2020

La guida strategica definitiva sull'email security

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

SINTESI

L'email è lo strumento di lavoro più importante di un'azienda. Oggi però è anche il principale vettore di invio di malware.[1] Terreno fertile per le minacce informatiche più dannose e per tutti i generi di frode[2], è diventata il canale con le maggiori probabilità di essere usato dai criminali informatici per violare i loro bersagli. Gli hacker inducono gli utenti a fare clic su un link non sicuro, a divulgare le proprie credenziali o addirittura a lanciare inavvertitamente loro stessi l'attacco (con l'esecuzione di un bonifico o l'invio di file sensibili).

Le minacce sono cambiate, eppure gran parte del settore della cybersecurity è fossilizzato su vecchi modelli di minaccia. Stenta così ad apportare le pur minime migliorie a strategie obsolete, che diventano di giorno in giorno meno efficaci.

È ora di adottare un nuovo approccio. Nel panorama odierno delle minacce, un efficace programma di sicurezza informatica si concentra innanzitutto sulle persone.

Misurazione, analisi e segnalazione dei rischi per gli utenti

Il primo passo per proteggere gli utenti consiste nell'identificare quelli più a rischio. 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 quali minacce. I privilegi contribuiscono a calcolare l'entità dei danni che un attacco potrebbe causare all'azienda.

Gli utenti che presentano un rischio più alto del normale, in base a una qualsiasi combinazione di questi fattori, vengono da noi definiti VAP (Very Attacked People™) ovvero le persone più attaccate. I VAP devono essere identificati rapidamente, in una modalità fruibile dagli addetti alla sicurezza, e segnalate, quando necessario, ad altre persone dell'azienda.

[1] Verizon. "2019 Data Breach Investigations Report" (Report dell'analisi sulle violazioni dei dati), luglio 2019.
[2] Proofpoint. "Report Il Fattore Umano 2019", settembre 2019.

Vulnerabilità: come lavorano le persone e dove cliccano

Per iniziare a valutare la vulnerabilità derivante dal modo in cui lavorano le persone è necessario sapere quali strumenti, piattaforme e applicazioni utilizzano. Per esempio quali app nel cloud vengono usate e se i dispositivi delle persone sono sicuri.

La seconda parte dell'attività di misurazione della vulnerabilità consiste nel capire il grado di suscettibilità degli utenti al phishing e agli altri attacchi informatici.

Il Security Awareness Training permette di capire quali sono gli utenti meno preparati a riconoscere le minacce informatiche, a contrastarle e a denunciarle. In generale gli utenti che non ottengono buoni risultati negli esercizi della formazione, o che non li completano, sono più vulnerabili di coloro che ottengono dei punteggi alti.

Ma la vera prova della resilienza degli utenti è la loro reazione alle tecniche di attacco del mondo reale. Gli attacchi simulati, soprattutto quelli che riproducono tecniche realmente usate, permettono di identificare le persone più suscettibili agli attacchi e a quali tattiche.

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. Informazioni dettagliate sulle minacce e analisi puntuali sono il segreto per determinare quali utenti sono interessati e in che misura.

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.

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 nemmeno 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.

Riduzione dei rischi

L'identificazione dei tuoi VAP è fondamentale per l'email security, ma è solo il primo passo. Un approccio people-centric garantisce una protezione più ampia perché applica i controlli in base ai rispettivi livelli di rischio.

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 malware, come la violazione dell'email aziendale (BEC, Business Email Compromise) e altre truffe, comprese quelle provenienti dagli account email violati nella tua stessa azienda.
- Protezione della navigazione web degli utenti e della loro email personale tramite l'email isolation.
- Rafforzamento della resilienza degli utenti con il Security Awareness Training.
- Protezione dei dati dalle violazioni e dalle minacce interne.

Livello VAP: controlli adattivi per chi ne ha più bisogno

Una strategia efficace per la sicurezza dell'email mette tutti al sicuro, ma un approccio incentrato sulle persone riconosce che alcuni utenti, ovvero i tuoi VAP, hanno bisogno di ulteriori livelli e controlli di sicurezza. Questi VAP 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.

Ecco alcuni dei controlli essenziali per gli utenti identificati come VAP:

- Security Awareness Training mirato.
- 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.

Risposta: azione efficace in caso di incidente

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 breve incidente e un danno duraturo.

In molte aziende la risposta agli incidenti può essere una procedura lenta e impegnativa. 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 degli elenchi di blocco della posta elettronica, 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.

Il risultato

L'email è lo strumento di lavoro più importante, ma oggi è anche il vettore preferito dai criminali informatici per veicolare le minacce. Anche se gli attacchi via email hanno varie forme, svariate origini e obiettivi specifici, hanno tutti una cosa in comune: le persone.

Fondamentalmente gli attacchi via email hanno lo scopo di indurre le persone a fare qualcosa che non dovrebbero: aprire un allegato dannoso, fare clic su un URL non sicuro, inviare informazioni sensibili oppure effettuare un bonifico verso un conto corrente fraudolento. È per questo che per proteggere l'email è necessario un approccio incentrato sulle persone.

Con la strategia, gli strumenti, le analisi e la formazione giusti, le aziende possono gestire i rischi inerenti all'email e salvaguardare il canale più importante delle comunicazioni aziendali.

INTRODUZIONE

L'email è di gran lunga il principale vettore delle minacce

In tutto il mondo, ogni giorno la battaglia per i dati aziendali ha luogo in uno degli strumenti più familiari e centrali del lavoro moderno: la casella inbox della posta elettronica.

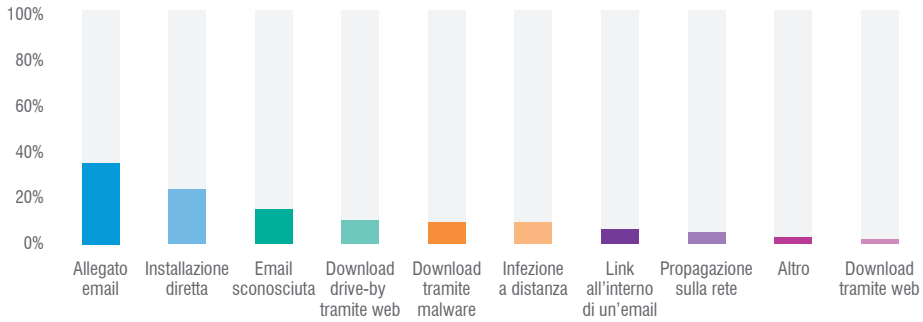
In qualità di principale vettore di invio del malware[3] e di terreno fertile per tutti i generi di minaccia[4], l'email è il canale con le maggiori probabilità di essere usato dai criminali informatici per violare i loro bersagli. Gli hacker inducono gli utenti a fare clic su un link non sicuro, a divulgare 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 dal caso di hardware e infrastrutture informatiche, gli attacchi via email sfruttano delle vulnerabilità a cui non si possono applicare patch: le persone.

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. Ma il vero obiettivo degli attacchi attuali è la natura umana, non solo la tecnologia, e un'email è il modo più facile per colpirla.

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.

Principali vettori di distribuzione del malware



Fonte: Verizon, 2019 Data Breach Investigations Report

Considera questa guida come un punto di partenza. Imparerai:

- perché l'email dovrebbe essere la tua principale priorità di sicurezza;
- cosa la rende così difficile da proteggere;
- in che modo la sicurezza incentrata sulle persone è più efficace e più conveniente rispetto agli approcci basati sul perimetro della rete che non sono efficaci contro le minacce odierne, volte a colpire le persone.

IN CIFRE

94%

degli attacchi esterni inizia con la ricezione di un'email.[5]

27%

degli attacchi esterni che hanno portato a una violazione dei dati sono stati sferrati utilizzando credenziali rubate, spesso ottenute con una semplice email di phishing.[6]

26 miliardi di dollari

Le perdite potenziali dovute alle violazioni dell'email aziendale e degli account hanno toccato i 26 miliardi di dollari in tutto il mondo[7].

90%

del malware rilevato viene recapitato via email[8].

47 tentativi di frode via email

Le aziende colpite hanno subito in media 47 frodi via email nel solo primo trimestre del 2019[9].

Tre volte tanto

Il costo medio in dollari sottratto in attacchi di violazione dell'email aziendale (BEC), un tipo di frode via email, è stato pari a 24.439 dollari, più del triplo del valore della violazione media di dati.[10]

3 Verizon. *"2019 Data Breach Investigations Report"*, luglio 2019.
4 Proofpoint. *"Report Il Fattore Umano 2019"*, settembre 2019.
5 Verizon. *"2019 Data Breach Investigations Report"*, luglio 2019.
6 Forrester Research. *"The Forrester Wave: Enterprise Email Security (sicurezza dell'email aziendale) secondo trimestre 2019"*, maggio 2019.
7 FBI. *"Business Email Compromise: the $26 billion scam."* *(Violazione dell'email aziendale: la truffa da 26 miliardi di dollari)*, settembre 2019.
8 Verizon. *"2019 Data Breach Investigations Report"*, luglio 2019.
9 Proofpoint. *"Report trimestrale sulle minacce primo trimestre 2019"*, maggio 2019.
10 Verizon. *"2019 Data Breach Investigations Report"*, luglio 2019.

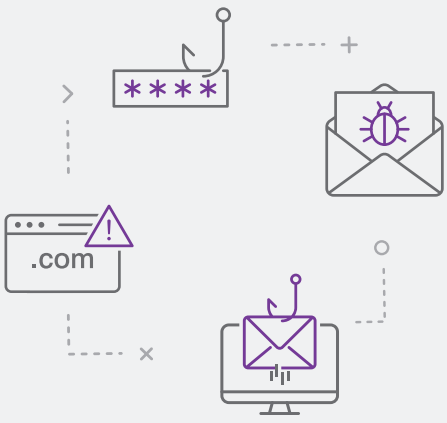
Gli attacchi via email si stanno evolvendo più velocemente dei meccanismi di difesa

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.

Tecniche di attacco via email



Ecco alcuni dei modi in cui i criminali informatici colpiscono le persone tramite l'email.

Malware: codice dannoso che infetta PC e server. Può essere distribuito come file allegato, come collegamento a un URL pericoloso o come download secondario da parte di un malware già installato nei sistemi infettati.
Phishing: email dannose concepite per indurre gli utenti a fare ciò che vogliono i cyber criminali, come digitare le credenziali di accesso a un account, inviare informazioni sensibili o anche eseguire un bonifico (vedi "Frode via email" sotto).

Frode via email: tipo di phishing concepito per indurre le persone a eseguire un bonifico o a rivelare informazioni sensibili a beneficio dell'autore dell'attacco. Generalmente la frode via email non include un malware, ma si basa sul social engineering per persuadere l'obiettivo dell'attacco ad agire per conto dei criminali informatici. Questi attacchi solitamente visualizzano dei nomi fuorvianti, usano lo spoofing del dominio o i domini lookalike (o domini cugini) per far sì che i destinatari si fidino del mittente.

Phishing interno: phishing che usa un account email violato per colpire gli utenti dello stesso dominio email, solitamente i colleghi della vittima. Questa forma di phishing è efficace perché la maggior parte delle aziende non cerca le minacce provenienti dal proprio dominio e i destinatari danno per scontata l'affidabilità delle email che apparentemente provengono dai colleghi.

Phishing della webmail personale: attacchi che colpiscono gli utenti tramite i loro account webmail personali. Molte persone accedono alla propria email personale sul luogo di lavoro, esponendo il proprio datore di lavoro alle minacce provenienti da questo vettore spesso non protetto.

Perché è necessario un approccio incentrato sulle persone

I criminali informatici hanno spostato la loro attenzione dall'infrastruttura alle persone. Di conseguenza il tradizionale modello di sicurezza informatica basato sul perimetro è diventato totalmente obsoleto, ammesso che abbia mai funzionato veramente.

Oggi non c'è più un perimetro da difendere. Le persone si muovono e accedono ai dati aziendali da qualsiasi luogo con ogni sorta di dispositivi, reti e piattaforme esterne alla rete aziendale tradizionale.

L'adozione diffusa del cloud non ha fatto che amplificare questo fenomeno. Anche se l'infrastruttura del cloud è sicura, le persone che la utilizzano sono umane.

È per questo che, per essere efficace, una qualsiasi strategia di protezione informatica deve concentrarsi innanzitutto sulle persone.

Il modello VAP (Vulnerabilità, Attacchi e Privilegi)

Così come ogni persona è unica, lo sono anche il suo valore per i criminali informatici e il rischio per i propri datori di lavoro. Ogni persona ha delle abitudini digitali distinte e differenti punti deboli, per cui viene presa di mira dai pirati informatici in maniera differenziata e con un'intensità variabile. Possiede inoltre specifici contatti professionali e privilegi d'accesso ai dati nella rete e nel cloud.

Insieme, questi fattori compongono il rischio complessivo di un utente in quello che definiamo indice VAP (vulnerabilità, attacchi e privilegi).

Vulnerabilità

La vulnerabilità degli utenti inizia con il loro comportamento digitale: come lavorano e dove cliccano. In alcuni casi, accedono all'email aziendale tramite un dispositivo personale non gestito. Potrebbero servirsi dell'archiviazione di file in cloud e installare componenti aggiuntivi di terze parti nelle loro app cloud. Oppure potrebbero essere particolarmente ricettivi rispetto alle tattiche di phishing delle email degli aggressori.

Attacchi

Oggigiorno gli attacchi informatici sono incessanti, assumono molte forme e cambiano in continuazione. È essenziale capire non solo chi è preso di mira in azienda, ma anche come, da chi e se l'attacco fa parte di una campagna più vasta. Per esempio, un utente colpito da un numero ridotto di minacce molto avanzate, può costituire un rischio maggiore di qualcuno che sia oggetto di una campagna di attacchi di massa indiscriminata.

Privilegi

Per privilegi si intendono tutti gli elementi potenzialmente preziosi a cui le persone hanno accesso, tra cui dati, autorizzazioni finanziarie, relazioni chiave, ecc. Valutare tale aspetto è essenziale perché riflette il potenziale guadagno per i criminali informatici e il potenziale danno che le aziende subirebbero se venissero violate.

Misurazione, analisi e segnalazione dei rischi per gli utenti

Il primo passo per proteggere gli utenti consiste nell'identificazione di quelli più a rischio. 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 quali minacce. I privilegi contribuiscono a calcolare l'entità dei danni che un attacco potrebbe causare all'azienda.

Gli utenti che presentano un rischio più alto del normale, in base a una qualsiasi combinazione di questi fattori, vengono da noi definiti VAP (Very Attacked People™) ovvero le persone più attaccate. I VAP devono essere identificati rapidamente, in una modalità fruibile dagli addetti alla sicurezza, e segnalati, quando necessario, ad altre persone dell'azienda.

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

Non è facile valutare le vulnerabilità degli utenti con i tradizionali strumenti di sicurezza focalizzati sulla tecnologia. Un approccio incentrato sulle persone permette invece capire come lavorano gli utenti e su cosa fanno clic.

Questi metodi di lavoro includono gli strumenti, i sistemi e le piattaforme che utilizzano per svolgere il proprio lavoro. Gli elementi su cui fanno clic sono una misura della loro sensibilizzazione alla sicurezza e della propensione a farsi ingannare dalle minacce.

Come lavorano le tue persone

La valutazione della vulnerabilità derivante dal modo in cui lavorano le persone inizia con il sapere quali strumenti, piattaforme e applicazioni utilizzano. Ecco qualche esempio:

- Le applicazioni cloud utilizzate
- Il numero e il tipo di dispositivi utilizzati per accedere all'email
- Il livello di sicurezza di tali dispositivi
- L'implementazione di buone pratiche digitali
- L'uso dell'autenticazione a più fattori

Una visibilità granulare è essenziale a tale scopo.

Dove cliccano le tue persone

La seconda parte dell'attività di misurazione della vulnerabilità consiste nel capire il grado di suscettibilità degli utenti al phishing e agli altri attacchi informatici.

Il Security Awareness Training, una parte essenziale di qualsiasi efficace strategia di sicurezza, 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.

Ma la vera prova della resilienza degli utenti è la loro reazione alle tecniche di attacco del mondo reale.

Senza far entrare i pirati informatici né vedere chi apre un file di malware o esegue un bonifico a favore di un criminale (situazione non ideale per ovvie ragioni), le simulazioni del phishing sono il modo migliore per valutare questo aspetto della vulnerabilità.

Gli attacchi simulati, soprattutto quelli che riproducono tecniche realmente usate, permettono di identificare le persone suscettibili agli attacchi e a quali tattiche. La persona che apre un'email di phishing simulato e il relativo allegato è quella più vulnerabile. Un utente che invece la ignora riceve una valutazione più bassa. Infine, gli utenti che segnalano l'email al reparto sicurezza o all'amministratore della posta elettronica vengono considerati i meno vulnerabili.

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 target.

Conoscere la differenza è fondamentale per identificare gli utenti che presentano un rischio più elevato. Informazioni dettagliate sulle minacce e analisi puntuali sono il segreto per determinare quali utenti sono interessati e in che misura.

I fattori da ponderare maggiormente in ciascuna valutazione degli utenti 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.

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, accesso a risorse finanziarie, relazioni chiave e molto altro.

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.

RECENTI ATTACCHI BEC ED EAC

Ecco alcune delle vittime eccellenti che sono state recentemente oggetto di attacchi BEC ed EAC.

Barbara Corcoran ospite di "Shark Tank":
400.000 dollari

Governo di Puerto Rico:
4 milioni di dollari

Nikkei America:
29 milioni di dollari

Red Kite Community Housing:
1,2 milioni di dollari

Distretto scolastico indipendente di Manor (Texas):
2,3 milioni di dollari

Toyota Boshoku:
37 milioni di dollari

Contea di Cabarrus, N.C.:
2,5 milioni di dollari

Ocala, Florida.:
750.000 dollari

Museo Rijksmuseum Twenthe:
3,1 milioni di dollari

So chi sono i miei VAP. E ora? People-centric security in azione

L'identificazione dei tuoi VAP è fondamentale per la sicurezza dell'email, ma è solo il primo passo. L'approccio people-centric mantiene una protetezione globale perché applica i controlli in base ai rispettivi livelli di rischio.

Livello base: sicurezza per tutti

La sicurezza della posta elettronica inizia da una protezione robusta per ogni utente. Poiché 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 gli 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 un gateway di posta sicuro. Bloccando il malware prima che raggiunga le caselle di posta degli utenti, il gateway protegge le aziende da un'ampia gamma di minacce, fra cui ransomware, banking trojan, remote-access trojan, information stealers, downloader, botnet e altro.

Blocco degli attacchi degli impostori senza malware

Sebbene sia essenziale bloccare il malware, alcuni degli attacchi via email più dannosi non lo utilizzano affatto, e invece si affidano al social engineering.

Un esempio è la violazione dell'email aziendale (BEC), un tipo di frode bancaria. Secondo l'FBI, le perdite potenziali derivanti dagli attacchi BEC dal 2016 ammontano a più di 26 miliardi di dollari. L'agenzia di intelligence interna afferma che 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[11].

Negli attacchi BEC e in altri attacchi privi di malware, il truffatore 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.

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.

[11] FBI. *"Business Email Compromise: the $26 billion scam." (Violazione dell'email aziendale: la truffa da 26 miliardi di dollari),* settembre 2019.

DMARC

Implementa il protocollo di autenticazione dell'email DMARC. 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 o SurveyMonkey. 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 truffatori 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. Per questo motivo la tua soluzione di protezione dell'email deve 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:

- Il contenuto, l'intestazione e l'indirizzo IP di un'email
- La reputazione del mittente
- La relazione fra mittente e destinatario

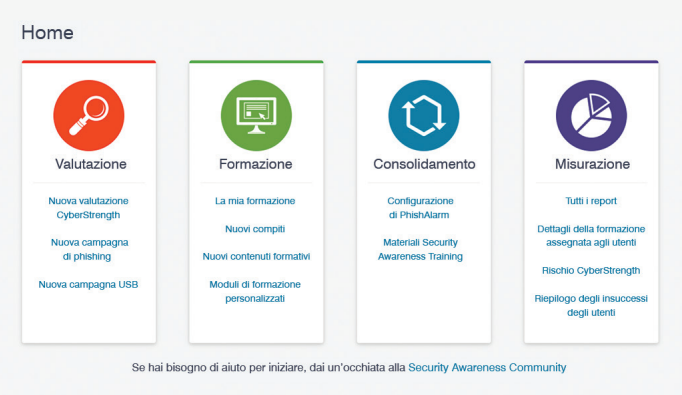
Protezione delle email interne

In alcuni casi gli autori degli attacchi non cercano neanche di camuffare il proprio indirizzo email, ma semplicemente si appropriano di un account legittimo. 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.

Rafforzamento della resilienza degli utenti con il Security Awareness Training

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. Come spieghiamo nel report **Il Fattore Umano 2019**, le email di phishing più efficaci vengono cliccate in media 1,6 volte. Ciò significa che per alcune di esse il destinatario non solo ha fatto clic sull'email, ma l'ha anche inoltrata ad altri che hanno fatto clic a loro volta[12].



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 disattenti, criminali o compromessi, hanno provocato nel 2018 danni per 8,76 milioni di dollari[13].

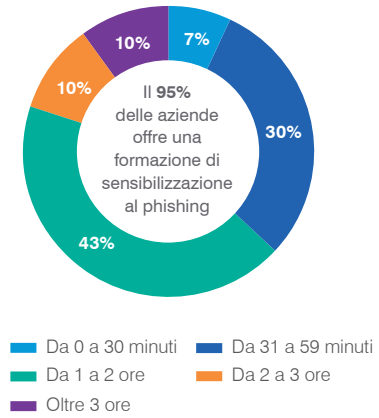
Sia che i dati fuoriescano dal tuo ambiente a causa di una violazione dall'esterno o di un attacco dall'interno, la prevenzione delle fughe di dati contribuisce a proteggerli.

[12] Proofpoint. *"Il fattore umano 2019",* settembre 2019.
[13] Ponemon Institute. *"2018 Cost of Insider Threats: Global." (Report gobale sul costo delle minacce internet),* aprile 2018.

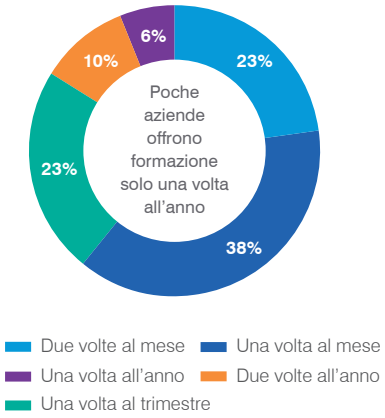
CONSAPEVOLEZZA E PREPARAZIONE

Di seguito riportiamo come le aziende implementano programmi Security Awareness Training.

Tempo dedicato ogni anno ai corsi Security Awareness Training



Frequenza dei corsi Security Awareness Training



Il livello adattivo: controlli per i VAP

Una strategia efficace per l'email security abilita una protezione totale, ma un approccio incentrato sulle persone riconosce che alcuni utenti, ovvero i tuoi VAP, hanno bisogno di ulteriori livelli e controlli di sicurezza. I VAP possono essere più vulnerabili agli attacchi, essere colpiti più pesantemente, avere privilegi elevati per dati e sistemi sensibili oppure una combinazione di queste tre caratteristiche.

Security Awareness Training mirato

Un Security Awareness Training 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 i VAP, non solo per i più vulnerabili.

Gli utenti identificati come VAP 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.

Protezioni adattive, risk-based

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

La violazione degli account email aziendali (EAC - Email Account Compromise), e in particolare degli account cloud, sta rapidamente diventando un vettore di attacco privilegiato. Per un criminale informatico, la violazione di un account equivale a un invito al furto.

Un account email violato può essere utilizzato per ogni sorta di attività illecita. Ottenendo il controllo dell'account giusto, un cyber criminale 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.

Una situazione di compromissione: metodi utilizzati dai criminali informatici per prendere il controllo degli account cloud

Nelle email BEC, l'account della email non solo *sembra* legittimo, ma lo è veramente. Ecco alcuni dei metodi utilizzati dai criminali informatici per assumere il controllo degli account dei tuoi utenti.

Attacchi di tipo brute-force. Solitamente usando uno script automatizzato, il criminale informatico cerca di accedere a molti account con la stessa combinazione nome utente/password, finché non ci riesce.

Attacco ripetitivo (replay attack). Sebbene questa pratica sia sconsigliata, molte persone usano la stessa password per diversi account. Se una di queste password viene trafugata durante una violazione dati non correlata, qualsiasi altro account che utilizza lo stesso nome utente (spesso un indirizzo email) e password è a rischio.

Phishing. Il phishing delle credenziali è ancora un modo efficace per ottenere la password di una vittima. Senza controlli aggiuntivi come l'autenticazione a più fattori (MFA), la perdita di credenziali può portare alla violazione degli account.

Risposta: azione efficace in caso di incidente

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
- 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: comprendere, stabilire le priorità e contrastare le reali minacce per la sicurezza.

Checklist: caratteristiche essenziali di una soluzione di sicurezza

Il settore della sicurezza informatica sta lentamente accettando l'idea che gli attacchi odierni colpiscono le persone, non la tecnologia. Ma la sicurezza incentrata sulle persone è più di uno slogan di marketing: è fondamentalmente un nuovo approccio alle minacce e a come fermarle.

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

Protezione efficace dell'email per tutti gli utenti

Il modo migliore per respingere gli attacchi sferrati tramite l'email è quello di fermarli prima che raggiungano la casella di posta in arrivo. Scegli una soluzione in grado di riconoscere e bloccare un'ampia gamma di attacchi e tattiche, fra cui:

- Attacchi basati su malware che usano allegati e URL
- Attacchi privi di malware come la violazione dell'email aziendale (BEC)
- Violazioni degli account email (EAC) e takeover di account cloud

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

- Formazione basata su metodologie comprovate e attacchi reali
- Simulazioni di attacchi di phishing ispirate da campagne del mondo reale, per preparare gli utenti alle minacce che hanno la maggiore probabilità di dover fronteggiare
- Formazione ulteriore per quegli utenti che hanno mostrato lacune o vulnerabilità critiche

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 DLP può svolgere i seguenti compiti:

- Analizzare in dettaglio il contenuto delle email e, quando necessario, impedire l'invio di parti delle email in uscita e di contenuti simili
- 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 i VAP

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 informazioni ricche e puntuali 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 e ri-autenticazione degli account in tutto l'ambiente, nel cloud e in sede.

Per saperne di più

Per saperne di più sull'adozione di un approccio alla sicurezza dell'email people-centric, visita il sito **www.proofpoint.com/it/products/email-protection/email-security-and-protection**.

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**.

proofpoint.

0301-001-01-01 03/20