

La comunicazione efficace tra il CISO e il top management



In un contesto aziendale sempre più digitalizzato e interconnesso, la sicurezza informatica è diventata un pilastro strategico. Tuttavia, il valore di una solida postura di cybersecurity dipende non solo dalla tecnologia impiegata, ma anche e soprattutto dalla capacità del **Chief Information Security Officer** (CISO) di comunicare efficacemente con il top management. Il dialogo tra chi si occupa della sicurezza e chi guida le decisioni aziendali è fondamentale per assicurare un'adeguata protezione degli asset digitali, garantendo al contempo la continuità operativa e la crescita dell'organizzazione.

Il CISO si trova oggi nella posizione delicata di dover tradurre concetti tecnici complessi in informazioni strategiche accessibili al Consiglio di amministrazione (CDA) e agli executive. Questo richiede non solo competenze tecniche, ma anche un'elevata intelligenza comunicativa e una visione orientata al business.

Importanza della reportistica sulla sicurezza informatica: come il CISO comunica i rischi al CDA

Una delle principali sfide nella comunicazione tra il Chief Information Security Officer e i vertici aziendali riguarda la reportistica. Fornire rapporti chiari, sintetici e significativi è essenziale per ottenere l'attenzione e il supporto del vertice aziendale.

Negli ultimi anni, l'attenzione crescente verso la cybersecurity ha rappresentato un valido supporto per i CISO

nel costruire un resoconto più efficace. Questo contesto favorevole consente loro di illustrare con maggiore chiarezza al CDA i punti di vulnerabilità dell'azienda, i limiti attuali dei controlli di protezione implementati e le aree in cui le infrastrutture e le informazioni aziendali risultano esposte ai rischi.

È in questo contesto che il report assume un ruolo strategico. Il Chief Information Security Officer deve saper costruire report periodici che offrano una panoramica aggiornata del panorama delle minacce, dello stato della sicurezza aziendale e delle iniziative in corso. Ogni informazione deve essere orientata a rispondere alla domanda: "Come questo influisce sul business?"

Un buon report di sicurezza non si limita a elencare gli eventi di pericolo rilevati o le vulnerabilità individuate. Deve collegare questi elementi a metriche di rischio, impatto economico potenziale e priorità aziendali. Ad esempio, la segnalazione di un aumento degli attacchi ransomware ha maggiore efficacia se accompagnata da un'analisi del potenziale **downtime** dei sistemi critici e delle implicazioni legali o regolatorie per l'organizzazione.

Quali sono, dunque, le informazioni fondamentali da sottoporre all'attenzione del Consiglio di amministrazione e qual è l'approccio più efficace per farlo?

Non esiste una risposta univoca, e questo per almeno tre motivi rilevanti:

In primo luogo, ogni CDA è unico, perché riflette non solo il tipo di prodotti e servizi offerti dall'azienda, ma anche – e soprattutto – le caratteristiche delle persone che lo compongono. La struttura stessa del Board può variare sensibilmente da un'organizzazione all'altra, rendendo necessario un adattamento su misura del report da parte dei CISO;

In secondo luogo, in base alla dimensione e alla complessità dell'impresa, alcune aree di responsabilità potrebbero non ricadere direttamente sul Chief Information Security Officer. In molte realtà aziendali, infatti, entrano in gioco altre figure chiave come il Risk Manager, il Data Protection Officer (DPO) o l'Internal Auditor, che condividono o presidiano specifici ambiti della sicurezza.

Infine, il settore di appartenenza influisce sulla rilevanza di determinati temi all'interno del reporting. Alcuni aspetti, come ad esempio la "tutela dei prodotti", potrebbero essere irrilevanti per aziende di servizi o consulenza, mentre risultano centrali in ambiti industriali o tecnologici.

L'adozione di framework riconosciuti come il NIST Cybersecurity Framework o ISO/IEC 27001 può fornire una base strutturata per la reportistica, facilitando la comunicazione anche con interlocutori non tecnici. L'obiettivo non è semplicemente "informare", ma influenzare le decisioni strategiche attraverso una narrazione basata sui dati.

In generale, comunque, ad alto livello, le informazioni da condividere sono comunemente individuabili. Ne riportiamo le principali.

Conformità a normative e adozione di framework di sicurezza

È fondamentale che il Chief Information Security Officer informi il CDA sullo stato di conformità dell'azienda alle normative in ambito sicurezza (come il GDPR), evidenziando sia il livello raggiunto sia le aree che richiedono miglioramenti. Devono inoltre essere segnalati eventuali aggiornamenti normativi rilevanti.

Parallelamente, va illustrato quali standard e framework di sicurezza sono stati adottati come ISO 27001, NIST, CIS

Controls o il Framework Nazionale e le motivazioni alla base di tali scelte. Il Chief Information Security Officer ha il compito di aggiornare regolarmente il Board sul grado di implementazione, sull'efficacia dei controlli introdotti e sui meccanismi messi in atto per monitorarne l'aderenza e l'impatto sulla postura di sicurezza dell'organizzazione.

Minacce informatiche e trend emergenti

Per consentire al CDA di comprendere meglio il contesto dinamico in cui si muove l'azienda, è fondamentale offrire una visione chiara delle principali minacce informatiche in atto e delle tendenze emergenti nel panorama cyber.

Negli ultimi anni, uno strumento prezioso a disposizione dei CISO in questo ambito è stato la **Threat Intelligence**. Questo tipo di analisi, diventata ormai un pilastro della difesa informatica, consente di raccogliere informazioni dettagliate da fonti open source o servizi professionali su chi sono gli attori malevoli e quali tecniche utilizzano per portare avanti gli attacchi.

Tuttavia, questi dati, per essere davvero utili al Board, devono essere rielaborati in chiave strategica. Il compito del Chief Information Security Officer è quindi quello di tradurre contenuti altamente tecnici in un linguaggio accessibile, offrendo una sintesi visiva e concisa dello scenario globale delle minacce. Supporti come infografiche o dashboard possono aiutare a rappresentare meglio i rischi potenziali e a spiegare in che modo questo trend potrebbero avere un impatto concreto sull'organizzazione.

Incidenti di sicurezza recenti

Nel presentare al Consiglio di amministrazione gli incidenti di sicurezza rilevanti accaduti nel periodo di riferimento, è

fondamentale adottare un approccio equilibrato e costruttivo. Il Chief Information Security Officer deve fornire una panoramica chiara dei principali eventi, spiegando la natura degli incidenti, il loro impatto sull'organizzazione e le misure adottate per contenerli e risolverli.

Oltre alla descrizione tecnica, è essenziale chiarire le cause alla base degli incidenti, anche quando si sono verificati nonostante i controlli esistenti. Questo passaggio consente di dimostrare al Board che l'azienda è in grado di analizzare criticamente le proprie vulnerabilità e che ha già messo in atto azioni correttive per prevenire eventi simili in futuro.

Il tono della comunicazione deve restare focalizzato sul miglioramento continuo, evitando accuse o colpe individuali. L'obiettivo è mostrare un'organizzazione matura, trasparente e orientata all'apprendimento, capace di trasformare ogni incidente in un'opportunità per rafforzare la propria postura di sicurezza. In questo modo, si trasmette al consiglio la certezza che la protezione dei dati e dei sistemi è una priorità costante, affrontata con responsabilità e visione strategica.

Presentazione dei dati di rischio in modo comprensibile

La gestione del rischio è uno degli aspetti centrali della cybersecurity. Tuttavia, il modo in cui i dati dello stesso vengono presentati fa spesso la differenza tra una decisione consapevole e una sottovalutazione del problema. Il CISO deve agire come un "traduttore" tra il linguaggio tecnico degli analisti e quello finanziario o operativo dei dirigenti.

I membri del CDA raramente sono esperti in cyber security e, spesso, non hanno il tempo o l'interesse per approfondire dettagli troppo tecnici. Tuttavia, sono pienamente consapevoli del potenziale impatto che un incidente di sicurezza può avere

su reputazione, conformità normativa e performance finanziaria.

È chiaro che una comunicazione realmente efficace deve considerare il punto di vista del Consiglio di amministrazione in merito alla questione trattata. Per catturare l'attenzione del Board e risultare davvero incisivi, è fondamentale inquadrare i temi legati alla cybersecurity all'interno del più ampio scenario degli obiettivi strategici dell'azienda.

Lo scopo della traduzione "dalla tecnologia al business" è individuare quei fattori tecnici che potrebbero causare un'interruzione dei servizi e metterli in relazione con gli obiettivi aziendali, in modo da presentarli al Board come rischi strategici rilevanti per il successo dell'organizzazione.

È fondamentale saper quantificare il rischio in termini comprensibili: probabilità, impatto e costi. Utilizzare modelli di risk scoring e heat map può aiutare a rappresentare graficamente la situazione, rendendo evidenti le aree di maggiore esposizione. Tuttavia, la rappresentazione grafica deve essere sempre accompagnata da una spiegazione semplice e diretta, evitando gergo tecnico e acronimi.

La comunicazione delle minacce deve inoltre essere personalizzata in base all'interlocutore. Il CFO, ad esempio, sarà interessato agli aspetti finanziari e assicurativi della sicurezza, mentre il CIO potrebbe focalizzarsi sull'impatto operativo. Al contrario, il CEO o il CDA vorranno una sintesi chiara: quali rischi sono accettabili, quali devono essere mitigati e quali richiedono investimenti immediati.

È importante anche spiegare la differenza tra rischio residuo, rischio trasferito (es. tramite assicurazioni) e rischio mitigato, in modo che la direzione esecutiva possa prendere decisioni strategiche ben informate. Il Chief Information Security Officer deve costruire una narrazione che leghi ogni

pericolo a uno specifico impatto sull'organizzazione, mostrando come la cyber security sia un fattore abilitante per il business, e non un costo da limitare.

Indipendentemente dal tipo di informazioni trattate nel report del CISO, per renderle più chiare e incisive è essenziale accompagnarle con metriche e dashboard. Questi strumenti permettono di quantificare l'efficacia delle strategie di cybersecurity, evidenziare i miglioramenti ottenuti e dimostrare che le decisioni sono supportate da dati concreti.

Organizzare le metriche in tre categorie:

Key Risk Indicators (KRI) per l'identificazione dei rischi, **Key Performance Indicators** (KPI) per valutare i risultati raggiunti, e **Key Control Indicators** (KCI) per verificare l'efficacia dei controlli, aiuta a fornire al Board una visione strutturata e completa dello stato della protezione aziendale.

Inoltre, ogni sezione del report dovrebbe includere una panoramica sui piani futuri e le iniziative strategiche. Questo spazio è fondamentale per evidenziare l'approccio proattivo dell'azienda nella gestione della sicurezza e nel rispondere alle minacce emergenti.

Vanno quindi illustrati i programmi di miglioramento, la formazione del personale, le simulazioni di incidenti e l'adozione di nuove tecnologie, insieme alle risorse economiche, umane e tecniche necessarie per realizzarli. È importante sottolineare come queste iniziative siano allineate agli scopi dell'azienda e contribuiscano concretamente al successo complessivo dell'impresa, rafforzando la fiducia dei clienti, la reputazione del brand e la continuità operativa.

Strategie per allineare le priorità

di sicurezza con gli obiettivi aziendali

Una delle principali cause di incomprensioni tra il CISO e il management è la mancata armonizzazione tra le priorità della cyber security e gli obiettivi di business.

Nel presentare i risultati delle valutazioni di rischio al CDA, l'obiettivo principale è comunicare chiaramente i rischi identificati, le misure di mitigazione adottate e la strategia complessiva per la gestione dei rischi informatici.

Quando la cybersecurity viene percepita come un freno all'innovazione o un ostacolo all'agilità operativa, il rischio è che le iniziative di protezione vengano messe in secondo piano o che vengano considerati solo gli aspetti minimi necessari alla compliance.

Per superare questo ostacolo, il CISO deve dimostrare che la sicurezza è un valore strategico che protegge la capacità dell'azienda di crescere, innovare e mantenere la fiducia del mercato. Ciò implica un profondo allineamento tra il piano strategico aziendale e le iniziative di cybersecurity.

È consigliabile presentare una sintesi delle più recenti valutazioni del rischio, chiarendo il metodo utilizzato per individuare le minacce e stimarne la probabilità e l'impatto, magari attraverso l'impiego di scale di classificazione che rendano più chiara la comprensione dei livelli di pericolo.

È utile inoltre descrivere le misure di mitigazione già adottate, valutandone l'efficacia nel contenere i rischi, e supportare il tutto con dati concreti, ad esempio, tassi di successo di specifici controlli per dimostrare il valore reale delle azioni intraprese.

Infine, è importante segnalare i rischi ancora parzialmente irrisolti, illustrando le iniziative in atto o pianificate per

affrontarli. Questo può includere l'introduzione di nuovi controlli, l'assegnazione di ulteriori risorse o l'elaborazione di strategie alternative per una gestione più efficace delle minacce residue.

Una strategia efficace è quella di partecipare attivamente ai tavoli decisionali che definiscono le roadmap digitali e tecnologiche, proponendo soluzioni di protezione già in fase di progettazione. In questo modo, la protezione non è più un'aggiunta tardiva e costosa, ma una componente integrata nei processi di trasformazione digitale.

Inoltre, il Chief Information Security Officer deve essere in grado di comunicare il ROI (Return on Investment) della sicurezza. Questo non significa solo quantificare i risparmi derivanti dalla prevenzione di incidenti, ma anche evidenziare come un buon livello di cybersecurity può facilitare l'accesso a nuovi mercati, attrarre clienti sensibili alla protezione dei dati, migliorare la reputazione aziendale o soddisfare requisiti contrattuali sempre più stringenti.

L'approccio **DevSecOps** deriva dalla combinazione di **Development (sviluppo)**, **Security (sicurezza)** e **Operations (operazioni)**, con l'intento di creare una cultura e una pratica che metta la sicurezza al centro dell'intero processo di sviluppo e distribuzione del software, o l'adozione di principi Zero Trust, possono diventare esempi concreti di come le priorità di tutela possano rafforzare e non ostacolare l'efficienza operativa e la capacità innovativa.

Gestione delle aspettative del CDA riguardo alla cybersecurity

Il Consiglio di amministrazione gioca un ruolo cruciale nella definizione delle priorità aziendali e nell'allocazione delle risorse. Tuttavia, le aspettative del CDA nei confronti della tutela informatica sono spesso irrealistiche o poco allineate

alla realtà operativa.

Il Chief Information Security Officer ha il compito delicato di istruire il CDA, gestendo le aspettative in modo realistico ma rassicurante. È necessario spiegare che il rischio zero non esiste, ma che esistono strategie per ridurlo ad un livello accettabile. Occorre chiarire che ogni decisione in materia di protezione è anche una decisione di business: ogni controllo aggiuntivo può comportare costi, ma anche benefici in termini di resilienza e fiducia.

La gestione delle aspettative richiede trasparenza, ma anche equilibrio. Non bisogna minimizzare le minacce, ma nemmeno creare allarmismo inutile. È utile comunicare con regolarità, utilizzando momenti strutturati (es. board meeting trimestrali) per aggiornare il CDA sulle principali tendenze di rischio, sugli incidenti evitati o gestiti, e sulle priorità per il periodo successivo.

Un'altra strategia efficace è il ricorso a simulazioni di crisi o **tabletop exercise**, in cui il CDA partecipa attivamente a scenari ipotetici di attacco informatico. Questo tipo di esperienza diretta aiuta i decisori a comprendere le implicazioni reali di una violazione, a prendere familiarità con le dinamiche della risposta agli incidenti e a sostenere più convintamente gli investimenti in sicurezza.

Infine, il CISO dovrebbe costruire relazioni personali con i membri chiave del CDA, identificando **alleati interni** con cui condividere obiettivi e visione strategica. Questo favorisce un clima di fiducia e collaborazione che rende la cybersecurity un tema condiviso, e non un problema tecnico da delegare.

Conclusione

La comunicazione tra il Chief Information Security Officer e i manager aziendali non può più essere unidirezionale o

episodica. Deve essere un processo continuo, bidirezionale e strategico. Solo attraverso una comunicazione efficace è possibile costruire una cultura aziendale resiliente, in cui la cyber security è percepita come parte integrante del successo dell'organizzazione.

Un buon reporting permetterà di fornire una risposta che si basi sull'impegno continuo dei CISO, e quindi dell'azienda, nel monitorare, migliorare e adattare le iniziative di sicurezza per affrontare le minacce emergenti.

Il Chief Information Security Officer moderno non è più (solo) un tecnico, ma un leader capace di parlare il linguaggio del business, di educare e influenzare, di orientare le scelte strategiche verso un equilibrio tra rischio e opportunità. In questo equilibrio, la comunicazione è lo strumento chiave per garantire che la sicurezza sia non solo compresa, ma anche sostenuta e integrata nei processi decisionali dell'intera organizzazione.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/ciso-top-management/>