proofpoint.

CASO CLIENTE

Una banca elimina quasi completamente le vulnerabilità di sicurezza legate alle identità grazie a Proofpoint

La sfida

- Identificare le lacune potenzialmente sfruttabili tra i controlli di sicurezza multilivello
- Accelerare la correzione dove necessario
- Contrastare i criminali informatici

La soluzione

Piattaforma Proofpoint Identity Threat Defense

- Proofpoint Spotlight
- Proofpoint Shadow

I risultati

- Riduzione dei privilegi amministratore di dominio da 350 a zero
- Identificazione e rimozione delle vie d'accesso ad alto rischio alle risorse strategiche
- Rafforzamento della fiducia di dirigenti e membri del consiglio d'amministrazione nei controlli organizzativi

L'azienda

Questa banca nazionale, di proprietà di una multinazionale di servizi finanziari, dispone di filiali in tutti gli Stati Uniti. Fornisce un'ampia gamma di servizi bancari, carte di credito, prestiti e gestione patrimoniale. Responsabile della gestione di diversi miliardi di dollari, la banca è impegnata a mantenere il numero di vulnerabilità di sicurezza informatica il più vicino possibile allo zero.

La sfida

Il team della sicurezza informatica della banca è responsabile di oltre 10.000 endpoint utente, nonché della protezione dei processi di progettazione, gestione e accesso. Aveva implementato diversi livelli di sicurezza, tra cui soluzioni di sensibilizzazione alle minacce e gestione dei rischi informatici, nella sua infrastruttura. Tuttavia, numerosi livelli di sicurezza erano separati l'uno dall'altro. Solo la soluzione SIEM della banca operava come livello "orizzontale" su tutti i controlli, eseguendo la raccolta e l'analisi degli eventi a livello di tutti i controlli. Tuttavia, nonostante le difese sofisticate, il team della sicurezza informatica ha riscontrato segnali di attacchi incessanti, sapendo che nessuna azienda è immune da potenziali violazioni.

"Sapevo ci sarebbe stato un certo livello di vulnerabilità con il quale convivere", spiega il CISO. "Alcune risorse sono molto difficili da correggere senza interrompere le attività, e non esistono best practice di sicurezza perfette. Desideravamo visibilità e protezione sulla nostra rete e su tutti gli endpoint per individuare le lacune, laddove i nostri altri controlli potrebbero non essere altrettanto efficaci".

La soluzione

Il CISO è venuto a conoscenza di Proofpoint Identity Threat Defense da colleghi del settore. Sapeva che diverse importanti banche avevano adottato la piattaforma, ma non la aveva ancora vista all'opera.

"Quando ho visto la piattaforma Proofpoint, la logica alla basa mi è sembrata molto interessante", conferma il CISO. "Ci ha permesso di vedere la rete con gli occhi di un criminale informatico".

Proofpoint Shadow è una soluzione senza agent basata sulla threat intelligence in grado di creare con facilità un'ampia rete di esche su tutta l'infrastruttura. Accelera in modo deterministico il rilevamento delle minacce, identificandole in base all'interazione del criminale informatico con le esche, senza dover ricorrere a analisi probabilistiche basate su firme o comportamenti. A differenza di altre tecnologie che implementano agent o honeypot che possono attirare l'attenzione del criminale informatico o essere da lui sfruttate, la sua architettura senza agent le impedisce di essere scoperta dal pirata informatico. Il CISO e il suo team hanno eseguito un POC (Proof of Concept) di 60 giorni con Proofpoint per mettere la soluzione alla prova. Hanno inoltre incaricato degli specialisti in test di intrusione di cercare di eludere la soluzione, ma hanno fallito ogni volta.

"Grazie a Proofpoint Identity Threat Defense abbiamo molta più fiducia nei nostri controlli di sicurezza. Ha migliorato in modo quantificabile la qualità complessiva della protezione."

CISO

Proofpoint Spotlight ha inoltre permesso al team di individuare vie d'accesso ad alto rischio che un criminale informatico può utilizzare per muoversi rapidamente attraverso la rete per accedere a risorse strategiche. Identifica costantemente privilegi d'accesso non utilizzati o superflui, nonché credenziali d'accesso archiviate in modo inadeguato che i criminali informatici possono compromettere e utilizzare a loro vantaggio.

"Proofpoint Spotlight ha individuato rapidamente le nostre lacune più sfruttabili in base ai percorsi d'attacco reali", afferma il CISO. "Ci ha fornito le prove e il contesto necessario per dare priorità alla correzione e ottimizzare altri controlli di sicurezza, se necessario".

Per massimizzare l'efficacia della soluzione, solo alcuni membri del team della sicurezza della banca sapevano che fosse stata implementata. Gli avvisi di Proofpoint Identity Threat Defense vengono gestiti come violazioni delle policy e inviati alla soluzione SIEM. La banca dispone di un analista dedicato alla revisione delle "violazioni delle policy" che provengono alla piattaforma. I membri del team della sicurezza che hanno implementato la soluzione non hanno avuto problemi di falsi positivi: tutti gli avvisi sono indice di un reale tentativo di spostamento laterale da parte di una persona sconosciuta sulla rete.

"Le informazioni acquisite da Proofpoint ci forniscono informazioni fruibili preziose che rappresentano un potente strumento di ricostruzione degli eventi."

CISO

I risultati

Eliminazione dell'accesso al dominio

Subito dopo la sua implementazione, Proofpoint Spotlight ha messo in luce e amplificato lacune sconosciute legate alle best practice, come errori di configurazione e problemi di controlli d'accesso. La piattaforma fornisce funzionalità di rilevamento continuo e automazione selettiva per individuare e rimuovere le vie d'accesso ad alto rischio con facilità. Proofpoint ha identificato non solo gli account con privilegi eccessivi, ma ha messo in luce le reali vie d'accesso alla rete che un criminale informatico potrebbe utilizzare per accedere alle risorse più preziose della banca. Grazie a questa visibilità, il team del CISO ha ottenuto il contesto necessario per comprendere esattamente come connessioni apparentemente innocenti abbiano esposto la banca a spostamenti laterali da parte dei criminali informatici. Tali informazioni hanno permesso al team di eliminare i punti di connessione non necessari in base a indicatori di rischio e impatto sulle operazioni e i flussi di lavoro aziendali. Inoltre, il CISO ha lavorato con il team IT per ridurre i privilegi in modo strategico e eliminare progressivamente tutti i privilegi di accesso in tutta l'infrastruttura.

"Abbiamo affinato le nostre policy e ridotto i privilegi di amministratore di dominio da 350 a zero", spiega il CISO. "In caso d'urgenza, l'accesso di emergenza è aperto per un periodo limitato".

La capacità di scoprire in modo semplice e rapido le lacune sfruttabili offre al team della sicurezza un vantaggio preventivo sui criminali informatici. Quando un collaboratore lascia l'azienda, utilizza le credenziali dell'ex-dipendente per individuare dove tali credenziali venivano utilizzate e colmare le lacune che non potrebbero essere rilevate altrimenti.

Conquista - e mantenimento - della fiducia del consiglio d'amministrazione

Oltre a rilevare efficacemente gli spostamenti laterali e ad aiutare il team a rafforzare la sicurezza dell'ambiente, la piattaforma Proofpoint Identity Threat Defense offre un elevato valore in termini di comunicazione. I ricchi dati di telemetria e la reportistica della soluzione Proofpoint hanno consentito al CISO di fornire ai dirigenti della banca e ai membri del consiglio di amministrazione delle spiegazioni visuali chiare di come i criminali informatici operano, perché gli spostamenti laterali sono così gravi e come le difese della banca proteggono l'ambiente.

Sebbene l'infrastruttura di sicurezza informatica della banca fosse già solida, Proofpoint ha migliorato il controllo, la visibilità e la capacità comunicativa del CISO. La possibilità di identificare le vulnerabilità, correggerle e dimostrare l'efficacia dei controlli ha rafforzato la sicurezza della banca.

"Grazie a Proofpoint Identity Threat Defense abbiamo molta più fiducia nei nostri controlli di sicurezza", spiega il CISO. "Ha migliorato in modo quantificabile la qualità complessiva della protezione".

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.