proofpoint.

Gestione delle minacce interne nel settore dei servizi finanziari

Proteggi i tuoi dati sensibili e la tua reputazione

proofpoint.com/it

Introduzione

Le società di servizi finanziari sono solitamente fra le prime ad adottare i nuovi strumenti di sicurezza informatica ma, nonostante tale investimento, il settore da solo rappresenta quasi un quarto di tutte le violazioni della sicurezza, di cui oltre la metà è imputabile a utenti interni.

Per la natura delle loro mansioni, i lavoratori di questo settore critico hanno accesso ai flussi digitali di denaro ma anche ai dati sensibili dei clienti. Ciò li rende un fattore di rischio aziendale intrinseco, oltre che bersagli altamente redditizi per i criminali informatici.

Alcuni dipendenti sono ostili, altri semplicemente negligenti, mentre altri ancora vengono violati da hacker esterni che sfruttano le loro vulnerabilità per accedere a dati, sistemi e risorse sensibili. Non deve sorprendere che le minacce interne siano un vettore particolarmente insidioso.

Questo eBook prende in esame la gestione delle minacce interne nel settore dei servizi finanziari. Attingendo a casi reali del settore assicurativo, bancario e gestione patrimoniale, esamina le problematiche legate alla gestione di tali minacce. Inoltre, scoprirai come Proofpoint può aiutarti a identificare, analizzare e neutralizzare questi incidenti di origine interna in modo rapido ed efficiente.

Il 24% delle violazioni di sicurezza si verifica nelle istituzioni finanziarie. Oltre la metà di questi attacchi proviene da utenti interni[1].

[1] Data Breach Investigations Report 2017 (Report 2017 sulla violazione dei dati), Verizon

CAPITOLO 1

Le minacce interne nell'attuale settore dinamico dei servizi finanziari

Dal 2018 le minacce interne nel settore dei servizi finanziari sono aumentate del 20,3%[2].

Tutte le aziende hanno l'obbligo di proteggere le informazioni riservate. Ciò significa tutelare le informazioni della clientela, i dati aziendali e la proprietà intellettuale. Tale mandato può avere una valenza ancora più critica per le banche, gli istituti di credito, le società di gestione degli investimenti e le assicurazioni.

Come altri settori, anche quello dei servizi finanziari deve far fronte a una forza lavoro sempre più distribuita e alla moltiplicazione delle applicazioni cloud: tendenze convergenti che rendono la gestione delle minacce interne ancora più complessa.

Oggi, l'infrastruttura informatica è condivisa da una gamma più ampia di utenti, collaboratori, fornitori di servizi, partner e dipendenti remoti. Definire esattamente cosa sia un "utente interno" non è quindi così semplice, come non lo è definire cosa costituisce una "minaccia".

La gestione delle minacce interne non si limita solo all'eliminazione degli utenti malintenzionati, ma si tratta anche di identificare e gestire le minacce provenienti dagli utenti negligenti o che sono stati compromessi.

[2] 2020 Cost of Insider Threat Global Report (Report 2020 sul costo delle minacce interne a livello mondiale), Ponemon Institute

CAPITOLO 2

La comprensione dei rischi interni

I rischi interni dovrebbero essere una delle priorità di un'azienda votata al digitale, ma è particolarmente importante per le società dei servizi finanziari.

Ma da dove iniziare? Il primo passo di qualsiasi programma per la gestione delle minacce interne tramite la tecnologia è la comprensione *(chi* e *cosa)* dei rischi interni:

- Chi sono le persone a rischio?
- Cosa deve essere protetto?

Chi sono le persone a rischio?

Per gestire le minacce interne è innanzitutto necessario identificare gli utenti che pongono i rischi maggiori di violazione interna. Ogni azienda e casi di utilizzo sono unici, ma ci sono alcuni profili comuni di utenti a rischio:

Collaboratori esterni: nel settore dei servizi finanziari catene di fornitura e di servizio dinamiche e disaggregate sono all'ordine del giorno. Non è raro che i dipendenti condividano l'infrastruttura informatica con collaboratori esterni, fornitori di servizi, consulenti e partner, ognuno dei quali è un potenziale vettore di rischio.

Utenti con privilegi: alcuni dipendenti hanno bisogno di accedere a infrastrutture e informazioni protette. Ecco alcuni esempi:

- Amministratori informatici
- Dipendenti dell'help desk
- Addetti al call center
- Amministratori finanziari

Dipendenti ad alto rischio: l'Ufficio Risorse Umane può considerare alcuni utenti ad alto rischio in base a fattori come:

- Comportamento
- Cambio di ruolo
- Problemi disciplinari o di prestazioni
- Rischio di dimissioni

Dipendenti interessati da fusioni e acquisizioni: il settore dei servizi finanziari è in costante cambiamento. Fusioni, acquisizioni e cessioni sono all'ordine del giorno. La base di utenti autorizzati di una società può quindi rapidamente raddoppiare e viceversa. Questi cambiamenti creano tensioni all'interno dell'azienda e possono sfociare in violazioni dei dati.

Telelavoratori: è un dato di fatto, il telelavoro è una tendenza a livello mondiale. Tuttavia, lavorare al di fuori del perimetro protetto della rete può aumentare il rischio di violazioni interne.

Non solo utenti malintenzionati

Il termine "minaccia interna" è comunemente associato agli utenti malintenzionati, le cui motivazioni possono essere finanziarie, politiche o di vendetta personale. Tuttavia, gli utenti negligenti o le vittime di furto d'identità (utenti compromessi) sono molto più spesso all'origine delle violazioni interne.

Per "utenti negligenti" si intendono coloro che agiscono al di fuori delle procedure approvate, esponendo inavvertitamente l'infrastruttura o i dati e aumentando i rischi.

Per "utenti compromessi" si intendono coloro che agiscono sotto l'influenza di criminali informatici esterni all'azienda. Alcuni di loro sono indotti, tramite tecniche di social engineering, a inviare i dati, mentre altri perdono semplicemente il controllo del loro account.

In ogni caso, che rientrino in una categoria o nell'altra, questi utenti rappresentano la più grande minaccia interna.

Utenti interni negligenti

Utenti interni malintenzionati

Utenti interni compromessi

Cosa deve essere protetto?

Come la maggior parte delle aziende, le società finanziarie devono poter contare su una protezione elevata delle loro transazioni digitali. Tale protezione dipende anche dall'integrità dell'infrastruttura informatica rivolta alla clientela e ai dipendenti. Ecco alcune delle loro principali preoccupazioni:

Protezione dei dati sensibili: le società di servizi finanziari gestiscono enormi volumi di dati a carattere privato, come le informazioni bancarie e i dati sanitari personali. Tali dati sono molto preziosi per i truffatori e spesso sono l'obiettivo principale delle violazioni dei dati.

Conformità: il settore dei servizi finanziari è soggetto a innumerevoli norme e obblighi di conformità, che governano il modo in cui le aziende proteggono i dati, le informazioni e l'integrità dei loro processi. Le lacune nella conformità e le violazioni dei dati possono essere particolarmente costose.

Frodi finanziarie: le società di servizi finanziari gestiscono enormi volumi di transazioni e capitali. I truffatori ingannano i dipendenti e si servono del loro accesso privilegiato per sottrarre denaro in vari modi.

Interruzione del servizio: le società di servizi finanziari si affidano alle infrastrutture informatiche per gestire i servizi rivolti sia alla clientela sia ai dipendenti. Se ottiene un accesso privilegiato, un criminale informatico può danneggiare o interrompere le attività di tali sistemi. Le ripercussioni di questa interruzione di servizio sono molteplici: perdita di fatturato, opportunità commerciali e fiducia.

Protezione delle informazioni proprietarie: per mantenere un vantaggio competitivo, molte società di investimento si affidano a informazioni proprietarie o algoritmi di compravendita. Il successo dei loro servizi dipende dalla loro capacità di mantenere protetti questi dati.

Danni alla reputazione: i servizi finanziari costruiscono la propria immagine sulla fiducia generata in clienti, partner commerciali e organismi di vigilanza. Quando si verifica una violazione della sicurezza tale fiducia viene meno, soprattutto se la violazione è stata causata da utenti interni. E la reputazione viene così danneggiata.

CAPITOLO 3

Il ruolo delle tecnologie di gestione delle minacce interne

Le soluzioni di gestione delle minacce interne (ITM) aiutano gli addetti alla sicurezza a controllare meglio questo vettore di rischio, che possiede caratteristiche uniche.

Tali soluzioni combinano funzionalità di prevenzione delle fughe di dati (DLP) e di analisi del comportamento degli utenti (UBA) per ridurre il rischio in tre modi principali:

Identificazione dei rischi legati agli utenti

Le soluzioni ITM consentono agli addetti alla sicurezza di rilevare rapidamente le potenziali violazioni. Gli strumenti più efficaci permettono di distinguere fra falsi positivi e attività interne che richiedono una verifica. Per farlo, analizzano, nel contesto, le attività degli utenti e i movimenti dei dati, soprattutto per gli utenti ritenuti ad alto rischio.

Protezione dalle perdite di dati

La maggior parte delle società finanziarie possiede dati da proteggere: algoritmi proprietari, segreti commerciali, informazioni personali e altri. Nessuna di esse vuole che tali dati fuoriescano dall'azienda n maniera inappropriata. La capacità di identificare e bloccare rapidamente la fuoriuscita di dati è una funzione essenziale di qualsiasi soluzione ITM moderna.

Accelerazione della risposta agli incidenti

Il costo delle minacce interne dipende dal tempo necessario per rispondere a un incidente. I moderni sistemi ITM permettono agli addetti alla sicurezza di reagire 10 volte più velocemente. Con la soluzione ITM giusta, compiti che richiederebbero giorni o settimane possono essere completati in pochi minuti. Indagini più rapide riducono il tempo medio di risoluzione.

CAPITOLO 4 - La soluzione Proofpoint ITM in azione

Casi clienti

Società internazionale di intermediazione in ambito assicurativo - Maggiore visibilità sull'attività dei dipendenti distribuiti

La sfida

Una società di intermediazione internazionale di prodotti assicurativi stava cercando un modo per proteggere i dati relativi alle richieste di risarcimento dei clienti.

A tale scopo, i suoi addetti alla sicurezza avevano bisogno di una maggiore visibilità sulle potenziali violazioni dei dati di origine interna. Sebbene l'azienda fosse in grado di monitorare la sua forza lavoro altamente distribuita tramite un'applicazione basata sul cloud, l'analisi e l'interpretazione dei registri attività generati da questa applicazione hanno richiesto molto tempo e lavoro. Inoltre la legislazione sempre più severa non faceva che aumentare le preoccupazioni relative alla protezione dei dati raccolti e gestiti dati tramite questa applicazione.

La soluzione

Al fine di tutelare attivamente la riservatezza dei dati in ogni momento e luogo, in particolare sugli endpoint remoti, la società di intermediazione aveva bisogno di uno strumento per la gestione delle minacce interne. Inoltre, desiderava una maggiore visibilità sulle modalità di interazione degli utenti con i dati e sulle loro attività negli endpoint. Era necessaria quindi una soluzione che potesse identificare attivamente i comportamenti ad alto rischio, inviare avvisi di conformità e facilitare le relative verifiche.

Il risultato

Grazie alla sua soluzione ITM, l'azienda ora gode dei seguenti vantaggi:

- Rilevamento di movimenti rischiosi degli archivi delle richieste di risarcimento, sia da applicazioni aziendali ed endpoint che a livello di server.
- Sensibilizzazione degli utenti e segnalazione in tempo reale dei comportamenti non in linea con le policy.
- Correlazione di prove inconfutabili e dettagliate (chi ha fatto cosa, quando, dove, come e perché) ad ogni indagine che segue un avviso. L'acquisizione delle schermate relative alle attività degli endpoint forniscono informazioni contestuali sugli eventi prima, durante e dopo una violazione. Questo dato aiuta a determinare se un atto è stato dovuto a negligenza, dolo o a una violazione operata dall'esterno.
- Salvaguardia di una traccia dettagliata di verifica delle attività di dipendenti e terze parti, per adempiere agli obblighi di conformità finanziaria.

Società indipendente di gestione patrimoniale - Salvaguardia dei beni e della fiducia dei clienti

La sfida

Le società indipendenti di gestione patrimoniale hanno la responsabilità di mantenere al sicuro le informazioni private e sensibili della loro clientela. Il loro successo si basa sulla fiducia.

La gestione dei dati privati dei clienti fa parte dell'attività quotidiani di questa azienda. Il personale interno non si limita ai gestori dei fondi, amministratori e agli altri dipendenti, ma comprende anche collaboratori terzi. La società doveva fronteggiare minacce costanti: crimini informatici, spionaggio industriale e sponsorizzato dagli Stati, frodi monetarie e altro ancora.

La soluzione

La società aveva bisogno di un solido sistema di sicurezza per proteggersi dai rischi di reati informatici e frodi monetarie. Agli addetti alla sicurezza serviva un modo facile per monitorare le attività potenzialmente pericolose a tutti i livelli dell'azienda, compresi gli utenti distribuiti e le terze parti.

Il risultato

Ecco i risultati conseguiti dall'azienda grazie alla soluzione ITM:

- Semplificazione delle policy di uso accettabile e conformità.
- Rilevamento automatico e in tempo reale di movimenti rischiosi delle informazioni sensibili e riservate.
- Ottimizzazione delle indagini sulle violazioni correlando tutti i movimenti dei dati con le attività degli utenti in tempo reale. L'acquisizione delle schermate relative alle attività degli endpoint fornisce prove inconfutabili delle azioni intraprese da un utente.
- Salvaguardia di una traccia dettagliata di verifica delle attività degli utenti, per adempiere agli obblighi di conformità finanziaria.

Banca regionale – Protezione dalle minacce interne nei call center finanziari

La sfida

A fronte della diffusione del telelavoro, una banca regionale doveva garantire la sicurezza dei propri call center.

Ad ogni chiamata ricevuta il personale aveva accesso ai dati dei membri della banca. Gli addetti alla sicurezza dovevano poter continuare a monitorare le attività interne e a rispondere ai potenziali incidenti anche se il personale lavorava da casa. La banca era particolarmente preoccupata dei dipendenti ad alto rischio, ovvero coloro che hanno accesso a informazioni private preziose che potrebbero essere rubate, trafugate o alterate. Desiderava inoltre identificare, raccogliere e condividere i dati forensi durante la risposta a un incidente.

La soluzione

Gli addetti alla sicurezza cercavano una soluzione per rilevare in tempo reale i comportamenti anomali. Era tuttavia necessario ottimizzare la raccolta e il monitoraggio dei dati in un contesto di telelavoro, senza compromettere la produttività e il servizio alla clientela.

Il risultato

La soluzione ITM ha aiutato il call center a risolvere il problema delle minacce interne, grazie alle seguenti misure.

- Rafforzamento della resilienza degli utenti. La soluzione ITM ha migliorato la sensibilizzazione alla sicurezza sulla base di casi concreti di minacce interne. Ha inoltre permesso alla banca di chiarire le policy sui dati aziendali.
- Distribuzione, a livello di endpoint, di strumenti leggeri di raccolta dati in modalità utente. Questo approccio ha contribuito a preservare la produttività degli utenti evitando di rallentare i dispositivi.
- Rilevamento in tempo reale dei comportamenti a rischio degli utenti e i movimenti dei dati.
- Collaborazione con gli uffici Risorse Umane, Legale, Conformità e Informatico. I gruppi hanno lavorato insieme per definire le modalità di raccolta dei dati di utenti e file, le esigenze di rilevamento dei comportamenti e i flussi di lavoro della risposta agli incidenti.
- Accelerazione delle indagini. La soluzione ITM ha fornito le informazioni contestuali relative agli utenti, semplificato la raccolta delle prove e agevolato la collaborazione fra i gruppi.

Conclusioni e raccomandazioni

Proofpoint: un partner di fiducia, soluzioni ITM ad alte prestazioni

Ogni giorno, i team IT e della sicurezza lavorano sodo per identificare, rilevare e neutralizzare le minacce informatiche. La soluzione Proofpoint Insider Threat Management (ITM) può essere d'aiuto. Protegge da perdite di dati, interruzioni dell'attività e altri danni causati dagli utenti, in modo intenzionale o meno.

La nostra premiata soluzione ha aiutato oltre 1.200 importanti aziende in più di 100 paesi:

- Riduci il tempo medio di rilevamento delle minacce interne che possono mettere in pericolo le tue informazioni sensibili e riservate.
- Riduci la frequenza, la gravità e il costo delle violazioni, con un tempo medio di risposta agli incidenti più breve.
- Migliora la produttività degli addetti alla sicurezza riducendo i costi. Proofpoint ti permette di riunire diverse tecnologie (come le analisi basate sugli utenti e gli strumenti DLP per gli endpoint) in un'unica piattaforma ITM.

Ecco come ti aiutiamo:

- Realizziamo con te a un PoC (Proof-of-Concept) per aiutarti a visualizzare meglio il tuo programma ITM.
- Ti aiutiamo a progettare e costruire il tuo programma di gestione interna delle minacce. Suddividiamo il tuo progetto in una serie di compiti facili da gestire e ordinati per priorità in base ai comportamenti ad alto rischio. Il PoC ti permette di visualizzare meglio il tuo programma ITM, mentre i nostri servizi ITM Jump Start ti permettono una valorizzazione più rapida.
- Infine, ti aiutiamo a rafforzare la resilienza dei tuoi utenti con il programma Proofpoint Security Awareness Training.

Il nostro obiettivo è uguale al tuo: proteggere le tue risorse più preziose e le persone che le gestiscono.

PER SAPERNE DI PIÙ

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

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, 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**.

0512-002-01-01 10/21