proofpoint.

EBOOK

Misurare l'efficacia della sensibilizzazione alla sicurezza per una protezione sostenibile

Una guida per i CISO e i responsabili IT

proofpoint.com/it

Introduzione

Questo nuovo decennio ha gettato i responsabili IT e della sicurezza in un turbinio di di sfide e cambiamenti. Dal repentino passaggio al telelavoro a seguito della pandemia all'aumento degli attacchi di phishing che hanno cercato di sfruttare a loro vantaggio la situazione, il 2020 ha segnato l'inizio di una nuova era per la sicurezza informatica.

In una recente indagine tra i professionisti della tecnologia, il 57% ha affermato che la propria azienda è stata vittima di un attacco di phishing nel 2020, rispetto al 55% dell'anno precedente[2]. E la situazione non accenna a migliorare. La crescente ondata di ransomware e violazioni di dati di alto profilo costringe le aziende a limitare i rischi a cui sono esposte.

Le violazioni sono una vera catastrofe per le vittime, ma possono anche innescare discussioni necessarie tra i dirigenti e il consiglio di amministrazione in merito alla sicurezza informatica e al ruolo che il comportamento degli utenti gioca nella protezione dell'azienda.

La maggior parte delle minacce trasmesse via email richiede generalmente una qualche forma di attivazione da parte dell'utente. Questo è il motivo per cui programmi di sensibilizzazione alla sicurezza efficaci, insieme ai cambiamenti nel comportamento degli utenti, possono giocare un ruolo di primo piano nella riduzione dei rischi[3]. Molti responsabili della sicurezza lo sanno. Ma misurare e comunicare l'impatto del tuo programma di sensibilizzazione alla sicurezza ai dirigenti non è sempre così semplice.

Questo eBook esamina i pro e i contro dei programmi di sensibilizzazione alla sicurezza per una protezione sostenibile dell'azienda. Delinea le strategie per ottenere, misurare e mantenere l'adesione delle parti interessate e mostra come trarre il massimo da questo investimento critico.

85%

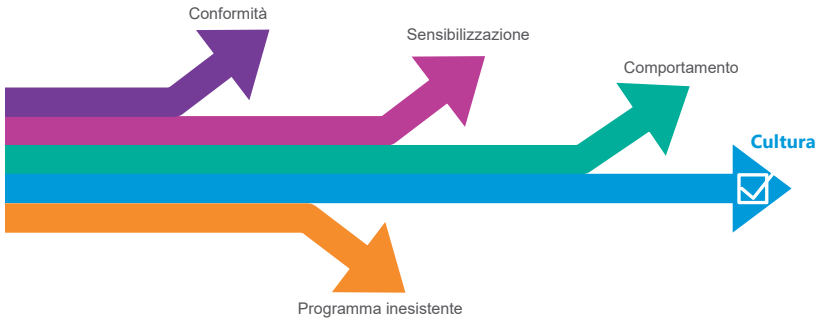
dei direttori finanziari con sede negli Stati Uniti ha riportato che il loro consiglio di amministrazione ha affrontato formalmente il problema dei recenti attacchi di cybersecurity e le conseguenze degli eventi[1].

[1] CNBC. "CNBC Global CFO Council Survey." (Sondaggio condotto dal consiglio mondiale dei CFO di CNBC), luglio 2021
[2] Proofpoint, "State of the Phish 2021.", febbraio 2021
[3] Proofpoint, "Proteggere lutente finale", febbraio 2019

L'importanza della sensibilizzazione alla sicurezza

La sensibilizzazione alla sicurezza non è una priorità di bilancio rispetto ai controlli tecnici. Ma questo non è un approccio corretto. Grazie a parametri convincenti e argomentazioni efficaci, puoi raggiungere due obiettivi fondamentali. In primo luogo puoi ridurre i rischi in modo tangibile e, altrettanto importante, puoi dimostrare al CISO e alle altre parti interessate l'importanza della sensibilizzazione alla sicurezza come strumento essenziale per garantire la protezione dell'azienda.

Le preoccupazioni della direzione saranno diverse a seconda dello stato e degli obiettivi del tuo programma. Per esempio, i programmi focalizzati sulla conformità si concentrano sul rispetto delle normative. Per contro, l'efficacia dei programmi basati sui comportamenti viene misurata in base a parametri come la percentuale di clic o il tasso di segnalazione durante le simulazioni.



Livelli di maturità dei programmi di sensibilizzazione alla sicurezza

Percorso di creazione di una cultura della sicurezza

La maggior parte delle aziende (98%) dispone di un programma di formazione di sensibilizzazione alla sicurezza[4]. Tuttavia il 64% di loro propone solo sessioni di formazione formale (in presenza o online), perdendo altre opportunità per migliorare la sensibilizzazione alla sicurezza. Solo il 23% combina tutti i tipi di contenuti disponibili (valutazioni, formazione e comunicazioni).

Una formazione continua tramite diversi canali può migliorare la memorizzazione di quanto appreso e i risultati del programma di sensibilizzazione alla sicurezza. Questo è il motivo per cui consigliamo vivamente di utilizzare il maggior numero di canali possibile.

Un punto fondamentale per una migliore sensibilizzazione alla sicurezza è creare una cultura in cui i dipendenti sono convinti che una sicurezza solida sia un bene non solo per l'azienda, ma anche per loro stessi. Per raggiungere questo obiettivo, puoi combinare diverse attività per aumentare la sensibilizzazione, modificare i comportamenti e incoraggiare i dipendenti a combattere i criminali informatici. Ciò significa proporre una formazione pertinente e utile agli utenti in modo continuativo e non solo una o due volte all'anno.

Approcci attuali alla sensibilizzazione alla sicurezza[5]:

29%
Solo simulazioni di attacchi di phishing

41%
Solo sessioni di formazione formale

7%
Solo contenuti informativi

23%
Combinazione di tipi di contenuti diversi

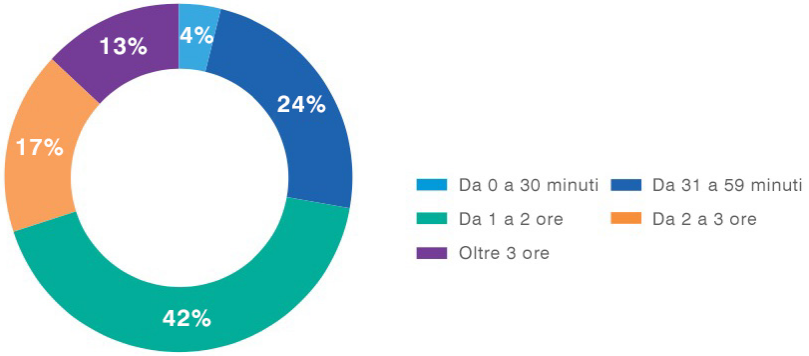
[4] Proofpoint. "State of the Phish 2021.", febbraio 2021
[5] Ibid.

Come sviluppare un programma efficace

Più tempo un'azienda dedica al suo programma di sensibilizzazione alla sicurezza, migliori sono le possibilità che sia efficace.

Tempo dedicato dalle aziende alla sensibilizzazione alla sicurezza

La maggior parte delle aziende dedica meno di due ore per utente all'anno alla sensibilizzazione alla sicurezza dei dipendenti.



Ogni anno sempre più aziende aumentano la frequenza delle loro attività di sensibilizzazione alla sicurezza.

Concentrare le attività di formazione sugli utenti vulnerabili

È possibile che i tuoi tentativi di ampliare tuo programma di sensibilizzazione alla sicurezza incontrino una resistenza. Gli scettici possono temere che il programma si aggiunga al carico di lavoro di troppi utenti, in particolare quelli che non rappresentano un rischio elevato.

Per placare alcune di queste preoccupazioni, considera di concentrare le attività di formazione più regolarmente sugli utenti vulnerabili, piuttosto che adottare un approccio generico che richiede un maggior numero di momenti formativi a tutto il personale. Con un approccio mirato, le parti interessate sanno che le sessioni di formazione supplementari e altre attività di sensibilizzazione alla sicurezza sono giustificate. Dal canto loro gli utenti capiscono perché vengono coinvolti.

Altri possono essere più preoccupati per il tempo dedicato alla formazione che per il numero di persone coinvolte. Fortunatamente, esistono dei modi per rafforzare la sensibilizzazione degli utenti senza far perdere loro tempo.

Utilizza newsletter, tavole rotonde, pagine wiki e notifiche via email per sensibilizzare i tuoi utenti alla sicurezza senza che vi dedichino troppo tempo.

Sai chi sono i tuoi utenti più vulnerabili?

Proofpoint utilizza il termine VAP (Very Attacked People™ ovvero le persone più attaccate) per descrivere la categoria di utenti che i criminali informatici prendono di mira con un'insolita intensità: elevati volumi di attacchi, minacce estremamente mirate, tattiche avanzate o tutte e tre le cose. Mentre tutti gli utenti sono potenziali obiettivi, i VAP hanno un valore inestimabile per i loro contatti professionali unici e l'accesso privilegiato a dati, sistemi e altre risorse.

I VAP vengono attaccati
da 3 a 12 volte
in più rispetto agli altri utenti

Secondo le nostre osservazioni, i VAP non sono sempre i VIP di un'azienda, come i dirigenti di alto livello. Possono far parte dei dipartimenti delle risorse umane, delle relazioni pubbliche, del marketing o della ricerca. Chiunque disponga del giusto accesso può essere un obiettivo di alto valore.

Una volta identificati i tuoi VAP, è fondamentale colmare le lacune in materia di sicurezza con una formazione estremamente mirata. Per esempio, puoi inviare ai tuoi VAP simulazioni di attacchi di phishing delle credenziali di accesso. Se non superano il test, offri loro una formazione opzionale. In questo modo puoi ridurre i rischi legati alle persone senza far perdere tempo agli utenti non coinvolti.

La sensibilizzazione alla sicurezza è un processo a lungo termine. Devi fornire una formazione completa e continua nel tempo per mantenere gli utenti informati sul panorama delle minacce informatiche in continua evoluzione. Questo processo include i seguenti elementi:

- Valutazioni periodiche
- Formazione
- Attività di rafforzamento
- Misurazione

Per procedere come previsto e allineare le parti interessate, puoi creare un calendario che riporti le attività, i canali, i messaggi e i temi del tuo programma.

Valutare l'efficacia del programma di sensibilizzazione alla sicurezza

Molte aziende valutano l'efficacia dei loro programmi basandosi esclusivamente sulle sessioni di formazione completate (per la conformità) e sul tasso di fallimento degli utenti nelle simulazioni di attacchi. Ma per modificare realmente il comportamento degli utenti e ridurre i rischi, devi andare oltre, stabilendo profili di rischio più completi.

Di seguito i principali parametri che ti aiutano a valutare il reale impatto dei programmi di sensibilizzazione alla sicurezza:

Tasso di segnalazione nelle simulazioni

Questo parametro ti fornisce informazioni non solo sugli utenti che evitano gli attacchi ma, ancor più importante, adottano un comportamento corretto, mettendo in pratica quanto appreso nella formazione di sensibilizzazione alla sicurezza quando rilevano qualcosa di sospetto.

Percentuale di clic reale

La protezione avanzata dell'email di Proofpoint ti permette di vedere la percentuale di clic su contenuti pericolosi anche se l'URL è bloccato o è stato riscritto per motivi di sicurezza. Questo parametro permette di valutare le conoscenze effettive degli utenti. Con questi dati puoi determinare se gli utenti sono migliorati nel rilevamento di contenuti pericolosi.

Tipi di messaggi segnalati

Grazie a un componente aggiuntivo nell'email, gli utenti possono segnalare i contenuti dannosi sospetti, proprio come farebbero con una casella di segnalazione degli abusi. Proofpoint Targeted Attack Protection (TAP) ti mostra come sono stati classificati i diversi tipi di email (dannose, spam, basso rischio, ecc.). Puoi valutare i miglioramenti degli utenti nel tempo in termini di segnalazione dei messaggi che potrebbero mettere in pericolo l'azienda.

Impatti reali

Questo è il parametro più importante di tutti. Tiene traccia degli impatti della formazione sugli utenti: riduzione degli attacchi di phishing riusciti, delle violazioni delle credenziali di accesso, degli incidenti di origine interna e del malware. Si tratta del parametro massimo dell'eccellenza. Inoltre, è indispensabile per ottenere l'adesione sul lungo termine delle parti interessate ai programmi di sensibilizzazione alla sicurezza

Rispondere alla domanda: Quali dovrebbero essere le nostre percentuali di clic e di segnalazione?

Raccomandazioni di Proofpoint:

<5%
Tasso di fallimento/clic

>70%
Tasso di segnalazione

Comunicare efficacemente con il tuo CISO e le principali parti interessate

Quando riporti i risultati ai vertici aziendali e alle parti interessate, la paura, l'incertezza e il dubbio sono efficaci solo parzialmente. Senza dubbio le minacce informatiche devono essere gestite. Ma un utilizzo eccessivo di tattiche allarmistiche, esagerando i pericoli, si rischia di creare il classico scenario del ragazzo che gridava "Al lupo! Al lupo" che fa più male che bene.

Strategie principali per comunicare le prestazioni dei programmi di sensibilizzazione alla sicurezza

Quantità

Il contesto è importante. Questo è il motivo per cui è essenziale comprendere le prestazioni complessive e il posizionamento rispetto ad altre aziende. Per metterti a confronto con i tuoi concorrenti, concentrati sui parametri positivi piuttosto che su quelli negativi come la percentuale di clic nelle simulazioni.

Ecco alcuni esempi di parametri positivi:

- Aumento nei tassi di segnalazione degli utenti delle email di simulazione di attacchi di phishing
- Miglioramento dei risultati delle valutazioni della conoscenza relativamente alla sicurezza
- Aumento della precisione dei messaggi dannosi segnalati dagli utenti
- Incremento del tasso di partecipazione degli utenti alle attività di sensibilizzazione alla sicurezza

Qualità

Le storie, combinate con i dati, contribuiscono a dimostrare che la sensibilizzazione alla sicurezza è molto più di un'attività di conformità forzata, che modifica il comportamento degli utenti e cambia attivamente la cultura dell'azienda nella misura in cui gli utenti comprendono meglio i rischi e partecipano alla protezione dell'azienda.

Esempi di storie:

- Un utente ha neutralizzato un attacco di phishing sofisticato reale.
- Gli utenti hanno espresso riscontri positivi sul programma di sensibilizzazione in un sondaggio sulla soddisfazione.
- Un membro della dirigenza o un dipendente conosciuto ha condiviso informazioni con il personale in merito alla sensibilizzazione alla sicurezza.

Visibilità sulla sensibilizzazione alla sicurezza tramite una dashboard

La sensibilizzazione alla sicurezza è uno dei passi più importanti che tu possa compiere per proteggere la tua azienda. Questo è uno dei motivi per cui abbiamo creato la dashboard del CISO. Permette ai team IT e della sicurezza di accedere ai principali parametri che indicano che i programmi di sicurezza favoriscono il cambiamento dei comportamenti e promuovono una cultura della sicurezza. Questi indicatori di successo evidenziano il ritorno sugli investimenti e favoriscono investimenti futuri.

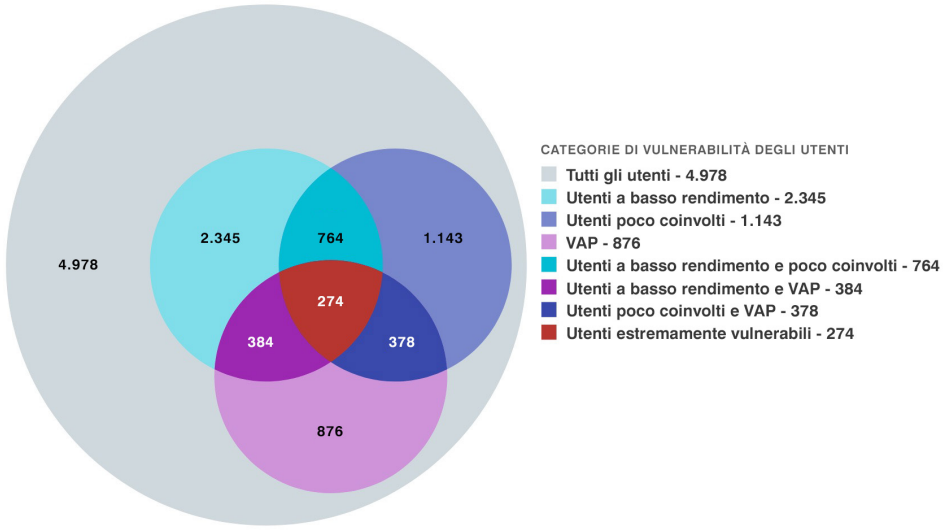
La dashboard del CISO di Proofpoint ti permette di accedere a parametri come la vulnerabilità degli utenti e il punteggio del tuo programma di sicurezza.

Vulnerabilità degli utenti

Identifica gli utenti a basso rendimento e poco coinvolti, così come quelli che fanno clic su messaggi dannosi. Se gli utenti vengono identificati come VAP da Proofpoint Targeted Attack Protection, questi dati vengono integrati per ottenere una migliore visione del profilo di rischio globale di questi utenti.

274 utenti altamente vulnerabili (su un totale di 4.978 utenti)

82 utenti altamente vulnerabili in meno negli ultimi 90 giorni

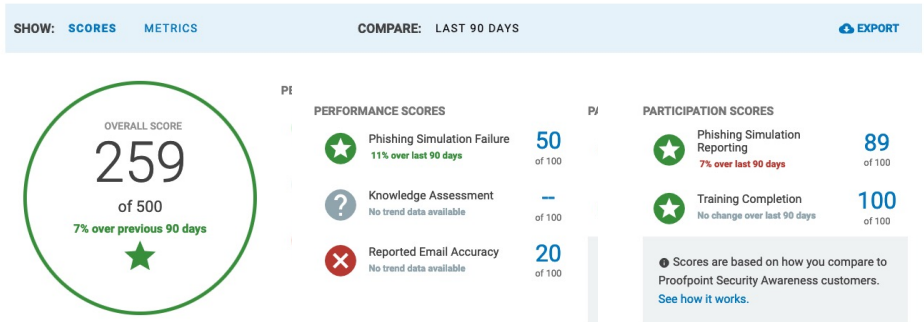


Punteggio del programma di sicurezza

I punteggi relativi alle prestazioni e alla partecipazione illustrano in quale percentile rientra la tua azienda in ogni area nonché l'evoluzione del punteggio complessivo. Le icone a semaforo ti permettono di identificare in un batter d'occhio dove il programma ha bisogno di essere migliorato.

Riassunto dei punteggi del programma di sicurezza

Traccia le prestazioni del tuo programma di sicurezza nel tempo grazie al punteggio del programma. Fai clic su ogni punteggio per vedere come è stato calcolato.



Sintesi della vulnerabilità degli utenti nella dashboard del CISO

Visibilità sulla sensibilizzazione alla sicurezza tramite una dashboard

Confronto dei percentili nel tempo

In combinazione con il punteggio del programma di sicurezza, scopri il percentile in cui ti trovi rispetto ad altre aziende del settore per effettuare un'analisi. Puoi valutare i tuoi progressi nel tempo.

Gli attacchi di oggi prendono di mira le persone, non soltanto la tecnologia. Ecco perché un approccio efficace e incentrato sulle persone per proteggere la tua azienda richiede una formazione mirata che renda la sicurezza informatica una priorità, soprattutto per gli utenti vulnerabili e i VAP.

La dashboard del CISO ti permette di accedere ai parametri necessari per ottimizzare la sensibilizzazione alla sicurezza. Comunicare con il tuo CISO, mantenere l'adesione delle parti interessate e ottimizzare il tuo programma non è mai stato così semplice.

Per saperne di più su come Proofpoint può aiutarti a modificare il comportamento dei dipendenti e rendere la sicurezza informatica un elemento essenziale della tua cultura aziendale, visita il sito 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 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.

0504-002-01-01 09/21