proofpoint.

EBOOK

Parametri che contano:

La guida del CISO per valutare, dare priorità e giustificare i budget della sicurezza informatica

proofpoint.com/it

SEZIONE 1

Da capro espiatorio a stratega

Per comprendere quanto il ruolo del CISO si sia evoluto negli ultimi anni, prendiamo in considerazione la testimonianza di un dirigente in una recente tavola rotonda di Proofpoint.

"Quando ho iniziato a lavorare nel settore, il ruolo del CISO tendeva ad essere quello del capro espiatorio", ha ricordato. Il team dirigenziale aveva bisogno di qualcuno da incolpare se le cose andavano male. Ma il più delle volte hanno dato la priorità a polizze assicurative generiche rispetto a investimenti nei team e in soluzioni di sicurezza. In altre parole, ha detto, i CISO erano esperti di tecnologia con risorse limitate.

Ma la situazione sta cambiando. Le minacce sono diventate sempre più complesse e possono colpire molto più di pochi sistemi limitati all'interno di un'azienda. E quando gli attacchi informatici si trasformano in violazioni di dati su larga scala, possono rapidamente danneggiare o distruggere un marchio.

Ciò ha cambiato il modo in cui il team dirigenziale considera gli investimenti in sicurezza informatica e il ruolo del CISO. Il consiglio di amministrazione dedica molta più attenzione all'attività dei CISO che vengono sempre più coinvolti nella strategia complessiva dell'azienda. Sempre più spesso aiutano a guidare il processo di trasformazione digitale in modo da gestire i rischi, ottimizzare i processi aziendali e ridurre le perdite evitabili.

"Quando ho iniziato a lavorare nel settore, il ruolo del CISO tendeva ad essere quello del capro espiatorio."

Nuove sfide portano nuovi costi

Questa evoluzione porta a nuove esigenze in termini di budget. Secondo un recente studio Forrester, il 60% dei responsabili delle decisioni aziendali in materia di sicurezza ha aumentato i budget di sicurezza nel 2020[1].

E quelli che non li hanno aumentati cercano di sfruttare al massimo i loro fondi. I budget per la sicurezza informatica oggi devono coprire molte sfide:

- Evoluzione di normative e requisiti
- Migrazione progressiva al cloud
- Passaggio repentino a modelli di lavoro ibridi e di telelavoro
- Evoluzione del panorama delle minacce

Prepararsi per il futuro

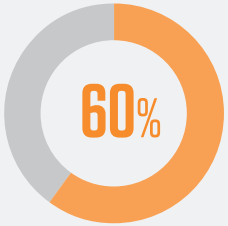
Mentre i CISO si adattano a questi cambiamenti, molti si aspettano che i budget continuino ad aumentare (in media dell'11%) per poter affrontare le sfide future.

Quasi due terzi (65%) ritengono che saranno in grado di affrontare meglio un attacco informatico e riprendersi di conseguenza entro il 2023[2].

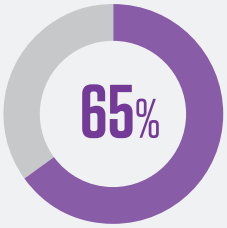
Tuttavia, il livello di preparazione rimane una delle principali preoccupazioni. Sebbene i leader aziendali esprimano ottimismo in merito alla loro capacità di affrontare e riprendersi dagli attacchi nel medio termine, sembrano meno fiduciosi nelle loro attuali capacità. Il nostro report Voice of the CISO 2021 ha rilevato che il 66% dei CISO ritiene che le loro aziende sono impreparate a far fronte a un attacco informatico mirato[3].

In ogni caso, il nuovo perimetro è costituito dai dipendenti, non dalle tecnologie di rete. Inoltre, l'adozione di nuovi modelli di lavoro (ibrido o telelavoro a tempo pieno) non fa che aggiungere sfide e complessità alla sicurezza.

In qualità di responsabile della sicurezza, puoi gestire il tuo budget per gestire meglio questi cambiamenti. Questo eBook delinea le migliori pratiche per valutare il rischio, stabilire la tolleranza al rischio della tua azienda, valutare la tua attuale soluzione, dare priorità alla spesa e giustificare il tuo budget al consiglio di amministrazione.



dei responsabili della sicurezza aziendale ha aumentato il budget per la sicurezza nel 2020



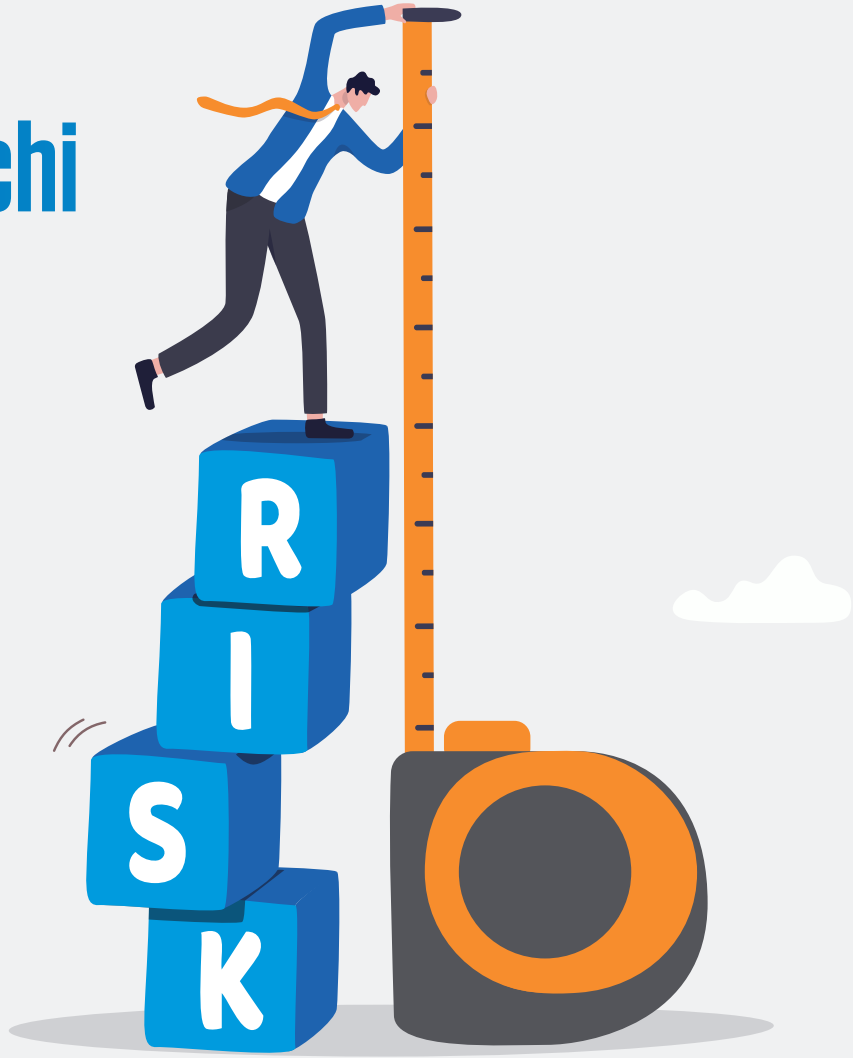
dei CISO ritiene che sarà in grado di affrontare meglio un attacco informatico e riprendersi di conseguenza entro il 2023

incremento previsto dei budget per soddisfare le sfide future

1 Forrester. "Global Security Budgets in 2021." (Budget complessivi per la sicurezza nel 2021), agosto 2021.
2 Proofpoint. "Voice of the CISO.", maggio 2021.
3 Proofpoint. "Voice of the CISO.", maggio 2021.

SEZIONE 2

Valutazione della tolleranza ai rischi



In primo luogo, valuta la tua esposizione alle minacce e la tua tolleranza ai rischi utilizzando un framework adatto alla tua azienda. Sono disponibili numerosi framework per aiutarti a farlo. Quando si discute di questi argomenti con la dirigenza e i membri del consiglio, assicurati di menzionare il framework che stai utilizzando e le motivazioni.

Una questione di numeri

Quantificare i rischi non è una scienza esatta e può essere complesso. Tuttavia, prendersi il tempo per quantificare i rischi e la propria tolleranza al rischio aiuterà a giustificare il budget in seguito. I rischi possono anche essere analizzati in termini qualitativi, ma i parametri monetari saranno meglio compresi da dirigenti e membri del consiglio.

È anche importante che tutte le parti interessate siano sulla stessa lunghezza d'onda. La tolleranza ai rischi che i leader aziendali esprimono durante la fase di pianificazione potrebbe non corrispondere sempre alla loro tolleranza reale. Considera la possibilità di tracciare scenari realistici con i dirigenti e i membri del consiglio per assicurarti di definire la reale propensione al rischio della tua azienda.

Principali framework per la sicurezza informatica

National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Il NIST, una divisione del Dipartimento del Commercio degli Stati Uniti, fornisce indicazioni sulla gestione dei rischi di sicurezza informatica e sul miglioramento delle comunicazioni interne ed esterne in materia di sicurezza informatica.

NISTIR 8286: Identificazione e valutazione dei rischi di sicurezza informatica per la gestione dei rischi aziendali

Questo documento si concentra sulla gestione dei rischi di sicurezza informatica a livello aziendale nel contesto della missione e degli obiettivi aziendali.

People-Centric Security Framework (PCSF)

Sviluppato da Proofpoint secondo un processo trasparente e fondato sul consenso che ha coinvolto parti interessate pubbliche e private, questo framework mira a promuovere le best practice in termini di rischio umano e ad aiutare le azienda a proteggere la riservatezza, l'integrità e la disponibilità dei loro ambienti.

SEZIONE 3

Gestione dei rischi

Una volta definita la tua esposizione alle minacce e la tolleranza ai rischi, devi valutare le tue protezioni attuali contro queste minacce.

Uno sguardo oltre le tecnologie

Potresti essere tentato di farlo attraverso la lente del tuo stack tecnologico esistente.

Tutti hanno familiarità con gli indicatori chiave di prestazione operativa, come il tempo di rilevamento, il tempo di risposta e il tempo per applicare le misure correttive.

Questi indicatori sono utili per generare report di basso livello e per comprendere le prestazioni quotidiane di soluzioni specifiche implementate. Ma non lo sono affatto per valutare e comunicare la tua posizione complessiva rispetto ai rischi di alto livello e alle priorità aziendali.

Modellazione delle minacce

Quando pianifichi un budget, prevedi di utilizzare un approccio di modellazione delle minacce per valutare gli indicatori chiave di rischio della tua azienda e le tue prestazioni rispetto ad essi. La modellazione delle minacce è un processo per l'identificazione delle minacce e del modo in cui si verificano per poi dare priorità alle misure di mitigazione di conseguenza. A differenza degli indicatori chiave specifici per le soluzioni, la modellazione delle minacce ti permette di avere una visione complessiva dei rischi per la tua azienda e di identificare le falle nella tua protezione.

La modellazione delle minacce ti aiuterà a identificare le misure efficaci, dove sono necessari maggiori investimenti e dove potrebbe essere accettabile un rischio residuo. In questo modo è possibile valutare una vasta gamma di rischi. Eccone alcuni da prendere in considerazione.

Modellazione delle minacce in azione

Ecco un esempio di come funziona in pratica la modellazione delle minacce. Consideriamo i rischi legati al mancato rispetto delle normative. Uno scenario che può portare a questo tipo di rischi è quello della perdita di dati, che può avvenire tramite diversi vettori di minaccia, tra cui:

- Perdita di dati dell'email
- Trasferimento nel cloud
- Salvataggio di dati su un disco locale
- Utilizzo di supporti rimovibili
- Trasferimento di dati in una zona non protetta
- Utilizzo di un sito per la condivisione di file esterno
- Taglia e incolla manuale
- Vulnerabilità nelle applicazioni

Nel momento in cui delinei ognuno di questi vettori per la perdita di dati, puoi valutare il tuo livello di protezione e decidere come affrontare le lacune.

Se passi direttamente alla valutazione delle prestazioni di tecnologie specifiche, come una soluzione CASB (Cloud Access Security Broker), un agent di protezione degli endpoint o una rete privata virtuale (VPN), rischi di trascurare le lacune nella copertura dei vettori di perdita di dati che questi prodotti non coprono.

Utilizzando un approccio di modellazione dei dati per valutare gli indicatori chiave di rischio, puoi delineare un quadro più completo e strategico del livello di preparazione della tua azienda ad affrontare i vari rischi.

SEZIONE 4

Scelta delle soluzioni

Puoi quindi utilizzare la tua valutazione della tolleranza al rischio e la tua analisi degli indicatori chiave di rischio per identificare le principali aree che necessitano di nuovi investimenti per la tua azienda.

In fase di valutazione di soluzioni specifiche per soddisfare queste esigenze, poniti le seguenti domande:

- La soluzione mitiga un rischio?
- La soluzione risolve un problema aziendale?
- La soluzione aiuta a migliorare l'attività aziendale? (Permette l'adozione di nuovi strumenti o processi)
- La soluzione aiuta a semplificare e ottimizzare le operazioni di sicurezza?
- La soluzione è in linea con gli obiettivi e la tolleranza ai rischi dell'azienda?

Puoi, e dovresti, porti le stesse domande anche per le soluzioni esistenti. Prima di continuare a investire in una tecnologia particolare, assicurati che soddisfi ancora le tue esigenze.

Quantificazione del ritorno sugli investimenti

Per giustificare i tuoi investimenti - e il budget necessario per supportarli - al consiglio di amministrazione devi quantificare il ritorno sull'investimento per ogni soluzione.

Non è sempre semplice quantificare il ritorno sull'investimento in soluzioni di sicurezza, ma può semplificare molto il sostegno da parte del team dirigenziale. Puoi farlo soppesando i vantaggi della soluzione rispetto al suo costo.

Assicurati di analizzare i costi nascosti di una soluzione, come i seguenti:

Hardware

Implementazione

Software

Gestione costante

Per ogni soluzione, confronta il costo con i vantaggi, tra cui la riduzione dei rischi e l'efficienza della forza lavoro. Conviene anche presentare l'opzione che consiste nel non fare nulla dettagliando l'esposizione alle minacce e facendo degli esempi.

Per esempio, se scegliessi di non ridurre l'impatto del ransomware o del malware, i costi potenziali potrebbero includere:

- Interruzione delle attività
- Perdita di produttività dell'utente finale
- Tempo dedicato all'analisi delle minacce e alla creazione di report
- Tempo trascorso a neutralizzare le minacce
- Tempo dedicato all'esecuzione manuale di compiti come la cancellazione di messaggi da una casella email o la risposta ai messaggi di phishing segnalati

Documentazione dei rischi residui

Assicurati di identificare la tua assicurazione contro i rischi informatici e il rischio residuo, ovvero l'esposizione alle minacce che sussiste dopo i tuoi investimenti. È praticamente impossibile portare la tua azienda a rischio zero e, se fosse possibile, probabilmente non ne varrebbe la pena. Nonostante ciò dovresti assicurarti che il tuo rischio residuo rientri nel livello di tolleranza ai rischi della tua azienda.

SEZIONE 5

Calcolo e comunicazione dei requisiti in termini di budget

Una volta determinate le tue esigenze di budget e le aree di investimento, devi comunicarli in modo convincente alla dirigenza e ai membri del consiglio di amministrazione. Probabilmente avrai diversi tipi di pubblico, tra cui:

- Il consiglio d'amministrazione
- I responsabili operativi, come il COO (Chief Operating Officer) o il CIO (Chief Information Officer)
- I responsabili finanziari, come il CFO (Chief Financial Officer)

Personalizzazione del messaggio

È consigliato adattare il business case dei tuoi investimenti in sicurezza a ogni pubblico di riferimento. Concentrati sull'impatto sulle aree dell'azienda che ognuno di loro supervisiona. È un po' come dire la stessa cosa in tre lingue diverse:

- **Il consiglio d'amministrazione:** quando ti rivolgi al consiglio, sottolinea come il piano soddisfi la tolleranza al rischio dell'azienda e identifica il rischio residuo che l'azienda è disposta ad accettare.
- **I responsabili operativi:** quando parli al COO o al CIO, enfatizza il lato operativo del tuo messaggio. Concentrati sulle lacune, sulle vulnerabilità rimanenti e su come il tuo piano compenserà i rischi per le operazioni aziendali.
- **I responsabili finanziari:** con il CFO, evidenzia come hai bilanciato le spese o come prevedi di risolvere le aree non equilibrate.

Qualunque sia il pubblico, comunica il ritorno sull'investimento delle soluzioni che hai quantificato durante la fase di pianificazione. Aiutali a capire cosa sta ottenendo l'azienda per i soldi che stai spendendo.

Ritorno sull'investimento decrescente

Preparati a spiegare il concetto di "ritorno sull'investimento decrescente". Potresti dover dedicare la stessa quantità di denaro ai problemi importanti ed evidenti e ai problemi più piccoli e meno evidenti che sono altrettanto critici. Una minaccia apparentemente "minore" può esporre l'azienda a un rischio significativo, come una violazione dei dati, giustificando spese consistenti per compensarla. Di nuovo, puoi far riferimento ai tuoi calcoli del ritorno sull'investimento per mettere il costo della soluzione in relazione con il rischio che riduce.

SEZIONE 6

Gestione delle esigenze fuori ciclo

Il processo di pianificazione del budget segue un ciclo annuale o trimestrale. Tuttavia, è inevitabile che sorgano dei problemi al di fuori del ciclo standard, come delle minacce emergenti o nuove tattiche utilizzate dai criminali informatici. Gli incidenti imprevisti sono praticamente impossibili da evitare, ma possono essere l'occasione per rivalutare il tuo livello di sicurezza e ripensare le tue priorità in materia di spese.

Costi nascosti

Non dimenticare di prendere in considerazione tutti i costi associati ad ogni soluzione che implementi. La maggior parte delle aziende prevede un budget per le licenze. Ma molte dimenticano di prendere in considerazione il costo della manutenzione o delle risorse umane necessarie per la soluzione. Tieni conto di questi "costi nascosti" nella fase di pianificazione per evitare di essere preso alla sprovvista.

SEZIONE 7

Accelerazione del processo

La pianificazione del budget può dimostrarsi un processo lento e laborioso. Tuttavia, ci sono dei modi per accelerare e facilitare il processo.

Approccio strategico

In primo luogo, abbraccia pienamente il tuo ruolo di partner strategico e ricorda che il ruolo stesso del CISO sta cambiando. Identifica gli obiettivi delle varie parti interessate e aiutale a raggiungerli con un rischio minimo.

Guarda oltre le operazioni e la leadership tecnica e considera come puoi aiutare l'azienda a guidare la trasformazione digitale e a conseguire gli obiettivi aziendali.

Equilibrio tra rischio e produttività

Ricorda che non puoi eliminare completamente il rischio. Come professionista della sicurezza, puoi forse preferire un approccio prudente relativamente alla tolleranza ai rischi, ma il consiglio di amministrazione e altri dirigenti vorranno trovare un equilibrio tra l'esposizione alle minacce e gli obiettivi aziendali. Per esempio, il tuo gateway email può essere efficace al 99,1%. Ma basta una sola email per subire un attacco ransomware, lasciando un rischio residuo pari allo 0,9%. Questo rischio residuo viene solitamente affrontato con l'aggiunta di ulteriori livelli di sicurezza come l'isolamento o la prevenzione della perdita dei dati (DLP). Tuttavia, tutte le parti coinvolte devono comprendere che non esiste il rischio zero.

Trova un terreno comune e cerca di evitare di diventare il "dipartimento che dice no". Il tuo budget e i tuoi piani dovrebbero bilanciare il rischio rispetto alle priorità dell'azienda e ridurre al minimo l'esposizione alle minacce entro la tolleranza al rischio dell'azienda.

Aspettative adeguate

Infine, modera le aspettative man mano che procedi. La maggior parte dei dipartimenti di un'azienda opera su un modello di produzione, dove risultati e ritorni elevati sono indicatori chiave di prestazione. Al contrario, la sicurezza informatica opera secondo un modello di resilienza.

Proprio come i vigili del fuoco sono pagati sia che ci sia un incendio o meno, la sicurezza informatica richiede un budget che non sempre si traduce in un ritorno più elevato. Ma nessuno sosterrà che i vigili del fuoco sono inutili. È tuo compito aiutare le altri parti coinvolte a considerare la sicurezza informatica allo stesso modo.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita la pagina **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0500-000-01-01 03/22