proofpoint.

GUIDA ALL'ACQUISTO

Guida del CISO per bloccare le minacce incentrate sulle persone e sull'IA

Principali funzionalità

Queste sono le cinque funzionalità di cui ha bisogno per proteggere la Sua azienda dalle minacce incentrate sulle persone e sull'IA :

1. Visibilità completa sulle minacce e analisi dei rischi
2. Protezione automatica contro le minacce per l'email e altri vettori
3. Sicurezza per le comunicazioni aziendali di fiducia
4. Sensibilizzazione dei collaboratori
5. Protezione contro il takeover degli account

Panoramica

I criminali informatici continuano a intensificare i loro sforzi di sottrazione di dati e sfruttamento delle comunicazioni aziendali a fini di lucro. Ma se il volume di queste minacce continua a crescere, le tattiche utilizzate, per contro, rimangono sostanzialmente le stesse. Phishing, malware, ransomware, violazione dell'email aziendale (BEC, Business Email Compromise) e social engineering si confermano tecniche preferite per prendere di mira gli utenti.

La novità è che l'IA ottimizza queste tattiche familiari. I criminali informatici utilizzano modelli linguistici di grandi dimensioni per creare esche di phishing iperpersonalizzate, automatizzare l'80-90% della catena d'attacco e lanciare campagne multicanale in più fasi su una scala senza precedenti. Nel 2025, Proofpoint ha osservato un aumento del 94% delle minacce via email rivolte ai clienti. L'IA introduce anche nuovi vettori d'attacco, come gli attacchi di iniezione di prompt che armano gli assistenti IA aziendali mediante l'inserimento di istruzioni nascoste nelle email.

In questa guida, prenderemo in esame le principali funzionalità di cui la tua azienda deve disporre per creare una difesa efficace contro tutte le minacce incentrate sulle persone, che siano trasmesse via email o altri vettori. Ti suggeriamo anche diversi criteri per guidarti nella scelta di una piattaforma di sicurezza adatta alle tue esigenze.

Figura 1. Minacceerischinegli ambienti di lavorodigitali

1. Visibilità completa sulle minacce e analisi dei rischi

Per bloccare le minacce incentrate sulle persone e sull'IA, devi stabilire chi sono gli utenti più colpiti e con quali mezzi vengono presi di mira. Potrai così applicare controlli di sicurezza adattivi per proteggere gli utenti più a rischio.

Una visibilità completa sulle minacce per l'email e i canali digitali ti offre un quadro completo delle tue vulnerabilità.

Ecco le informazioni che una soluzione deve essere in grado di comunicarti:

- **Persone prese di mira**, nonché le minacce che si trovano a affrontare e le loro eventuali interazioni con i criminali informatici
- **Informazioni forensi**, tra cui il criminale informatico, la famiglia delle minacce, gli utenti interessati, le tecniche d'attacco, gli argomenti sfruttati nonché gli obiettivi della campagna d'attacco
- **Utenti a rischio**, identificando le persone che mettono più a rischio la tua azienda e i motivi
- **Minacce associate alle comunicazioni aziendali di fiducia**, inclusi i domini o i siti web fotocopia o contraffatti che possono danneggiare l'immagine del tuo marchio
- **Cambiamenti di comportamento e threat intelligence**, che possono rivelare segnali di violazione di uno dei tuoi fornitori o di una terza parte di fiducia
- **Attività sospette**, che potrebbero indicare potenziali takeover degli account

Una piattaforma ottimizzata dall'IA può correlare i segnali attraverso queste dimensioni, utilizzando grafici di relazione per definire una base di riferimento dei comportamenti di comunicazione, modelli linguistici per interpretare l'intento del messaggio e threat intelligence per contestualizzare il comportamento dei criminali informatici. Di conseguenza, ottieni informazioni sui rischi più precise e fruibili rispetto alla sola analisi manuale.

La visibilità non è importante solo per le implementazioni iniziali, deve essere costante. Potrai così adattare costantemente il tuo livello di protezione, poiché le caratteristiche degli attacchi cambiano.

4,88 Mln di dollari

Costo medio di una violazione dei dati in un attacco di phishing o di violazione dell'e-mail aziendale (BEC) [1]

1. IBM. *Cost of a Data Breach Report (Report sul costo delle violazioni dei dati)*, 2024.

2. Protezione automatica contro le minacce per l'email e altri vettori

Il panorama delle minacce è in costante evoluzione. Purtroppo, le aziende spesso non dispongono delle competenze in sicurezza e delle risorse necessarie per tenere il passo. Di conseguenza, è comune che i team non abbiano il tempo di indagare su ogni incidente di sicurezza. Inoltre, il costo di questi eventi è in aumento.

Per questo motivo hai bisogno di una soluzione che sia in grado di rilevare e bloccare in modo preciso e efficace le minacce, senza incidere sulla produttività. Dato il ruolo crescente giocato dall'IA nella generazione e consegna delle minacce, è fondamentale che anche le tue funzionalità di rilevamento siano ottimizzate dall'IA.

Ecco tutte le azioni che una soluzione dovrebbe poter eseguire automaticamente:

- **Blocco delle minacce prima della consegna** con un'efficacia di almeno il 99,999% in modo che non raggiungano mai le caselle email dei tuoi utenti
- **Rilevamento e blocco delle minacce generate dall'IA**, inclusi messaggi BEC creati dall'IA, il phishing personalizzato dall'IA e gli attacchi tramite iniezione di prompt nascosti che prendono di mira gli assistenti IA come Microsoft Copilot
- **Analisi dei modelli comportamentali delle email inviate internamente**, utilizzando una threat intelligence ottimizzata dall'IA e modelli di machine learning per rilevare le attività di phishing laterale
- **Disamina e blocco degli URL dannosi in tempo reale** per assicurare che non raggiungano gli utenti attraverso l'email o le piattaforme di messaggistica e collaborazione
- **Rilevamento e neutralizzazione degli account dei fornitori d'identità compromessi** ospitati nel cloud
- **Analisi dei codici QR sospetti prima della consegna** con computer vision ottimizzata dall'IA e analisi semantica, e sandboxing
- **Inserimento di avvisi** nei messaggi sospetti

Quando un criminale informatico ottiene l'accesso iniziale, è fondamentale rilevare e neutralizzare rapidamente quella minaccia. Un intervento rapido può fare la differenza tra un incidente minore e una violazione su larga scala.

3. Sicurezza per le comunicazioni aziendali di fiducia

Le comunicazioni digitali sono un elemento vitale per le aziende. Non sorprende perciò che i criminali informatici si impegnino così tanto per infiltrarsi nelle comunicazioni di fiducia. Attacchi come il phishing, il ransomware o la violazione dell'email aziendale (BEC) sono più efficaci quando i destinatari pensano, erroneamente, di interagire con fonti affidabili.

Per aumentare le loro possibilità di successo, i criminali informatici utilizzano un'ampia gamma di tattiche di furto d'identità. Tali tattiche sono diventate molto più efficaci grazie all'IA. I criminali informatici possono ora generare in pochi secondi messaggi curati e contestualizzati, in grado di imitare il tono e lo stile di scrittura di un dirigente. È perciò fondamentale disporre di molteplici livelli di protezione per contrastarli.

Scegli una soluzione che offra i seguenti vantaggi:

- **Autenticazione delle email** generate dagli utenti e dalle applicazioni
- **Ambiente dedicato sicuro** per l'inoltro delle email transazionali generate dalle applicazioni
- **Supporto dell'implementazione di DMARC** per massimizzare l'efficacia dell'autenticazione delle email e garantire piena conformità con DMARC
- **Protezione contro i domini fotocopia**, tra cui funzionalità di rilevamento e aiuto nello smantellamento di questi domini dannosi
- **Monitoraggio degli account dei fornitori compromessi** tramite l'IA comportamentale e la threat intelligence, e esecuzione di azioni automatiche per difendersi

La protezione delle tue comunicazioni aziendali di fiducia permette di proteggere non solo i tuoi collaboratori ma anche i tuoi partner commerciali e i tuoi clienti.

71%

Collaboratori che hanno ammesso di aver avuto comportamenti a rischio come riutilizzare le password o fare clic su link sconosciuti[2]

2. Proofpoint. *report State of the Phish*, 2024

4. Sensibilizzazione dei collaboratori

Anche se la tecnologia blocca il 99% delle minacce, il rimanente 1% può ancora causare un incidente importante. È qui che il comportamento umano diventa un fattore decisivo. I criminali informatici generalmente hanno bisogno dell'intervento dei tuoi utenti per le loro campagne dannose.

E gli attacchi non sono l'unica preoccupazione in quest'ambito. Gli utenti spesso sacrificano la sicurezza della loro azienda a favore della facilità d'uso. Secondo il report *2024 SState of the Phish* di Proofpoint:

- Il 71% dei collaboratori ha ammesso di aver avuto comportamenti a rischio come riutilizzare le password o fare clic su link sconosciuti.
- Il 96% di questi collaboratori sapeva che il proprio comportamento comportava dei rischi ma ha comunque eseguito le azioni pericolose.

Con la crescente integrazione degli strumenti di IA nei flussi di lavoro quotidiani, i collaboratori devono affrontare anche nuovi rischi, come la condivisione di dati sensibili con applicazioni di IA non approvate o l'attivazione involontaria di iniezioni di prompt nascoste nel corso dell'interazione con gli assistenti di IA.

Quando si combinano attacchi e comportamenti negligenti, le possibilità di una violazione si moltiplicano. Ecco perché devi sensibilizzare i tuoi utenti alla sicurezza informatica.

Scegli una soluzione che offra i seguenti vantaggi:

- **Utilizzo dei dati sulle minacce** per identificare gli utenti più colpiti e a rischio
- **Formazione degli utenti basata sui rischi** che utilizza esempi presi dalla vita reale, come quelli che prendono di mira la tua azienda
- **Cambiamento reale dei comportamenti**, anziché limitarsi a fornire la formazione annuale obbligatoria agli utenti
- **Motivazione dei collaboratori** offrendo loro visibilità sul loro punteggio di rischio individuale e sul loro impatto sul livello di sicurezza dell'azienda
- **Valutazione dell'efficacia** e disponibilità di report utili che ti aiutano a affinare la tua strategia
- **Presentazione dei rischi legati all'IA nei contenuti di formazione**, spiegando come utilizzare gli strumenti di IA generativa in modo sicuro e identificare gli attacchi di social engineering generati dall'IA.

Una tecnologia efficace combinata con la vigilanza umana è fondamentale per bloccare le minacce incentrate sulle persone. Tutti hanno un ruolo fondamentale nella protezione delle operazioni aziendali.

5. Protezione contro il takeover degli account

I dati di Proofpoint mostrano che il 99% delle aziende subisce tentativi costanti di takeover degli account. Questi attacchi sono una forma di furto d'identità in cui il criminale informatico ottiene accesso a un account online e ne prende il controllo. Non sorprende che fornitori di identità cloud, come Microsoft Entra ID, Google e Okta, siano quelli più presi di mira. Questi account sono utilizzati come Single Sign-On in una serie di applicazioni aziendali.

Inoltre, i tuoi account non sono gli unici di cui devi preoccuparti. I criminali informatici compromettono anche gli account di partner commerciali di fiducia per condurre operazioni di ricognizione e lanciare nuovi attacchi. Questi account compromessi fungono da punto di accesso per lanciare attacchi in più fasi che si diffondono nell'intero ecosistema di un'azienda per rubare dati sensibili, effettuare transazioni fraudolente e seminare il caos.

L'IA e il machine learning sono essenziali per monitorare le comunicazioni aziendali su larga scala e automatizzare la risposta. I modelli di IA comportamentale sono in grado di rilevare i segnali più sottili di violazione dell'account, come comportamenti di accesso e di invio di email insoliti, o cambiamenti nelle relazioni di comunicazione, che potrebbero sfuggire ai sistemi basati su regole.

Scegli una soluzione che offra i seguenti vantaggi:

- **Monitoraggio costante di tutti gli account** associati a servizi di fornitori d'identità basati su cloud , come Microsoft Entra ID, Google e Okta.
- **Threat intelligence** utilizzata insieme a dati comportamentali e machine learning per rilevare gli account compromessi
- **Protezione contro gli attacchi di account takeover** che eludono l'autenticazione a più fattori; il 65% degli account violati era protetto dall'autenticazione a più fattori[4]
- **Accelerazione delle indagini** grazie a una vista centralizzata delle attività successive al takeover degli account
- **Automazione della risposta** attraverso azioni come la sospensione degli account, la reimpostazione forzata delle password e l'annullamento di modifiche dannose alle regole della casella email e alle configurazioni dell'autenticazione a più fattori
- **Rimozione di applicazioni di terze parti sospette nell'ambito** della bonifica successiva al takeover degli account

I takeover degli account possono essere costosi e danneggiare l'immagine del tuo marchio. Una protezione rigorosa è fondamentale per limitare i rischi.

99%

Aziende che subiscono regolarmente tentativi di takeover degli account[3]

3. Ricerca Proofpoint.
4. Ibid.

Evitare gli approcci frammentati

Quando crei le tue difese per l'email e altri canali, le soluzioni individuali di più fornitori di soluzioni specializzati possono sembrarti la scelta più ovvia. Dopo tutto, questi ultimi possono sembrare ben preparati per rispondere a tipi specifici di attacchi. Tuttavia, questo approccio a silos presenta diversi svantaggi.

In primis, genera punti ciechi nella sicurezza. Quando gli strumenti non sono ben integrati, i team della sicurezza faticano a ottenere visibilità sull'intero ambiente di sicurezza. Ciò non solo aumenta il rischio che delle minacce non vengano rilevate, ma ritarda la risposta agli incidenti.

Inoltre, gli strumenti frammentati non sono in grado di offrire l'approccio globale all'IA necessario per contrastare le minacce attuali. I modelli linguistici, la computer vision, l'analisi comportamentale e la threat intelligence devono operare di concerto e condividere i dati relativi al contesto per rilevare gli attacchi sofisticati generati dall'IA.

La gestione di diversi strumenti di sicurezza è inoltre un'attività dispendiosa in termini di tempo per i team che devono correlare i dati tra punti di controllo isolati . Senza contare che l'elevato numero di avvisi generati da queste piattaforme porta a un calo di concentrazione e al mancato rilevamento delle minacce. Tutto ciò contribuisce a aumentare i costi operativi.

Privilegia un approccio più efficace. Adotta una piattaforma di sicurezza globale e pre-integrata che affronta tutte le minacce incentrate sulle persone. Inoltre, la collaborazione con un unico partner di fiducia ti garantisce non solo una gestione ottimizzata ma anche una riduzione dei costi.

Conclusione

Una strategia di sicurezza completa , incentrata sulle persone, ti aiuta a proteggere la tua azienda da un'ampia gamma di minacce. Il tuo percorso verso questo obiettivo deve iniziare con la scelta della soluzione giusta. Scegli una soluzione che raggruppa la threat intelligence proveniente da diversi vettori: email, strumenti di collaborazione, piattaforme di messaggistica e applicazioni cloud. Deve inoltre fornire informazioni pertinenti sui comportamenti a rischio degli utenti e aiutarti a rafforzare la tua cultura della sicurezza informatica.

La tua soluzione attuale si limita all'email? Ti affidi a soluzioni singole frammentate? Se la situazione è questa, puoi migliorarla. È giunto il momento di valutare l'efficacia della tua sicurezza attuale contro tutte le minacce incentrate sulle persone diffuse tramite l'email e altri vettori.

Consolida le tue difese con Proofpoint

Proofpoint Prime Threat Protection offre una piattaforma pre-integrata di protezione contro le minacce per una sicurezza completa. La soluzione blocca le minacce negli ambienti di lavoro moderni, inclusa l'email e i canali digitali. Non solo ti protegge contro la più ampia gamma di minacce ma lo fa con una precisione del rilevamento senza pari. Ottimizzato dalla piattaforma Proofpoint Nexus AI - un insieme di motori di IA che include modelli linguistici, machine learning, computer vision, grafici relazionali e threat intelligence - Proofpoint Prime offre un'efficacia di rilevamento del 99,999% contro le minacce tradizionali e quelle generate dall'IA.

Fornisce anche informazioni dettagliate sul fattore di rischio umano e rafforza la resilienza degli utenti. Inoltre, ti difende dagli account degli utenti e dei fornitori compromessi per mantenere al sicuro le tue comunicazioni aziendali.

Proofpoint offre l'unica architettura di sicurezza informatica moderna che fornisce un approccio adattivo per proteggere le risorse più importanti e più a rischio della tua azienda: i tuoi collaboratori. Ecco perché più di 2,7 milioni di clienti di tutte le dimensioni, tra cui più di 80 aziende della classifica Fortune 100, si affidano a Proofpoint.

proofpoint.

Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per ulteriori informazioni, visitare il sito: www.proofpoint.com/it.

Seguici : LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →