il principale referente per tutte le questioni legate alla sicurezza, ma oggi è sempre più chiaro che da solo non può gestire tutte le sfide.

Negli ultimi anni, l'attività di CIO e CISO si è trasformata profondamente, spinta dalla crescente attenzione verso la tutela e la protezione dei dati. L'approccio più efficace è quello che punta a una strategia di protezione e resilienza integrata, in cui CIO e CISO collaborano strettamente. Dalla costruzione di una rete aziendale sicura alla gestione dell'impatto delle normative sempre più stringenti, le rispettive competenze devono essere coordinate e complementari, evitando sovrapposizioni o contrasti e rafforzando così le misure di protezione, sempre in equilibrio con le esigenze di efficienza operativa.

Un'ulteriore sfida significativa è rappresentata dalle crescenti complessità legate alle normative e alla conformità. In questo contesto, è fondamentale che i team responsabili lavorino in sinergia: il CIO deve assicurare l'aderenza alle normative come il GDPR (General Data Protection Regulation), mentre il CISO deve concentrarsi sulla minimizzazione dei rischi di violazione dei dati. Senza un approccio strategico integrato, risulta difficile ottenere risultati realmente efficaci.

Migliorare la collaborazione tra CIO, CISO e i rispettivi team consente di consolidare una posizione più forte per allineare gli obiettivi IT e di sicurezza con le priorità strategiche dell'azienda. Raggiungere questo livello di integrazione favorisce anche una gestione più efficace della crescente

complessità tecnologica e della continua evoluzione dell'innovazione digitale, oggi sempre più centrale per il successo organizzativo.

Anche il livello di maturità organizzativa può essere determinante per rendere i team dirigenziali più resilienti ai naturali cambiamenti di personale. Considerando che la durata media dell'incarico di CIO e CISO è di circa 3-5 anni, è essenziale integrare processi solidi all'interno delle rispettive aree di competenza, in modo da limitare al massimo eventuali discontinuità strategiche al momento del passaggio di leadership.

L'integrazione dei ruoli di CIO e CISO richiede dunque un'attenta valutazione di diversi fattori, con priorità e livelli di efficacia che possono variare a seconda del contesto aziendale. In ogni caso, le imprese che riconoscono l'importanza di una collaborazione stretta tra queste due figure chiave sono nettamente avvantaggiate nel garantire agilità, sicurezza e prestazioni elevate, qualità sempre più richieste dai Consigli di amministrazione a livello globale.

Implementazione delle politiche di sicurezza dal CISO al team IT

Per ottenere una protezione realmente efficace, le politiche di sicurezza non possono rimanere documenti isolati; devono essere vissute come parte integrante dei processi IT. La collaborazione tra il CISO e il team IT è essenziale per tradurre le politiche in pratiche operative concrete.

Il primo passo è l'integrazione delle policy di tutela già in fase di progettazione dei sistemi. Quando il team IT sviluppa nuove applicazioni o aggiorna le infrastrutture esistenti, il CISO deve essere coinvolto fin dalle fasi iniziali. L'approccio "security by design" consente di costruire sistemi più resilienti, riducendo la necessità di interventi

correttivi successivi, che sono spesso più costosi e complessi.

Le politiche di cyber security di un'azienda devono essere sviluppate su misura per rispondere alle sue specifiche esigenze operative. Possono essere strutturate come un unico documento unificato oppure suddivise in diversi documenti tematici che trattano vari aspetti della sicurezza.

In ogni caso, indipendentemente dalla modalità scelta, tutte le organizzazioni dovrebbero assicurarsi che le loro politiche di tutela contengano alcune informazioni fondamentali. Che siano articolate in documenti separati o raccolte in un'unica policy, una strategia efficace di protezione informatica dovrebbe prevedere:

- **Uso accettabile**: indicazioni su come gli utenti possono utilizzare i sistemi IT aziendali.
- **Gestione del cambiamento**: linee guida sui processi di implementazione, aggiornamento e dismissione delle risorse tecnologiche.
- **Conservazione dei dati**: criteri sulla durata della conservazione dei dati e modalità corrette di eliminazione.
- **Risposta agli incidenti**: procedure operative da seguire in caso di incidenti di sicurezza.
- **Sicurezza della rete**: regole per proteggere l'infrastruttura di rete aziendale.
- **Gestione delle password**: direttive sulla creazione e l'amministrazione sicura delle credenziali utente.
- **Consapevolezza della sicurezza**: programmi formativi per sensibilizzare i dipendenti sui rischi legati alla cybersecurity.

Oltre a questi elementi di base, una politica di sicurezza informatica può essere ampliata con sezioni specifiche che riflettano le particolari necessità e priorità dell'organizzazione.

Un altro aspetto cruciale riguarda la standardizzazione dei processi. Attraverso la collaborazione, il CISO e il team IT possono definire standard tecnici chiari che includano, ad esempio, l'uso obbligatorio di protocolli sicuri, la crittografia dei dati, la gestione sicura delle credenziali e il controllo degli accessi. Questi standard devono essere applicati sistematicamente a tutte le componenti dell'infrastruttura tecnologica.

Inoltre, la collaborazione facilita l'adozione di strumenti di automazione per la sicurezza, come il **provisioning** sicuro degli account utente o la configurazione automatica dei sistemi secondo policy predefinite. Automatizzare la conformità alle policy non solo migliora la protezione, ma riduce anche l'onere operativo sul team IT, liberando risorse per attività più strategiche.

La cyber security non è un processo statico, al contrario richiede un monitoraggio continuo.

Monitorare quindi l'efficacia delle politiche è altrettanto importante. Attraverso audit periodici e sistemi di monitoraggio continuo, il CISO e il team IT possono individuare eventuali deviazioni rispetto alle policy aziendali e correggerle tempestivamente, migliorando progressivamente il livello di maturità della sicurezza informatica dell'organizzazione.

Gestione delle vulnerabilità e delle patch di sicurezza

Uno degli ambiti in cui la collaborazione tra il CISO e il team IT risulta più evidente è nella gestione delle **vulnerabilità**. In un panorama di minacce in costante evoluzione, la capacità di identificare rapidamente le vulnerabilità e applicare le patch di sicurezza è fondamentale per proteggere le risorse aziendali.

La gestione delle vulnerabilità, elemento centrale della gestione del rischio IT, si basa su un’attività continua di individuazione, analisi delle priorità e risoluzione delle debolezze presenti nell’infrastruttura tecnologica e nei software aziendali. Tuttavia, questa funzione, per essere davvero efficace, richiede una stretta collaborazione tra il Chief Information Security Officer (CISO) e il team IT operativo.

Il CISO, in qualità di responsabile della sicurezza a livello strategico, ha il compito di definire le politiche di controllo delle vulnerabilità, stabilendo criteri di valutazione del rischio, priorità di intervento e metodologie di risposta. D’altro canto, è il team IT che possiede la conoscenza pratica dei sistemi, delle configurazioni e delle dinamiche operative quotidiane, elementi indispensabili per applicare in modo tempestivo ed efficace le correzioni necessarie.

In questo rapporto di collaborazione, il CISO fornisce la visione d’insieme, individuando quali vulnerabilità rappresentano minacce concrete per la sicurezza e quali invece possono essere gestite con interventi pianificati, riducendo il pericolo senza compromettere la continuità operativa. Il team IT, a sua volta, è responsabile di implementare materialmente le patch, correggere le configurazioni errate, sostituire componenti obsoleti e monitorare l’effettiva risoluzione delle criticità.

Un aspetto cruciale di questa sinergia riguarda la **prioritizzazione**: non tutte le vulnerabilità devono essere risolte immediatamente, ma è essenziale avere un processo condiviso che consenta di distinguere tra le falle ad alto pericolo, che richiedono un intervento immediato, e quelle a rischio minore, che possono essere gestite in un secondo momento o abbinate a interventi di aggiornamento programmato.

Inoltre, il CISO e il team IT devono collaborare anche nella

comunicazione interna: la gestione delle vulnerabilità non è un'attività isolata, ma coinvolge spesso più dipartimenti. Ad esempio, l'applicazione di una patch critica su un sistema ERP potrebbe richiedere il coordinamento con il dipartimento finance o supply chain. Il CISO deve quindi garantire che ci sia chiarezza sugli impatti di business legati alle operazioni di mitigazione delle vulnerabilità, mentre il team IT deve predisporre procedure di aggiornamento che minimizzino i tempi di inattività.

Infine, la **gestione delle vulnerabilità** in un contesto di collaborazione efficace si basa su strumenti condivisi: soluzioni di **vulnerability scanning**, **sistemi di patch management automatizzati** e **dashboard comuni** che permettano a entrambi i livelli strategico e operativo di avere una visione aggiornata dello stato di rischio dell'organizzazione.

Riassumendo, la gestione delle vulnerabilità non può essere vista come una semplice attività tecnica. Essa è un processo strategico che richiede un'integrazione stretta tra la visione di governance del CISO e l'azione concreta del team IT. Solo attraverso una collaborazione strutturata, basata su obiettivi comuni e strumenti condivisi, le organizzazioni possono davvero mitigare i rischi di sicurezza e assicurare la resilienza del loro ambiente digitale.

È qui che la collaborazione diventa cruciale. Stabilire priorità comuni è il primo passo: non tutte le vulnerabilità possono essere corrette immediatamente; quindi, è necessario valutare il pericolo associato e concentrarsi prima sulle minacce più gravi. Il CISO può fornire una valutazione del pericolo, mentre il team IT può indicare le tempistiche e i potenziali impatti operativi degli aggiornamenti.

Un altro elemento importante sopra anticipato è la creazione di un processo di **patch management** strutturato. La gestione delle patch consiste nell'applicazione degli aggiornamenti forniti dai produttori, con l'obiettivo di correggere

vulnerabilità di sicurezza e migliorare il funzionamento di software e dispositivi. Questo processo è spesso considerato una componente integrante delle attività di gestione delle vulnerabilità.

Questo processo dovrebbe prevedere una fase di test per le patch, al fine di ridurre il rischio di impatti negativi sui sistemi in produzione. Inoltre, è utile programmare finestre regolari di manutenzione, durante le quali applicare aggiornamenti senza compromettere la disponibilità dei servizi critici.

In sostanza, la amministrazione delle patch si basa sulla ricerca di un equilibrio tra la protezione informatica e la continuità operativa dell'azienda. Le vulnerabilità presenti nei sistemi IT possono essere sfruttate dagli hacker per condurre attacchi informatici o diffondere malware. Per contrastare queste minacce, i fornitori rilasciano aggiornamenti correttivi, noti come "patch". Tuttavia, l'applicazione di queste patch può interferire con i processi aziendali, provocando interruzioni e tempi di inattività. L'obiettivo del controllo delle patch è quindi quello di ottimizzare l'applicazione degli aggiornamenti, riducendo al minimo l'impatto sulle attività quotidiane.

La comunicazione costante e la trasparenza tra il CISO e il team IT riducono il rischio di incomprensioni e ritardi, favorendo una gestione più rapida ed efficace delle vulnerabilità. In un contesto in cui i cyber attacchi possono sfruttare falle non corrette nel giro di poche ore, questa collaborazione può fare la differenza tra un'organizzazione sicura e una vulnerabile.

Rilevamento e risposta alle minacce

in tempo reale

In un mondo dove le minacce informatiche possono emergere ed evolversi in pochi minuti, il rilevamento e la risposta in tempo reale sono fondamentali. Nessun sistema è completamente immune dalle minacce; per questo motivo, l'obiettivo non può essere solo prevenire gli attacchi, ma anche rilevarli e reagire il più rapidamente possibile.

Il rilevamento e la risposta alle minacce **(TDR)** sono un processo di cybersecurity per identificare le minacce informatiche alle risorse digitali di un'organizzazione e adottare misure per attenuarle il più rapidamente possibile.

Per affrontare le minacce informatiche e altri problemi legati alla sicurezza, molte organizzazioni istituiscono un **Centro Operativo per la Sicurezza (SOC)**, una struttura o un team centralizzato incaricato di rafforzare la postura di cybersecurity dell'azienda e di gestire la prevenzione, il rilevamento e la risposta agli attacchi informatici. Oltre a monitorare e intervenire su incidenti di sicurezza in tempo reale, il SOC ad esempio tramite Azure Security Center svolge anche attività preventive, finalizzate all'individuazione di nuove minacce emergenti e vulnerabilità che potrebbero compromettere la protezione aziendale. Generalmente, i team SOC, che possono operare internamente o essere esternalizzati, garantiscono la copertura continuativa 24 ore su 24, 7 giorni su 7.

Per individuare e fronteggiare violazioni, tentativi di intrusione o attacchi in corso, il SOC si avvale di tecnologie avanzate e di informazioni provenienti dall'intelligence sulle minacce. Una volta rilevato un pericolo, il personale addetto alla protezione utilizza strumenti specializzati di rilevamento e risposta per neutralizzare o mitigare il rischio.

Il processo di rilevamento e risposta alle minacce si articola

generalmente in diverse fasi operative:

- **Rilevamento**: attraverso strumenti di sicurezza che monitorano costantemente endpoint, identità, reti, applicazioni e ambienti cloud, vengono individuati rischi e possibili violazioni. Gli analisti di sicurezza utilizzano anche tecniche specifiche di threat hunting per scovare minacce particolarmente sofisticate, capaci di sfuggire ai sistemi di difesa tradizionali.
- **Indagine**: una volta segnalato un pericolo, il SOC impiega l'intelligenza artificiale e altre tecnologie analitiche per confermare l'effettiva esistenza della minaccia, analizzare come è avvenuta l'intrusione e identificare gli asset aziendali coinvolti.
- **Contenimento**: per limitare la propagazione dell'attacco, i team di cybersecurity isolano rapidamente dispositivi compromessi, identità violate o segmenti di rete, infatti, impedendo così ulteriori danni alle risorse aziendali.
- **Eliminazione**: l'obiettivo in questa fase è rimuovere definitivamente la causa dell'incidente di sicurezza, eradicando qualsiasi presenza residua dell'attore malevolo e correggendo eventuali vulnerabilità che potrebbero essere nuovamente sfruttate.
- **Ripristino**: una volta verificato che l'ambiente sia stato bonificato e reso sicuro, i sistemi precedentemente isolati vengono reintegrati nella rete aziendale.
- **Report**: a seconda della gravità dell'incidente, il team di sicurezza prepara una documentazione dettagliata, informando i responsabili, la dirigenza e, se necessario, il Consiglio di amministrazione sugli eventi accaduti e sulle azioni correttive adottate.
- **Mitigazione dei rischi**: come fase finale, viene condotta un'analisi approfondita dell'incidente per identificare le misure da implementare allo scopo di rafforzare l'ambiente IT e migliorare le procedure di risposta

futura, riducendo così la probabilità di eventi simili.

Il CISO, insieme al team IT, deve costruire una strategia di rilevamento che sfrutti soluzioni come i sistemi di **Intrusion Detection (IDS)**, le piattaforme **SIEM (Security Information and Event Management)** e i sistemi di monitoraggio comportamentale basati su intelligenza artificiale. Tuttavia, la tecnologia da sola non basta: serve anche una collaborazione umana efficace.

Il team IT deve essere coinvolto nella configurazione e nella gestione degli strumenti di rilevamento, garantendo che siano adeguatamente integrati nei sistemi aziendali. Parallelamente, il CISO deve fornire indicazioni su quali tipi di eventi monitorare e come interpretarli correttamente per individuare segnali di compromissione.

Quando una minaccia viene rilevata, la rapidità della risposta è determinante. La collaborazione pregressa tra il CISO e il team IT permette di attivare procedure di risposta già testate e conosciute da entrambi. Ad esempio, può essere necessario isolare rapidamente una macchina compromessa, applicare regole firewall ad hoc o modificare configurazioni di rete per contenere un attacco.

La gestione efficace degli incidenti richiede anche esercitazioni periodiche congiunte. Simulare scenari di attacco realistici consente di testare le capacità di risposta, identificare eventuali lacune e migliorare continuamente la prontezza operativa.

Infine, la fase post-incidente è altrettanto importante: una volta contenuta una minaccia, il CISO e il team IT devono analizzare insieme l’accaduto per capire cosa è andato storto e come rafforzare ulteriormente le difese. Questo approccio orientato al miglioramento continuo contribuisce a rendere l’organizzazione sempre più resiliente.

Conclusioni

La collaborazione tra il CISO e il team IT non è solo auspicabile, è ormai una necessità critica. La sicurezza informatica deve permeare ogni aspetto delle operazioni IT, dalla progettazione dei sistemi alla gestione delle vulnerabilità, fino al rilevamento e risposta agli incidenti. Solo attraverso una comunicazione aperta, una comprensione reciproca delle sfide e la costruzione di processi integrati sarà possibile affrontare efficacemente il panorama di minacce in continua evoluzione.

Investire in questa collaborazione significa costruire fondamenta solide non solo per la sicurezza, ma per la continuità e il successo dell’intera organizzazione.

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