proofpoint.

EBOOK

2022

La guida strategica definitiva sull'email security

Un approccio incentrato sulle persone per bloccare ransomware, attacchi malware, phishing e frodi via email

proofpoint.com/it

Email: il vettore delle minacce più critico

In tutto il mondo, ogni giorno una battaglia silenziosa ha luogo in uno degli strumenti più familiari e centrali del lavoro moderno: la casella inbox dell'email.

L'email è il principale vettore di invio del malware e un terreno fertile per tutti i generi di minaccia. È attraverso questo mezzo che i criminali informatici hanno maggiori probabilità di raggiungere i loro obiettivi. Gli hacker inducono gli utenti a fare clic su un link non sicuro, a divulgare le proprie credenziali o addirittura a lanciare loro stessi dei comandi (come l'esecuzione di un bonifico o l'invio di file sensibili).

Non è difficile capire perché gli autori degli attacchi preferiscano l'email che utilizza un'architettura vecchia di decenni, non progettata pensando alla sicurezza. È universale e, diversamente da ciò che accade con hardware e infrastrutture informatiche, gli attacchi via email sfruttano delle vulnerabilità a cui non si possono applicare patch: le persone.

La migrazione verso il cloud e il passaggio al telelavoro rappresentano una minaccia ancora più temibile.

Ogni anno le aziende spendono miliardi in strumenti di sicurezza progettati per rafforzare il perimetro della rete, rilevare le intrusioni e mettere in sicurezza gli endpoint. Eppure il volume e il costo del ransomware, della violazione dell'email aziendale (BEC, Business Email Compromise), del phishing delle credenziali di accesso e delle violazioni dei dati a causa del malware non è mai stato così elevato[1].

In effetti, gli attacchi attuali sfruttano la natura umana, non solo la tecnologia, e l'email è il modo più facile per raggiungere gli utenti.

Ecco i risultati di recenti ricerche:

14,8 milioni di dollari
Costo annuale medio del phishing per una grande azienda, ovvero oltre il triplo della media del 2015[2]

86%
delle aziende ha subito attacchi di phishing inviati in blocco nel 2021[3]

77%
delle aziende è stata presa di mira da attacchi BEC nel 2021[4]

78%
delle aziende ha subito attacchi ransomware tramite email nel 2021[5]

85%
delle violazioni dei dati implica un intervento umano[6]

1 Ponemon Institute. "The 2021 Cost of Phishing Study" (Studio 2021 sul costo del phishing), giugno 2021.
2 Ponemon Institute. "The 2021 Cost of Phishing Study" (Studio 2021 sul costo del phishing), giugno 2021.
3 Proofpoint. "State of the Phish 2022.", febbraio 2022.
4 Ibid.
5 Ibid.
6 Verizon, "Data Breach Investigations Report Executive Summary" (Sintesi del report sulle violazioni dei dati), maggio 2021.

È ora di adottare un nuovo approccio. L'attuale panorama delle minacce richiede un cambio di mentalità e una nuova strategia incentrata sulla protezione delle persone anziché dell'infrastruttura.

Che tu sia a capo di un centro operativo di sicurezza multinazionale o di un piccolo team di sicurezza affiatato, considera questa guida come un punto di partenza. Prenderemo in esame i seguenti punti:

- Perché l'email dovrebbe essere la tua principale priorità di sicurezza
- Cosa la rende così difficile da proteggere
- In che modo una sicurezza multilivello integrata e incentrata sulle persone è più efficace
- Come ottimizzare le tue operazioni di protezione dell'email per risparmiare denaro e ottimizzare le misure di risposta

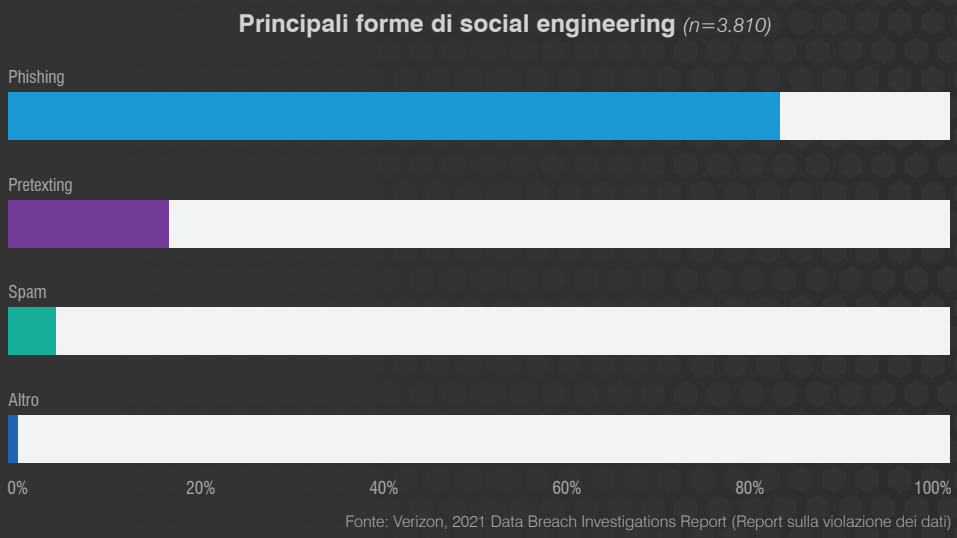


Figura 1. Principali forme di social engineering

SEZIONE 1

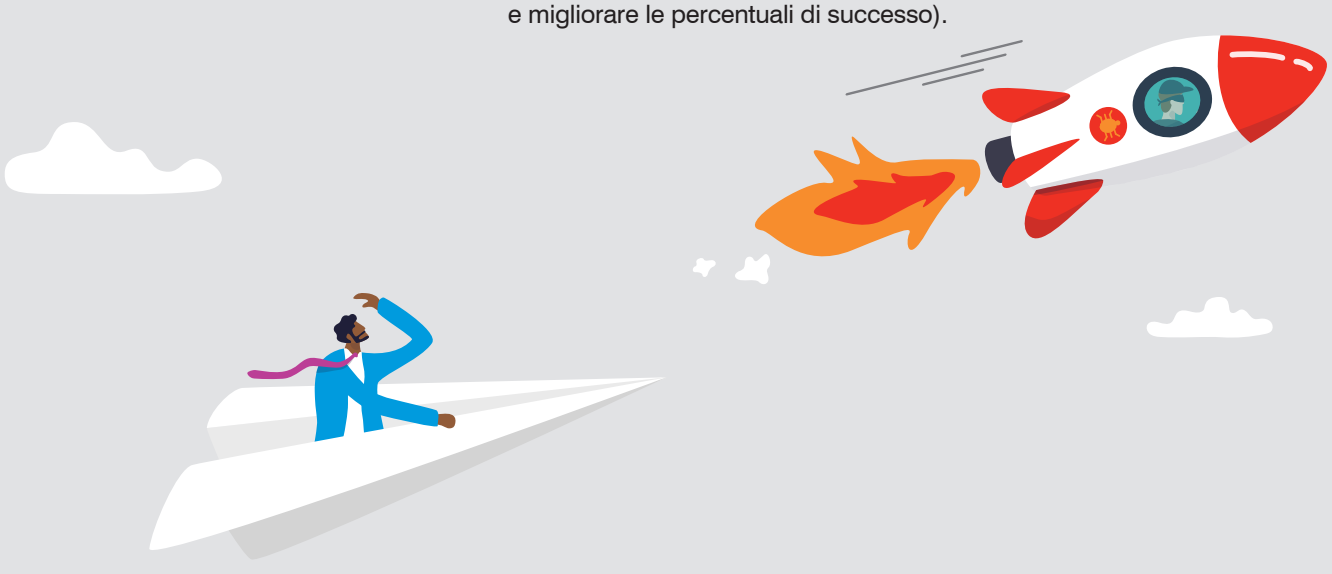
Gli attacchi informatici si stanno evolvendo più velocemente dei meccanismi di difesa tradizionali

La salvaguardia dell'email è fondamentale per proteggere l'azienda, ma si tratta di una sfida complessa.

Ciò è dovuto al fatto che le minacce via email sono numerose e varie. Le tecniche di attacco sono in costante evoluzione e le persone, l'anello debole di ogni azienda, sono prese di mira costantemente.

Non meraviglia che le soluzioni progettate solo due o tre anni fa per contrastare gli attacchi, siano già obsolete.

Questa sezione descrive alcuni dei metodi utilizzati dai criminali informatici per prendere di mira gli utenti (In molti casi, i criminali informatici combinano diverse tecniche per aggirare le difese e migliorare le percentuali di successo).



Ransomware

Il ransomware è una minaccia vecchia ma ancora rilevante. Questo tipo di malware, così chiamato per via del riscatto (ransom in inglese) chiesto alla vittima dopo il blocco dei file, è un problema molto serio per tutte le organizzazioni moderne. È una delle forme di attacco informatico più deleterie.

I gravi incidenti che hanno interessato nel 2021 la fornitura di carburante[7], i prodotti alimentari[8] e la sanità[9] negli Stati Uniti hanno chiaramente dimostrato che nessun obiettivo è irraggiungibile.

Circa tre-quarti degli attacchi ransomware iniziano, direttamente o indirettamente, con un'email di phishing[10]. Queste email inducono gli utenti ad aprire un allegato pericoloso o a fare clic su un URL dannoso.

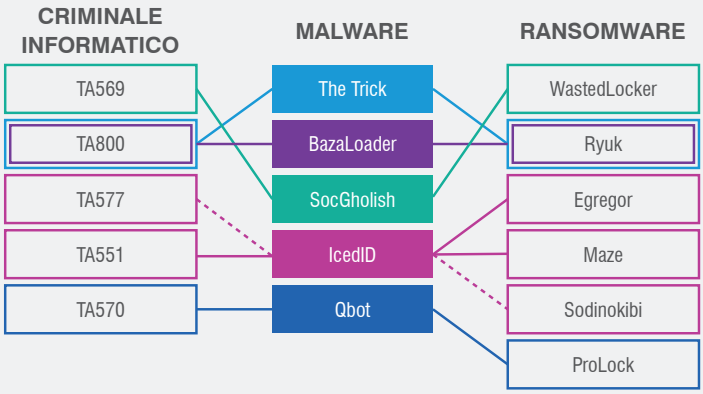


Figura 2. Legami tra criminali informatici, malware iniziale e ransomware

La maggior parte del ransomware viene inviata come infezione secondaria dopo che un sistema è già stato infettato con un trojan o un loader. Molti criminali informatici specializzati in loader o trojan vendono poi questo accesso agli operatori di ransomware. Per la maggior parte delle aziende, la prima linea di difesa contro il ransomware consiste quindi nel proteggersi contro gli altri tipi di malware.

Non esiste necessariamente un legame univoco tra il malware utilizzato per l'accesso iniziale e il ceppo di ransomware che successivamente infetta le vittime. Tuttavia, i ricercatori di Proofpoint e altre aziende del settore hanno identificato delle interessanti associazioni, come mostrato nella figura 2.

7 David E. Sanger, Clifford Krauss, Nicole Perlroth (New York Times) "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." (Un attacco informatico costringe alla chiusura il più grande oleodotto degli USA), maggio 2021.
8 Julie Creswell, Nicole Perlroth, Noam Schreiber (New York Times) "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business." (Un ransomware paralizza delle fabbriche di carne nell'ultimo attacco contro aziende critiche americane), giugno 2021.
9 Nicole Perlroth, Adam Satariano (New York Times) "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks." (Ospedali irlandesi tra le ultime vittime degli attacchi di ransomware), maggio 2021.
10 Unit 42, Palo Alto Networks, "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" (Famiglie di ransomware: dati 2021 a completamento del report sui ransomware di Unit 42), luglio 2021

Frode via email e violazione dell'email aziendale (BEC)

Le truffe legate alla violazione dell'email aziendale note anche come BEC (Business Email Compromise) sono una delle minacce più costose e meno comprese nel campo della sicurezza informatica. Non sempre questa categoria in rapida espansione ottiene un'attenzione pari agli altri reati informatici di alto profilo, anche se, in termini di costo finanziario diretto, la violazione dell'email aziendale li supera facilmente.

Nel solo 2020, le truffe BEC sono costate ad aziende e singoli 1,8 miliardi di dollari[11] (un aumento di oltre 100 milioni dal 2019, somma che rappresenta il 44% delle perdite totali legate al crimine informatico).

Gli attacchi BEC sono difficili da rilevare. Non includono i payload che siamo soliti analizzare come gli URL o gli allegati dannosi. I truffatori sfruttano invece il furto d'identità e altre tecniche di social engineering per ingannare gli utenti.

Molti degli schemi BEC attuali sono estremamente sofisticati, ben finanziati e sostenuti da un'attenta attività di ricerca e pianificazione. Un crescente numero di criminali informatici si concentra sempre più sulle frodi delle fatture dei fornitori e sulle transazioni di grandi dimensioni tra aziende che possono violare.

Gli attacchi BEC sfruttano le debolezze della natura umana e abusano della fiducia delle persone.

Ecco come operano:

1. In primo luogo, i criminali informatici specializzati in attacchi BEC si fingono una persona o un'entità di cui i destinatari possono fidarsi, come un collega, un superiore o un fornitore.
2. I criminali informatici inviano un'email che incita i destinatari a compiere un'azione volta a estorcere denaro o informazioni finanziarie sensibili dell'azienda: bonifici fraudolenti, fatture fasulle, sottrazione di stipendi, modifica delle informazioni bancarie per i pagamenti futuri, e innumerevoli altre tecniche.
3. Quando l'azienda scopre l'errore, spesso è troppo tardi per recuperare il denaro.

TIPI DI ATTACCHI BEC

Gli attacchi BEC possono assumere diverse forme. L'unico limite è la creatività dei criminali informatici. Di seguito sei tipi comuni:

1. **Frode delle fatture.** I criminali informatici inducono le vittime a pagare false fatture o a deviare pagamenti legittimi.
2. **Dirottamento degli stipendi.** In questo schema, i criminali informatici si spacciano per un dipendente e chiedono all'ufficio paghe di dirottare gli stipendi sul loro conto.
3. **Estorsione.** In questo caso, i criminali informatici minacciano di far del male alla vittima in caso di mancato pagamento.
4. **Esche e richieste di favori.** I criminali informatici ingannano le vittime con una semplice domanda come "Ci sei?" prima di eseguire altre forme di attacchi BEC.
5. **Truffa delle carte regalo.** I criminali informatici ingannano i destinatari e li inducono ad acquistare carte regalo e a inviare loro il numero e il codice PIN.
6. **Frode del pagamento anticipato.** Truffa di vecchia data in cui i criminali informatici chiedono alle vittime di sbloccare una cifra di denaro ancora più elevata, che non verrà mai versata.

11 FBI. Internet Crime Report (Report sui crimini di Internet) 2020, marzo 2021.

Violazione/takeover di un account

La violazione degli account consiste nell'ottenere il controllo dell'account di un servizio email o cloud di un utente legittimo, al fine di ottenere l'accesso a una vasta gamma di dati, contatti, voci di calendario e email.

Oltre ai dati dell'utente compromesso, il criminale informatico può utilizzare l'account per impersonare l'utente in attacchi di social engineering, sia all'interno che all'esterno dell'azienda (attacchi BEC, attacchi alla supply chain, ecc.).

I criminali informatici possono accedere a dati sensibili, convincere utenti o partner commerciali esterni a inviare denaro o danneggiare la reputazione e le finanze di un'azienda. Peggio ancora, possono anche installare backdoor per mantenere l'accesso per attacchi futuri.

Anatomia di un takeover degli account

Ecco come si svolge la maggior parte degli attacchi di takeover degli account cloud.

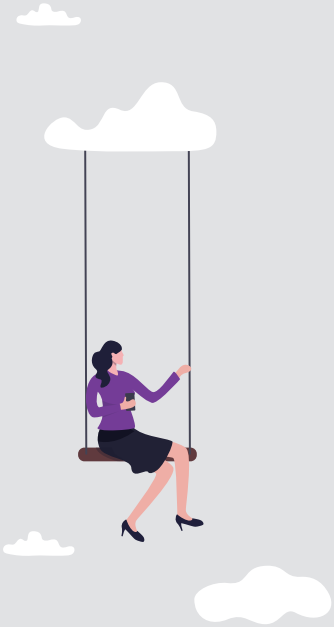
Furto delle credenziali d'accesso. Il criminale informatico si impossessa delle credenziali di accesso dell'utente attraverso il phishing delle credenziali (che da solo rappresenta quasi i due terzi di tutti gli attacchi di phishing), gli attacchi di forza bruta, il riciclaggio delle credenziali d'accesso ("credential stuffing") o il malware che ruba le credenziali.

Infiltrazione. Una volta entrato nell'account dell'utente, il criminale informatico ha accesso all'email, ai contatti, al calendario e ai file della vittima. Il criminale informatico può rubare questi dati direttamente o usarli per impersonare l'utente in modo convincente. Alcuni truffatori rispondono a thread email esistenti o inviano email che contengono malware o URL non sicuri a colleghi e partner commerciali esterni. Fingendo di essere l'utente compromesso, il criminale informatico può prendere di mira altre persone all'interno e all'esterno dell'azienda inviando loro fatture false o istruzioni per il reindirizzamento dei pagamenti. Può anche caricare malware nelle condivisioni di file aziendali o sabotare l'azienda in altri modi.

Persistenza. Spesso, il criminale informatico imposta furtivamente regole di inoltro automatico che gli permetteranno di accedere all'email dell'utente anche se l'utente modifica la password. Avendo accesso a tutte le email in entrata e agli inviti del calendario, il criminale informatico ottiene dettagli chiave che potrà sfruttare per attacchi futuri.

SEZIONE 2

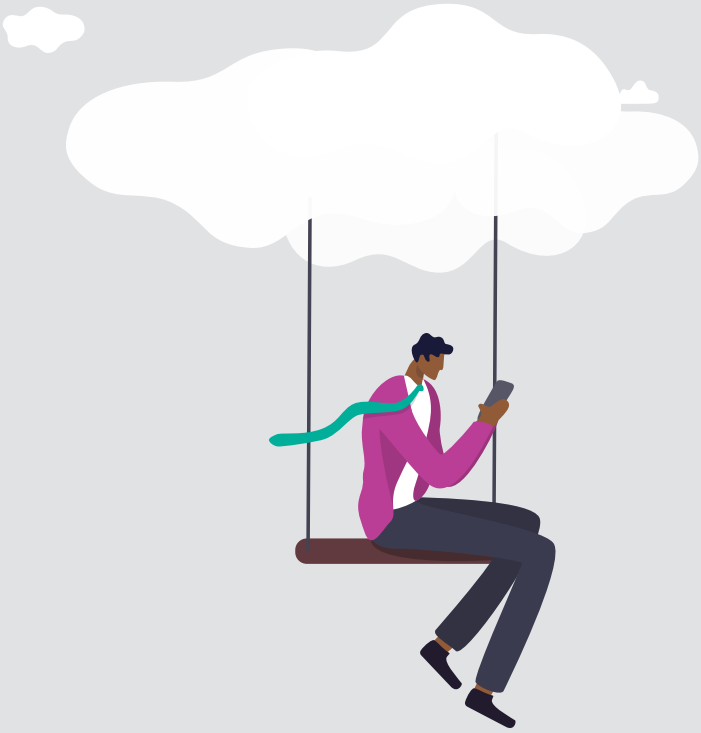
L'evoluzione del panorama delle minacce

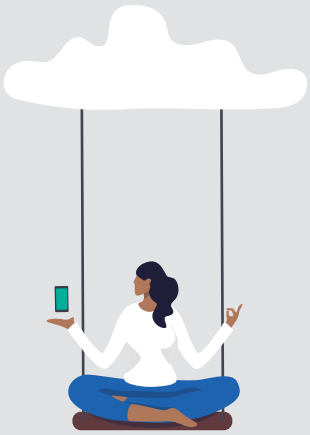


I modelli di telelavoro e ibridi oggi adottati da numerose aziende dipendono dal cloud e dalle tecnologie mobile.

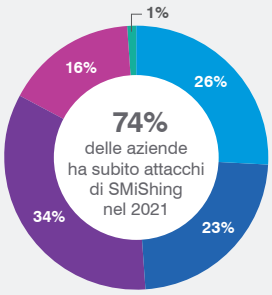
I perimetri rafforzati e le strutture di rete tradizionali appartengono al passato. I dipendenti sono il nuovo perimetro di sicurezza.

Purtroppo, la maggior parte dei budget di sicurezza, che devono tener conto di altre priorità e categorie di prodotti, non sono più all'altezza del compito.

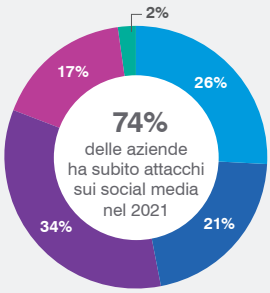




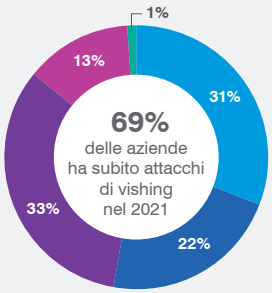
Volume degli attacchi di SMiShing



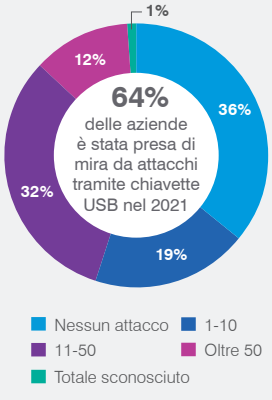
Volume degli attacchi sui social media



Volume degli attacchi di vishing



Volume di attacchi tramite chiavetta USB



Fonte: Report State of the Phish 2022

Gli attacchi prendono di mira le persone, non l'infrastruttura

In un momento in cui le aziende spendono miliardi ogni anno per consolidare la propria infrastruttura, è importante non trascurare i rischi per la sicurezza associati agli utenti. Dopo tutto, i dipendenti sono il punto d'ingresso al tuo ambiente più facilmente accessibile e redditizio.

In base al report di Verizon sulle violazioni dei dati, l'85% delle violazioni dei dati implica un intervento umano[12]. I tuoi utenti devono affrontare un'ondata incessante di link pericolosi, di allegati dannosi, tentativi di furto delle credenziali di accesso, attacchi di social engineering e altre minacce fraudolente.

Gli attacchi spesso coprono diversi vettori

Per prendere di mira le persone è necessario interagire con le persone sulle piattaforme e con gli strumenti che utilizzano. I criminali informatici seguono gli utenti come la loro ombra.

I flussi di lavoro moderni sono dinamici e imprevedibili. Un utente può iniziare una conversazione tramite email, programmare un incontro successivo nella sua applicazione di chat e collaborare su file archiviati nel cloud.

Gli attacchi moderni sono anche dinamici e imprevedibili. Vanno in esecuzione su diversi canali, utilizzano una serie diversificata di tattiche e strumenti e sfruttano tutte le piattaforme che i dipendenti utilizzano per svolgere il loro lavoro.

Un attacco può iniziare con un'email contenente un link che reindirizza a un malware ospitato su un sito di file sharing. Ma può anche assumere la forma di un'applicazione cloud non autorizzata per sottrarre le credenziali d'accesso per compromettere un account legittimo da cui lanciare attacchi BEC.

Questa minaccia è in costante aumento. Spesso, un criminale informatico sofisticato crea il "prodotto" malware e imposta un'infrastruttura tale da trasformarlo in un pacchetto o servizio di facile utilizzo. I criminali informatici meno sofisticati possono noleggiare il servizio per sferrare i propri attacchi, pagandolo per un periodo di tempo prestabilito oppure cedendo una quota per ogni violazione riuscita. In altri casi fungono da distributori, inviando email contenenti il malware e guadagnando una commissione per ogni infezione.

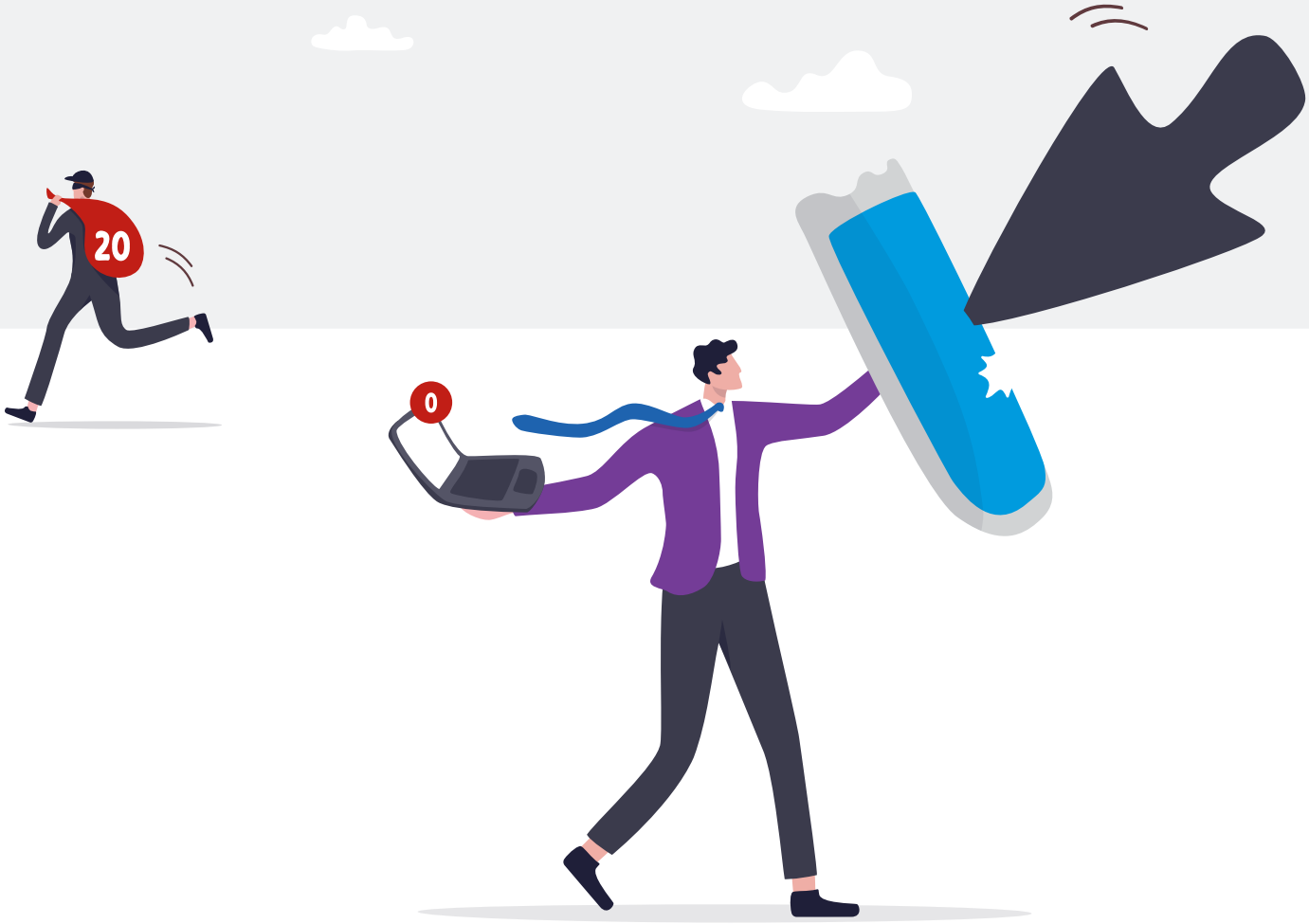
12 Verizon, "Data Breach Investigations Report Executive Summary" (Sintesi del report sulle violazioni dei dati), maggio 2021.

Proteggere ogni vettore non è sufficiente

Le aziende possono essere in grado di capire che le minacce odierne presentano diverse sfaccettature e prendono di mira principalmente le persone, e investire di conseguenza in strumenti di sicurezza per coprire tutti i rischi potenziali. Se questi strumenti non operano in modo coordinato, non possono fornire la visibilità e le informazioni di cui i team della sicurezza hanno bisogno per gestire i rischi.

Immaginiamo una squadra di stelle del calcio che non si allenano insieme, un'orchestra di virtuosi che non sente gli altri strumenti, o un'equipe chirurgica che non riesce a mettersi d'accordo sul trattamento del paziente. Un singolo, anche se estremamente competente, non sarà mai efficace come un insieme ben coordinato.

Oggi, i criminali informatici combinano diverse tecniche per lanciare attacchi più sofisticati. Gli strumenti isolati complicano inutilmente il compito dei team della sicurezza che già faticano a gestire i rischi odierni. Ecco perché la sicurezza incentrata sulle persone richiede un approccio globale e coordinato.



SEZIONE 3

Focalizzazione sugli utenti più a rischio

Il primo passo per proteggere gli utenti consiste nell'identificazione di quelli che rappresentano il rischio maggiore. Ogni azienda può valutare i vari fattori di rischio in modo differente, ma è essenziale che tutti tengano conto della vulnerabilità, degli attacchi e dei privilegi.

La vulnerabilità identifica chi ha la maggiore probabilità di essere colpito da una minaccia. L'analisi di un attacco aiuta a comprendere chi viene preso di mira in azienda, in che misura e da che tipo di minacce. I privilegi contribuiscono a calcolare l'entità dei danni che un attacco potrebbe causare all'azienda.

Concentrati sugli utenti che presentano un rischio più alto del normale, in virtù di una qualsiasi combinazione di questi fattori. Il team della sicurezza e le parti interessate devono dedicare loro un'attenzione prioritaria per comprendere perché sono vulnerabili.

Questo livello di visibilità sui tre aspetti è essenziale per la sicurezza incentrata sulle persone. Senza tale visibilità, le aziende non hanno modo di sapere chi ha bisogno di ulteriori livelli di sicurezza né come meglio proteggerlo.

Vulnerabilità: metodi di lavoro e dove cliccano gli utenti

Quantificare la vulnerabilità non è facile con gli strumenti di sicurezza tradizionali incentrati sulla tecnologia. Un approccio incentrato sulle persone permette invece di misurare come lavorano e su cosa fanno clic gli utenti.

Il modo in cui lavorano comprende gli strumenti, i sistemi e le piattaforme che utilizzano per svolgere il loro lavoro. Dove fanno clic indica la loro sensibilizzazione alla sicurezza e la loro propensione a farsi ingannare dalle tattiche di attacco.

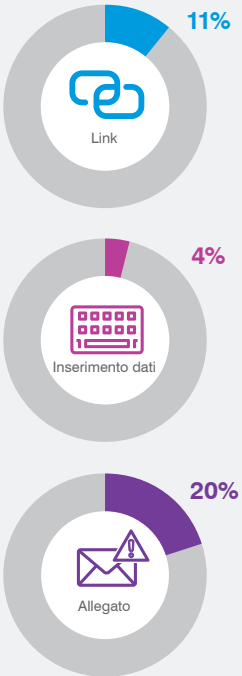
Come lavorano le tue persone

Puoi avere un'idea generale della vulnerabilità degli utenti valutando gli strumenti, le piattaforme e le applicazioni che utilizzano. Per esempio:

- Le applicazioni cloud utilizzate dagli utenti e se sono state convalidate dal dipartimento IT
- Il numero e il tipo di dispositivi utilizzati per accedere all'email
- Il livello di sicurezza di tali dispositivi
- Se applicano buone pratiche digitali (password solide ed uniche, software aggiornati)
- Se utilizzano costantemente l'autenticazione a più fattori per accedere ai sistemi aziendali e persino ai loro account personali.

Una visibilità granulare è essenziale a tale scopo.

Tipi di modelli di phishing: percentuali medie di insuccesso



Fonte: Report State of the Phish 2022

Dove cliccano le tue persone

La vulnerabilità può essere valutata in modo più preciso grazie alla formazione sulla sicurezza, alle simulazioni di attacchi di phishing e all'analisi delle reazioni dei dipendenti alle minacce reali.

Parte essenziale di qualsiasi strategia di sicurezza efficace, la formazione di sensibilizzazione alla sicurezza informatica permette di capire quali sono gli utenti meno preparati a riconoscere le minacce informatiche, a contrastarle e a segnalarle. In generale gli utenti che non ottengono buoni risultati negli esercizi di formazione, o che non li completano, sono più vulnerabili di coloro che ottengono dei punteggi alti.

A meno che i criminali informatici non siano liberi di identificare gli utenti che cliccano su un link, compilano un modulo o aprono un file, le simulazioni di attacchi di phishing sono uno dei modi migliori per valutare il livello di vulnerabilità.

Infine, è fondamentale tenere traccia dei dipendenti che interagiscono con le email dannose note, anche in caso di blocco, isolamento o riscrittura del clic.

Questi dati reali, combinati con le informazioni sulla sensibilizzazione alla sicurezza informatica, offrono una visione completa della vulnerabilità dell'email, monitorando i corsi di formazione completati, le simulazioni di attacchi di phishing e le interazioni con i messaggi dannosi.

Attacchi: strategie utilizzate per colpire le persone

Anche se tutti gli attacchi informatici sono potenzialmente dannosi, alcuni sono più pericolosi, mirati o sofisticati degli altri. Per questo motivo, la valutazione di questo aspetto di rischio può essere più difficile di quanto sembri.

Gli attacchi "classici" ad ampio spettro sono probabilmente più numerosi di altri tipi di minaccia, ma sono ben compresi e più facilmente bloccati.

Altre minacce compaiono in un numero esiguo di attacchi ma rappresentano un problema più serio, a causa del loro livello di sofisticatezza o delle persone che prendono di mira.

Conoscere la differenza è fondamentale per identificare gli utenti che presentano un rischio più elevato. Proofpoint definisce questi utenti VAP (Very Attacked People™ ovvero le persone più attaccate). Una visibilità completa su tutto il traffico email e una ricca threat intelligence sono essenziali per stabilire quali utenti vengono presi di mira e in che misura.

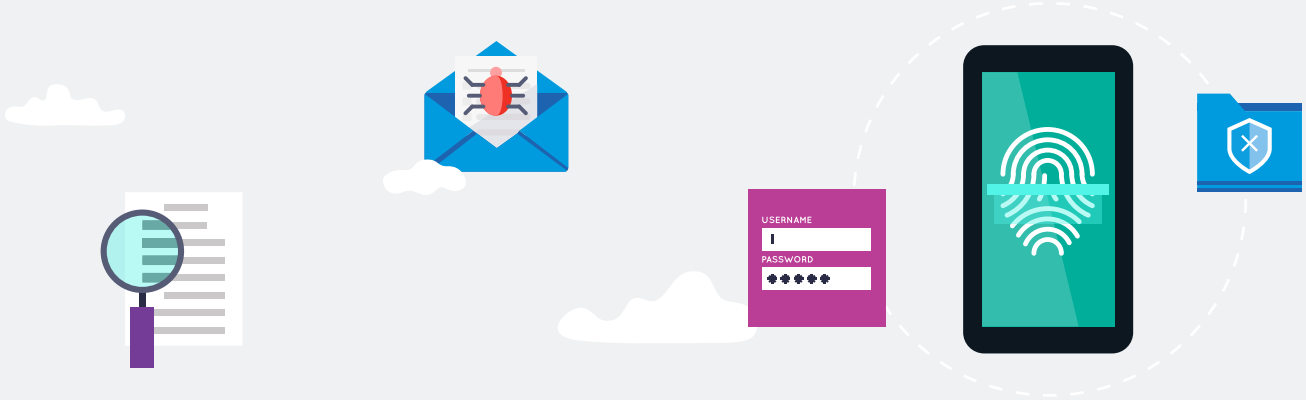
I fattori da ponderare maggiormente in ciascuna valutazione sono:

- Livello di sofisticazione del criminale informatico
- Diffusione e obiettivo degli attacchi
- Tipo di attacco
- Volume complessivo degli attacchi

È inoltre necessario tenere conto del dipartimento, gruppo o divisione cui appartiene il singolo utente.

Per esempio, alcuni utenti potrebbero sembrare non a rischio in base al volume o al tipo di email ostili che ricevono direttamente. Corrono invece un rischio maggiore di altri perché lavorano in un reparto molto esposto agli attacchi e pertanto hanno maggiore probabilità di diventare un bersaglio chiave in futuro.

Una threat intelligence rilevante permette di identificare gli strumenti utilizzati dai criminali informatici e associare gli incidenti senza un'apparente gravità a campagne più ampie.



Privilegi: gli elementi a cui hanno accesso gli utenti

Per un'attenta valutazione dei privilegi degli utenti è necessario partire da un inventario di tutte le risorse preziose a cui accedono: dati, poteri finanziari, relazioni fondamentali e molto altro. Devi sapere dove risiedono i dati più sensibili e quali utenti e applicazioni vi accedono.

Gli utenti che hanno accesso ai sistemi critici o alle proprietà intellettuali, per esempio, potrebbero avere necessità di una maggior protezione, anche se non sono particolarmente vulnerabili o non sono ancora presi di mira.

La posizione di un utente nell'organigramma è naturalmente un fattore da tenere in considerazione nella valutazione dei privilegi, ma non è l'unico, anzi spesso non è neanche il più importante.

Ai fini dello spionaggio industriale una segretaria potrebbe essere un bersaglio più invitante di un dirigente di medio livello, dal momento che la segretaria ha accesso al calendario dell'amministratore delegato. Analogamente, per i ladri d'identità l'infermiere di un ospedale che consulta le cartelle cliniche dei pazienti potrebbe essere più utile di un amministratore delegato.

Per i criminali informatici, chiunque possa aiutarli a raggiungere il loro fine è un obiettivo prezioso.

Proteggere gli utenti con privilegi elevati da attacchi esterni è fondamentale quanto proteggere la tua azienda dagli utenti con privilegi elevati. Nelle mani sbagliate, un accesso con privilegi può causare danni considerevoli, che sia per dolo, negligenza o come risultato di una violazione. Gli account compromessi possono esportare file sensibili o tentare di compromettere o manipolare altri utenti interni.

SEZIONE 4

Creare una difesa incentrata sulle persone

Un approccio incentrato sulle persone garantisce una protezione più ampia perché applica i controlli in base ai rispettivi livelli di rischio. È efficace su tutte le piattaforma utilizzate dai dipendenti, contro tutte le tattiche impiegate dai criminali informatici e su tutti i vettori di minaccia rilevanti.

Livello base: sicurezza per tutti

Dal momento che gli attacchi tramite email assumono molte forme, hai bisogno di un sistema di difesa che blocchi l'intero spettro delle minacce che si propagano via email.

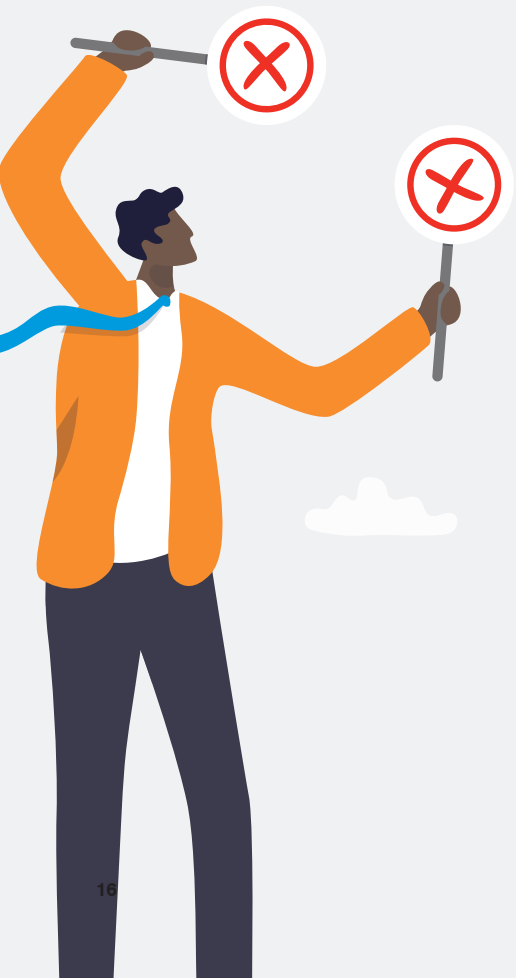
Elenchiamo alcuni dei passaggi essenziali per garantire la protezione dell'email dalle minacce moderne:

- Blocco degli allegati malware e degli URL dannosi prima che raggiungano le caselle di posta in arrivo degli utenti.
- Blocco degli attacchi degli impostori senza payload, come gli attacchi BEC e altre truffe, comprese quelle provenienti dagli account email violati nella tua stessa azienda e presso i fornitori.
- Protezione della navigazione web degli utenti e della loro email personale tramite l'email isolation.
- Rafforzamento della resilienza degli utenti fornendo loro formazione di sensibilizzazione alla sicurezza informatica e informazioni contestuali.
- Applicazione di controlli come l'isolamento del web per isolare le abitudini di navigazione potenzialmente pericolose degli utenti del tuo ambiente.
- Integrazione della protezione dei dati nella tua strategia di protezione delle email.

Blocco degli allegati malware e degli URL dannosi prima che raggiungano le caselle di posta in arrivo degli utenti.

La maggior parte degli attacchi informatici richiede un'azione da parte della vittima designata. In molti casi, si tratta di aprire un allegato o di fare clic su un URL. Ma questi attacchi ad "attivazione umana" possono avere successo solo se la vittima vede il messaggio.

È qui che entra in gioco una soluzione avanzata di protezione dell'email. Bloccando i payload dannosi prima che raggiungano le caselle di posta degli utenti, una soluzione efficace può proteggere la tua azienda da un'ampia gamma di malware, fra cui ransomware, trojan dei servizi bancari, trojan di accesso remoto, ladri di informazioni, downloader, botnet e altro.



Blocco delle minacce fraudolente difficili da rilevare

Sebbene sia essenziale bloccare il malware, alcuni degli attacchi via email più dannosi non utilizzano affatto un payload, ma si affidano al social engineering.

Un esempio sono gli attacchi BEC, un tipo di frode dei bonifici bancari. Secondo l'FBI, gli attacchi BEC sono stati segnalati in tutti i 50 stati americani e in 177 paesi del mondo, con bonifici fraudolenti inviati ad almeno 140 paesi[13].

Negli attacchi BEC e in altre forme di frodi via email, un criminale informatico impersona qualcuno di cui il destinatario si fida, usando un account email falsificato, compromesso o simile a quello reale. Sotto questa falsa identità, il criminale informatico chiede alla vittima di fare qualcosa per proprio conto, ad esempio effettuare un bonifico su un conto corrente estero, inviare file sensibili, ecc.

13 FBI. Internet Crime Report (Report sui crimini di Internet) 2020, marzo 2021.

Le minacce degli impostori sono un problema complesso, dalle molte sfaccettature. Per bloccarle, è necessaria una difesa a più livelli che protegga le email in entrata, in uscita e interne, lavorando in modo completo e coeso.

Oltre alla formazione degli utenti e agli altri controlli di sicurezza descritti in questa sezione, elenchiamo di seguito alcuni elementi chiave di una strategia di difesa contro le email degli impostori.

DMARC

Implementa il protocollo DMARC (Domain-based Message Authentication, Reporting and Conformance) per agevolare l'autenticazione dell'email. Questo protocollo Internet verifica che il mittente di un'email sia davvero chi dice di essere e che sia autorizzato a scrivere per conto dell'azienda.

Con DMARC hai la visibilità su tutte le email inviate usando il tuo dominio di posta, comprese quelle di mittenti terzi affidabili come Marketo, Salesforce, ecc. Con questa visibilità puoi autorizzare tutti i mittenti validi che cercano di inviare un'email per tuo conto e bloccare chi invece vuole usare i tuoi domini affidabili per sottrarti denaro o danneggiare il tuo marchio.

Classificazione dinamica

Sebbene DMARC contribuisca a bloccare le minacce che falsificano il tuo dominio, i criminali informatici usano anche altre tecniche per ingannare gli utenti. Ecco perché l'analisi e la classificazione dinamica dei contenuti delle email rappresentano un altro componente essenziale per bloccare le minacce prive di malware. Questo aspetto della sicurezza dell'email comporta l'analisi del contenuto del messaggio, non solo della sua provenienza. La tua soluzione di protezione dell'email deve quindi essere in grado di rilevare i segnali di frode e bloccare o analizzare ulteriormente qualsiasi contenuto sospetto. La classificazione dinamica analizza e gestisce le email in base a diversi fattori, fra cui i seguenti:

- L'intestazione dell'email, l'indirizzo IP e la reputazione del mittente
- L'analisi dei contenuti guidata dal machine learning per rilevare il dirottamento degli indirizzi di risposta, determinate parole o frasi
- La relazione fra mittente e destinatario
- Informazioni contestuali sul mittente, per esempio se sembra impersonare un fornitore noto

Informazioni sulla protezione delle email interne e i rischi legati ai fornitori

In alcuni casi i criminali informatici non cercano neanche di camuffare il proprio indirizzo email, ma semplicemente si appropriano di un account legittimo appartenente all'azienda, a un fornitore o a un partner. La violazione degli account email (EAC) può essere utilizzata in un'ampia gamma di attacchi, ma è una tecnica d'inganno particolarmente efficace per i seguenti motivi:

- La maggior parte delle aziende non sottopone le email interne allo stesso livello di esame e controlli di sicurezza delle email esterne.
- La maggior parte degli utenti si fida delle email che riceve dalle persone che conosce.
- I criminali informatici che assumono il controllo di un account accedono a una miniera di informazioni relative all'utente violato: con chi è in corrispondenza, di cosa discute e perfino il suo stile di scrittura. Questi dettagli rendono particolarmente convincente l'impersonificazione.

La protezione degli utenti interni e la raccolta di informazioni contestuali sui rischi legati ai fornitori sono fondamentali per una protezione efficace dell'email.

Rafforzamento della resilienza degli utenti con la formazione di sensibilizzazione alla sicurezza

I criminali informatici sono diventati esperti nello sfruttare la natura umana attraverso tecniche di camuffamento convincenti, righe di oggetto accattivanti e irresistibili inviti all'azione. In molti casi, il destinatario di queste email non è l'unico a fare clic su di essere, poiché vengono inoltrate ad altre persone che fanno lo stesso.

La formazione di sensibilizzazione alla sicurezza informatica, soprattutto se parte integrante di una solida cultura della sicurezza, può trasformare i tuoi utenti in una solida ultima linea di difesa. Ma deve essere mirata e sostenuta nel tempo per essere veramente efficace sui dipendenti. Una formazione annuale generica non è sufficiente per cambiare i comportamenti degli utenti né per creare una cultura della sicurezza.

I tag email che forniscono agli utenti informazioni contestuali sulla natura del messaggio possono anche aiutarli a rilevare e segnalare potenziali minacce. Per esempio, un tag che informa l'utente che l'email proviene da un indirizzo esterno o che il dominio dell'email è stranamente simile a quello di un marchio affidabile può aiutarlo a individuare un potenziale tentativo di phishing.

L'isolamento del web e dell'email permette di arginare e analizzare automaticamente i clic legati a messaggi che possono reindirizzare a siti fasulli che richiedono di fornire le credenziali d'accesso, allegati o URL dannosi che contengono malware o altre minacce. Ciò può essere applicato agli utenti più a rischio, ai VIP o a un gruppo di utenti più ampio a seconda del livello di rischio.

15,4 milioni di dollari

di danni per azienda nel 2021

Protezione dei dati dalle violazioni e dalle minacce interne

Nessuna soluzione di protezione dell'email è in grado di fermare da sola tutte le minacce e anche fra i dipendenti meglio addestrati, ci sarà qualcuno che resterà vittima di un attacco di social engineering mirato.

È per questo che ogni sistema di difesa dell'email deve includere gli strumenti per la prevenzione delle fughe di dati, inclusa la crittografia. Anche se qualcosa va storto, una risposta rapida e un sistema DLP impediscono la diffusione dell'attacco e ai criminali informatici di mettere le mani sui tuoi dati più sensibili.

DLP fornisce anche una protezione efficace contro le minacce interne. A nessuno piace pensare ai propri colleghi come a dei potenziali nemici della sicurezza. Tuttavia le minacce interne, che includono dipendenti negligenti, criminali o compromessi, sono costate a ciascuna azienda in media 15,4 milioni di dollari nel 2021[14].

Sia che i dati fuoriescano dal tuo ambiente a causa di una violazione dall'esterno o di un attacco dall'interno, la prevenzione delle fughe di dati contribuisce a proteggerli.

14 Ponemon Institute. "2022 Cost of Insider Threats Global Report" (Report 2020 sul costo delle minacce interne a livello mondiale), gennaio 2022.

Sicurezza adattiva: controlli adattivi per gli utenti più a rischio

Un approccio incentrato sulle persone efficace tiene conto del fatto che alcuni utenti hanno bisogno di ulteriori livelli e controlli di sicurezza. Questi utenti possono essere più suscettibili agli attacchi, essere colpiti più duramente e avere un accesso con privilegi elevati a dati e sistemi sensibili, oppure una combinazione di questi tre fattori, con un conseguente rischio complessivo più alto.

Di seguito i controlli fondamentali da applicare agli utenti più a rischio:

- Formazione mirata di sensibilizzazione alla sicurezza informatica
- Protezioni adattive, basate sui rischi, come misure di autenticazione più severe e web e URL isolation.
- Protezione dalla compromissione (takeover) degli account basati sul cloud.

Formazione mirata di sensibilizzazione alla sicurezza informatica

La formazione di sensibilizzazione alla sicurezza a livello aziendale è utile per identificare le vulnerabilità e per ridurre la superficie di attacco umana. Oltre a rivelare le lacune evidenti, la formazione mirata costituisce anche un'utile misura preventiva per tutti gli utenti a rischio, non solo per quelli più vulnerabili.

Gli utenti che presentano un rischio più elevato a causa del loro profilo di attacco, per esempio, possono beneficiare di una formazione sulle particolari minacce che li colpiscono in modo specifico. Dal canto loro, gli utenti con privilegi elevati possono ricevere una formazione aggiuntiva, legata alle campagne di attacco che puntano ai dati cui hanno accesso.

Controlli adattivi basati sul livello di rischio

Applicare continuamente i controlli di sicurezza più rigorosi a tutti gli utenti non è pratico per la maggior parte delle aziende. Si tratta di un'arma a doppio taglio, poiché controlli inutilmente rigorosi possono ostacolare la produttività degli utenti e incoraggiarli a eludere le misure di sicurezza per svolgere il proprio lavoro.

Tuttavia, a volte un livello di sicurezza in più è necessario. Un operatore in prima linea potrebbe essere particolarmente esposto a un attacco distribuito nel suo settore. Un ricercatore potrebbe essere preso di mira da un criminale informatico particolarmente sofisticato. Oppure un amministratore delegato, data la natura del suo lavoro, potrebbe avere accesso ai dati più sensibili dell'azienda.

In alcuni casi potresti dover rinforzare i requisiti di autenticazione. In altri casi potresti dover usare la web isolation per qualsiasi URL contenuti nelle email su cui l'utente fa clic.

Qualunque forma assuma, la chiave per le protezioni adattive consiste nell'avere una visione puntuale dei fattori di rischio associati ai VAP e nell'applicare controlli commisurati a tali rischi.

Protezione degli account cloud

Per un criminale informatico, la violazione di un account equivale a un invito al furto.

Un account compromesso può essere utilizzato per ogni sorta di attività illecita. Ottenendo il controllo dell'accesso dell'utente giusto, un criminale informatico può spostarsi lateralmente nel tuo ambiente, sottrarre dati oppure ingannare partner commerciali e clienti. Per questo motivo è fondamentale proteggere gli account email, soprattutto gli account cloud.

Risposta: neutralizzazione delle minacce più rapida ed efficace

Gli incidenti di sicurezza sono inevitabili, ma non devono essere per forza catastrofici.

Quando un attacco riesce a violare le difese, la velocità con cui si riesce a limitare e riparare i danni può fare la differenza tra un incidente di piccola entità e un danno duraturo. È per questo che un framework di risposta rigoroso è parte fondamentale di ogni piano per la sicurezza incentrato sulle persone.

In molte aziende la risposta agli incidenti può essere una procedura lenta e impegnativa.

- Indagine e verifica dell'incidente
- Quarantena delle email pericolose
- Contenimento della minaccia
- Identificazione della causa e portata dell'attacco
- Risanamento dei sistemi infettati

Tutti questi passaggi sono fondamentali per una risposta efficace ma, come sanno fin troppo bene i responsabili della sicurezza, la risposta manuale ha dei limiti. Ed è qui che entra in gioco l'automazione.

Processi di risposta efficaci automatizzano le attività laboriose, come la correlazione e l'analisi degli avvisi di sicurezza, la verifica degli indicatori di violazione e la raccolta dei dati forensi. L'automazione agevola inoltre l'applicazione delle misure correttive, come l'aggiornamento del firewall e blocklist delle email, il ritiro delle email dannose dalle caselle di posta in arrivo e la limitazione dell'accesso agli account degli utenti colpiti.

Utilizzata in modo strategico, l'automazione accelera la risposta agli incidenti e consente di riassegnare il personale di sicurezza ai compiti per i quali è più competente. Piuttosto che reagire a una valanga di minacce, può applicare misure di protezione proattive.

Vantaggi dell'intelligenza artificiale e del machine learning

I criminali informatici prendono di mira le persone. Sfruttano le persone. In fin dei conti, loro stessi sono persone.

Per fermarli occorrono soluzioni moderne in grado di adattarsi al comportamento umano. Ecco perché il machine learning è un componente essenziale di qualsiasi strategia di sicurezza incentrata sulle persone.

Il machine learning è più rapido ed efficiente dell'analisi umana manuale. Inoltre, a differenza degli algoritmi tradizionali basati su regole, è in grado di adattarsi rapidamente all'evoluzione delle minacce e delle tendenze.

Il machine learning nella lotta contro gli attacchi BEC

Prendiamo l'esempio degli attacchi BEC. Gli attacchi BEC di frode delle fatture dei fornitori sono tattiche sofisticate e complesse per rubare denaro. Per ingannare le vittime, i criminali informatici presentano una fattura fraudolenta come legittima o reindirizzano un pagamento verso un conto bancario sotto il loro controllo.

Gli strumenti di sicurezza tradizionali faticano a neutralizzare questo tipo d'attacco, poiché sono altamente mirati e non includono alcun carico di virus. Il machine learning può analizzare un'ampia gamma di attributi, tra cui le informazioni di intestazione, il dominio e il corpo del messaggio, per rilevare un messaggio fraudolento o un fornitore compromesso.

Analisi del phishing delle credenziali di accesso

Un altro esempio è quello degli attacchi di phishing delle credenziali d'accesso. Questi attacchi di social engineering spesso utilizzano siti fasulli per incitare le vittime a inserire le loro credenziali d'accesso. Spesso, sono così ben progettati che gli utenti non sanno distinguere tra il sito fasullo e quello legittimo che riproduce. Sfruttando il machine learning e la computer vision per analizzare rapidamente gli URL, i moderni strumenti di sicurezza sono in grado di rilevare e bloccare tutte le email che reindirizzano verso i siti contraffatti. Il machine learning è in grado di rilevare gli URL pericolosi, anche se sono stati registrati di recente, ospitati da siti di condivisione di file o che utilizzano tecniche di elusione avanzate come CAPTCHA.

Garbage in, garbage out (GIGO)

Contrariamente ai sistemi software standard basati su regole, il comportamento del machine learning è guidato dai dati, non viene codificato manualmente. Ciò significa che l'efficacia dei sistemi di machine learning dipende dalle persone che li addestrano e dai dati su cui si basano.

Quando si valutano i fornitori che vantano le loro funzionalità di machine learning, bisogna cercare modelli basati sul machine learning addestrati con un'ampia serie di dati sulle minacce. I dati dovrebbero includere informazioni sulle minacce raccolte dalle principali aziende Fortune 100, Fortune 1000 e Fortune Global 2000, nonché dal maggior numero possibile di fornitori di servizi internet (ISP) e piccole e medie imprese. Questi dati devono coprire diversi vettori d'attacco, tra cui l'email, il cloud, le reti e i social media. Questi canali sono fondamentali in quanto i criminali informatici estendono il loro raggio d'azione oltre le minacce basate su email.

E non bisogna dimenticare il ruolo dei ricercatori sulle minacce esperti nell'attività di addestramento dei modelli di machine learning. Anche i migliori data scientist non possono sviluppare da soli un modello di machine learning efficace. Hanno bisogno delle competenze di professionisti con una vasta esperienza nell'analisi e nella ricerca sulle minacce.

LISTA DI CONTROLLO

Caratteristiche essenziali di una soluzione di sicurezza

La sicurezza incentrata sulle persone è più di uno slogan di marketing: è fondamentalmente un nuovo approccio alle minacce e a come fermarle. Un approccio adeguato deve essere accompagnato da strumenti e funzionalità efficaci.

Elenchiamo di seguito le caratteristiche essenziali di qualsiasi soluzione di sicurezza incentrata sulle persone.

Piattaforma unificata, integrata e scalabile

Una soluzione di sicurezza incentrata sulle persone è più della somma delle sue parti. Gli strumenti isolati possono risolvere alcuni aspetti del tuo problema di sicurezza, ma la lotta contro le minacce moderne richiede un approccio completo e integrato che tenga conto di tute le tattiche, strumenti e vettori utilizzati dai criminali informatici, su tutti i dispositivi, le piattaforme e i canali utilizzati dai tuoi dipendenti.

I prodotti di sicurezza non integrati, tutti con le proprie console, moltiplicano il tempo e le risorse sprecate in flussi di lavoro complessi e ridondanti. I team della sicurezza hanno una visione frammentata delle minacce, si perdono in attività inutili e devono affrontare una gestione sempre più complessa.

Privilegia soluzioni che coprono un'ampia gamma di minacce e si integrano con il tuo ecosistema di sicurezza. In funzione della tua azienda, possono includere componenti come firewall di nuova generazione, sistemi di gestione degli eventi e delle informazioni di sicurezza (SIEM) e strumenti di gestione dell'identità.

Protezione efficace per tutti gli utenti

Il modo migliore per contrastare gli attacchi email è adottare un approccio a più livelli come raccomandato da Gartner e da altri esperti.

Assicurati che le tue difese informatiche siano in grado di neutralizzare le seguenti minacce:

- Spam e email indesiderate inviate in massa
- Attacchi che utilizzano allegati e URL dannosi
- Attacchi privi di payload come gli attacchi BEC
- Violazioni degli account email (EAC) e takeover di account cloud

Gli utenti giocano un ruolo fondamentale negli attacchi email attuali, perciò la formazione di sensibilizzazione alla sicurezza dev'essere una parte essenziale della tua strategia per la sicurezza dell'email. Accertati che il tuo programma di formazione includa quanto segue:

- Brevi sessioni di formazione per promuovere l'impegno e il cambiamento dei comportamenti
- Simulazioni di attacchi di phishing basate su campagne del mondo reale, per preparare gli utenti alle minacce che hanno la maggiore probabilità di dover fronteggiare
- Formazione regolare basata sui dati per gli utenti vulnerabili presi di mira dai criminali informatici o che interagiscono con messaggi di phishing reali
- Tag email che segnalano agli utenti i messaggi sospetti, con meccanismi di segnalazione integrati e feedback agli utenti

Per proteggere i dati rubati, condivisi accidentalmente o divulgati volontariamente da parte di un utente interno, la crittografia e le altre misure DLP sono fondamentali. Una soluzione efficace di prevenzione della perdita di dati può svolgere i seguenti compiti:

- Analizzare e classificare i contenuti in dettaglio e, se necessario, bloccarne l'invio tramite email, il trasferimento nel cloud o il caricamento su chiavetta USB.
- Identificare gli utenti malintenzionati, negligenti o compromessi e aiutare i team IT, delle risorse umane, legali e della sicurezza a intraprendere le misure appropriate per evitare danni duraturi.
- Identificare e proteggere tutte le forme standard di contenuti riservati, come PCI, HIPAA, FINRA e altri materiali soggetti a regolamentazione.
- Reinstradare, crittografare o rifiutare automaticamente quelle email che violano le policy di sicurezza e non solo, avvisando le persone giuste nella tua azienda.

Controlli adattivi per gli utenti più a rischio

Gli utenti più a rischio (in base alla loro vulnerabilità, profilo di attacco e privilegi) richiedono ulteriori controlli di sicurezza. Una soluzione per la sicurezza dell'email incentrata sulle persone ti aiuta a identificare tali VAP e a proteggerli con livelli di sicurezza ulteriori. Scegli una soluzione che offra i seguenti vantaggi:

- Visibilità fruibile sui tuoi VAP grazie a una threat intelligence ricca e puntuale e a un'analisi dettaglia del profilo di rischio degli utenti
- Strumenti di reportistica che semplificano l'analisi e la comunicazione delle vulnerabilità, del profilo di attacco e dei privilegi degli utenti, con un confronto fra i diversi dipartimenti e settori d'attività
- Risposta automatica alle variazioni dei profili di rischio degli utenti grazie al rafforzamento dell'autenticazione, alla riduzione dei privilegi, all'isolamento degli URL, ecc.

Risposta rapida ed efficace in caso di incidente

L'automazione delle fasi fondamentali del processo di risposta agli incidenti permette di ottimizzare le attività critiche che richiedono molte risorse di personale e consente di riassegnare il personale di sicurezza ai compiti per i quali è più competente. Scegli strumenti di risposta automatizzata che offrano:

- Verifica delle minacce, identificazione degli utenti coinvolti e raccolta di dati forensi e contestuali relativi a tali utenti
- Arricchimento degli avvisi di minaccia con informazioni fruibili
- Contenimento e neutralizzazione delle minacce in tutto l'ambiente, nel cloud e in sede. Le misure correttive automatizzate possono includere l'analisi delle email segnalate dagli utenti, l'estrazione di minacce verificate dalle caselle di posta degli utenti e la reimpostazione delle password degli account compromessi.

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 il 75% delle Fortune 100, 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.

0301-001-01-03 03/22