proofpoint

CASO CLIENTE

# Una società di finanziamenti per auto estende il suo programma di gestione delle vulnerabilità ai rischi legati alle identità con Proofpoint

## La sfida

- Integrazione dei rischi legati all'identità nel programma di gestione delle vulnerabilità
- Difficoltà a supportare le applicazioni di vecchia generazione con la soluzione di gestione degli accessi con privilegi (PAM)
- Mancanza di visibilità costante sui rischi legati alle identità con privilegi

## La soluzione

Proofpoint Identity Threat Defense

- Proofpoint Spotlight

## I risultati

- Sensibilizzazione rafforzata dei rischi principali legati alle identità
- Immediato miglioramento del livello di sicurezza
- Supporto del principale vettore d'attacco, l'identità, da parte del programma di gestione delle vulnerabilità

## L'azienda

Questa azienda è un fornitore mondiale di soluzioni di finanziamenti per auto con oltre 9.000 collaboratori e attività in Nord America, Sud America e Asia. Offre programmi di finanziamento al dettaglio e di leasing a consumatori e concessionarie di auto, nonché prodotti di prestito commerciale ai concessionari per aiutarli a finanziare e a far crescere le loro attività. Dispone di un patrimonio di circa 60 miliardi di dollari.

## La sfida

Quest'azienda ha un'infrastruttura IT ampia e diversificata e ha problemi con le sue applicazioni di vecchia generazione. Sebbene abbia implementato una soluzione di gestione degli accessi con privilegi (PAM), non proteggeva molte applicazioni di vecchia generazione, in particolare quelle troppo costose da aggiornare o per le quali era previsto il ritiro. Inoltre, alcuni account amministrativi e di servizio non potevano essere protetti. Di conseguenza, l'azienda non disponeva di un controllo completo sulle credenziali d'accesso e le identità con privilegi né aveva una visibilità sufficiente sui rischi potenziali legati alle identità. Ciò riguardava sia gli amministratori IT che gli utenti normali.

Come afferma il SVP of Global Cybersecurity Strategy and Operations dell'azienda: "Se si dispone di un'infrastruttura on premise di grandi dimensioni e si utilizza Active Directory da anni, le vulnerabilità sono frequenti come risultato delle decisioni prese tempo addietro. Il debito tecnologico è elevato. Inoltre, la migrazione al cloud e le attività di fusioni-acquisizioni aumentano la complessità".

## La soluzione

L'azienda ha preso in considerazione Proofpoint Identity Threat Defense come un'importante espansione della propria strategia completa di gestione delle vulnerabilità. Tradizionalmente, l'approccio dell'azienda in tal senso si è focalizzato su CVE e CWE. L'azienda era consapevole che passi falsi nella configurazione delle identità stavano creando molti rischi potenziali. Ha perciò iniziato a tracciare tutti gli elementi del loro ambiente che presentavano un rischio per la sicurezza informatica, che fossero o meno associati a una vulnerabilità CVE. Utilizzando il modello ISO a 7 livelli come guida, ha rivisto il proprio approccio alla valutazione automatizzata dei rischi per essere certa di coprire l'ambiente IT nel suo complesso e ha concluso che le mancavano delle funzionalità di gestione dei rischi legati alle identità.

> "Lo strumento Proofpoint ci ha offerto nuove prospettive. Sapevamo di dover analizzare in modo approfondito questi rischi legati alle identità, ma non avevamo alcun mezzo per farlo."
>
> AVP IT Vulnerabilities

Sulla base di questa consapevolezza, l'azienda ha implementato la soluzione Proofpoint per la gestione dei rischi legati alle identità all'inizio del 2021. Proofpoint Identity Threat Defense si integra con l'infrastruttura Active Directory (AD) dell'azienda e analizza ogni endpoint su base regolare per produrre un repository dei rischi legati all'identità, che l'azienda recupera attraverso l'API. Il team della sicurezza IT esamina questi rischi e si confronta regolarmente con il team di correzione delle vulnerabilità informatiche per implementare cambiamenti volti a ridurre i rischi per il loro ambiente e tracciarli. Si tratta di uno sforzo collaborativo, come spiega l'AVP IT Vulnerabilities: "Facciamo del nostro meglio per collaborare con il team IT".

In combinazione con gli sforzi dell'azienda per correggere le vulnerabilità, degli accordi di livello di servizio (SLA) che variano in base al livello di criticità permettono di assegnare la priorità agli elementi più critici.

## I risultati

Subito dopo l'implementazione della soluzione, l'azienda ha visto migliorare il proprio livello di sicurezza. Dopo aver utilizzato il prodotto per oltre un anno, l'azienda rileva in genere diversi nuovi problemi critici alla settimana e li risolve rapidamente. "Generalmente questi problemi sono dovuti alla disattenzione degli utenti. Non hanno intenzioni dannose, ma a volte commettono errori o agiscono troppo in fretta".

Alla domanda su cosa farebbero senza la soluzione di Proofpoint, il team non ha saputo cosa rispondere, dato che non conoscono altri modi per ottenere il tipo di informazioni sulle identità (soprattutto sugli endpoint) che la soluzione fornisce. L'AVP IT Vulnerabilities dell'azienda spiega: "Non abbiamo alcun modo di vedere una password memorizzata in PuTTY, per esempio".

"Le fusioni-acquisizioni rappresentano un caso d'uso interessante, perché effettuiamo un'analisi prima e dopo l'integrazione. Con Proofpoint Identity Threat Defense posso valutare l'integrità dell'ambiente e il livello di debito tecnologico."

SVP Global Cybersecurity Strategy and Operations

L'SVP of Global Cybersecurity Strategy and Operations aggiunge: "Le fusioni-acquisizioni sono un caso d'uso interessante, perché l'analisi viene effettuata prima e dopo l'integrazione. Grazie alla soluzione posso valutare l'integrità dell'ambiente e il livello di debito tecnologico".

Quando gli è stato chiesto se consiglierebbe la soluzione Proofpoint Identity Threat Defense ad altri professionisti ha risposto: "Sulla base dei risultati conseguiti, e conoscendo la nostra direzione, raccomanderei questa soluzione a tutti i professionisti che desiderano migliorare la gestione delle vulnerabilità. Questo strumento permette di visualizzare tutto: vulnerabilità tradizionali, vulnerabilità legate alle identità e errori di configurazione".

Ha inoltre aggiunto: "È sufficiente una sola vulnerabilità legata alle identità per mandare in tilt l'intero ambiente. Qualsiasi strumento permetta di migliorare la gestione delle vulnerabilità offre un valore aggiunto, soprattutto quando permette di visualizzare i rischi e ridurli nel tempo. La soluzione Proofpoint ci ha permesso di chiudere centinaia di migliaia di porte: un risultato incredibile".

## PER SAPERNE DI PIÙ

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