Servizi gestiti per Proofpoint Security Awareness Training - Commercial

Sfrutta la nostra competenza leader del settore per la configurazione e la gestione del tuo programma di sensibilizzazione alla sicurezza

Prodotti

- Formazione Proofpoint Security Awareness Training

Vantaggi principali

- Esperti dedicati ridurranno il rischio degli utenti più velocemente implementando un programma di sensibilizzazione alla sicurezza di punta basato sulle best practice
- Serie completa di risorse di formazione, tra cui strumenti di rafforzamento per migliorare il comportamento degli utenti e la cultura organizzativa
- Report dettagliati e approfonditi che forniscono una visione olistica del programma di sensibilizzazione alla sicurezza e della preparazione degli utenti della tua azienda

Concentrati sull'attività principale e lascia che ci accolliamo noi il programma di sensibilizzazione alla sicurezza. Servizi gestiti per Proofpoint Security Awareness Training - Commercial gestisce le sfide legate alla progettazione, esecuzione e segnalazione sui programmi per i clienti commerciali con un massimo di 2.500 utenti. Ti metteremo a disposizione esperti dedicati che, con un approccio misurato e personale, ti aiuteranno a impostare e ad eseguire la formazione di sensibilizzazione alla sicurezza. Insieme, svilupperemo un programma per te che sia facile ed efficace e in grado di coinvolgere i tuoi utenti finali per tutto l'anno.

Pianificazione

Il nostro team di esperti gestirà il tuo programma di sensibilizzazione alla sicurezza. Le nostre risorse dedicate si concentreranno sull'implementazione di un programma predefinito basato su collaudate best practice. Dall'avvio del programma, ti incontrerai ogni mese con i membri del tuo team a cui sei stato assegnato. Questi esperti saranno i tuoi rappresentanti personali e punti di contatto principali.

Avvio

Definiremo dei piani iniziali per coinvolgere i principali stakeholder, tra cui risorse umane, IT e sicurezza, e stabiliremo il modo migliore per presentare il programma agli utenti. Il tuo contatto ti metterà a disposizione una serie di indicazioni, strumenti e modelli da utilizzare nel corso del programma. Tali risorse saranno ad esempio:

- Guida alle best practice
- Calendario delle best practice
- Modelli campione di phishing simulato
- Modelli di notifica per gli incarichi di formazione
- Modelli di comunicazione IT ed help desk
- Documenti di safelisting

Comunicazione

La comunicazione è importante per qualsiasi impresa. Consigliamo caldamente di concepire un piano di comunicazione completo per mantenere aggiornati tutti i principali stakeholder. Tale piano deve stabilire le attese rispetto agli obiettivi del programma. Deve anche includere un punto di contatto della tua azienda che possa rispondere a qualsiasi dubbio o domanda. Possiamo consentirti di inviare notifiche ai tuoi team interni IT e di help desk quando vengono programmate le campagne. Ciò fornirà all'help desk informazioni dettagliate sulle campagne e sui gruppi coinvolti per poter rispondere alle domande e alle richieste degli utenti. Possiamo anche fornire esempi di comunicazioni per aiutarti a mantenere gli utenti informati sul tuo programma di sensibilizzazione alla sicurezza, perché una comunicazione efficace può promuovere la proprietà e l'accettazione di importanti esperienze di apprendimento.

Preparazione tecnica

Ti forniremo documenti per la creazione di una safelist di indirizzi IP per i server email e per condurre test sui filtri antispam. Potrebbe anche essere necessario creare delle eccezioni nei firewall o nei dispositivi di sicurezza per consentire il traffico verso i nostri server.

Gestione utenti

Insieme al tuo contatto, affronterete il tema del bacino di utenza del programma. Dovrete definire se lo strumento End-User Sync per attirare gli utenti direttamente nella nostra piattaforma dall'Active Directory (AD) della tua azienda o da Azure sia o meno una possibilità. Se non lo è, richiederemo un elenco di utenti corredato da dati quali email, nome, cognome, unità aziendale, gruppo, posizione e altre proprietà (fino a tre in più). Metteremo in relazione i tuoi requisiti di segnalazione con le informazioni pertinenti ottenute dalle nostre discussioni. Affronteremo anche la questione di come le informazioni degli utenti vengano aggiornate nel tempo per rispecchiare nuove assunzioni, persone non più impiegate e aggiornamenti su criteri come responsabile e reparto.

Componenti della sensibilizzazione alla sicurezza

Il tuo programma di sensibilizzazione alla sicurezza può includere quanto segue (a seconda dei prodotti con licenza):

- Attacchi simulati
- Valutazioni della conoscenza
- Formazione
- Materiale sulla sensibilizzazione
- Strumenti di rafforzamento

Implementazione

Le valutazioni di Proofpoint stabiliscono una base realistica della vulnerabilità della tua organizzazione contro diversi vettori di attacco.

Simulazioni di phishing

Un esperto di Proofpoint sarà l'amministratore pratico del nostro strumento di simulazione di phishing. Creeremo, programmeremo e implementeremo ogni campagna in base al piano nel corso della durata della licenza. Prima di iniziare, esamineremo insieme l'ambito della campagna e gli utenti da coinvolgere nel phishing. Un attacco di phishing simulato cieco, che dirige gli utenti ingannati a una pagina di errore 404, sarà inviato ai tuoi utenti all'inizio del periodo della licenza per fornire dati iniziali di base. Per tutta la durata della licenza, condurremo degli attacchi simulati di phishing incorporati con Teachable Moments per un feedback immediato. Tali Teachable Moments sono pagine di destinazione a cui viene indirizzato qualsiasi utente che viene raggirato dagli attacchi di phishing.

Valutazione della conoscenza

Le valutazioni della conoscenza forniscono una panoramica della conoscenza dei dipendenti e misurano l'efficacia della formazione. Consigliamo di condurre una valutazione con argomenti di ampia portata all'inizio del periodo di licenza. Ulteriori valutazioni delle conoscenze possono essere inviate in sostituzione di esercizi di formazione programmati.

Formazione di sensibilizzazione alla sicurezza

Proofpoint assegnerà moduli di formazione a qualsiasi utente che sia vittima degli attacchi di phishing negli esercizi programmati di formazione al phishing tramite iscrizione automatica. Suggeriremo anche moduli di formazione e creeremo incarichi per ogni utente, che sia vittima o meno di un attacco simulato. Questo approccio equilibrato non solo consente di identificare e affrontare specifiche aree critiche, ma rafforza anche complessivamente le difese facilitando l'apprendimento tra tutti gli utenti. Ricorderemo agli utenti la data di scadenza all'avvicinarsi della conclusione della formazione. Misureremo anche le competenze degli utenti per pianificare le valutazioni e le assegnazioni successive dei moduli di formazione.

Nota: se utilizzi un sistema di gestione dell'apprendimento (LMS) personale per alcuni o per tutti gli incarichi di formazione, allora sarai tu, e non il tuo contatto, a occuparti della gestione degli utenti, degli incarichi e dei rapporti LMS. Contenuti formativi e iscrizione automatica non sono disponibili per i moduli basato su LMS.

Calendario del programma

1° TRIMESTRE	2° TRIMESTRE	3° TRIMESTRE	4° TRIMESTRE
Riunione di avvio	Esercizio di phishing	Riunione - Analisi aziendale del cliente	Esercizio di phishing
Gestione della piattaforma - Utenti	Esercizio di formazione - Iscrizione automatica al phishing	Esercizio di phishing	Esercizio di formazione - Iscrizione automatica al phishing
Esercizio di phishing	Esercizio di formazione o valutazione della conoscenza	Esercizio di formazione o valutazione della conoscenza	Esercizio di formazione o valutazione della conoscenza
Gestione della piattaforma - Notifiche			Riunione - Revisione di fine anno

Rafforzamento

I materiali di sensibilizzazione alla sicurezza sono disponibili in un'ampia gamma di formati, tra cui infografiche, articoli e video. Puoi scaricarli e personalizzarli a piacere. Sono progettati per rafforzare i principi chiave insegnati nei nostri moduli di formazione. Sottolineano anche le best practice e migliorano la conservazione delle conoscenze. Proofpoint può consigliare materiali di sensibilizzazione alla sicurezza basati sulle aree critiche identificate nella valutazione delle conoscenze.

Il componente aggiuntivo email PhishAlarm fornisce un rafforzamento positivo ai tuoi utenti che segnalano potenziali truffe. Esso segnalerà ai team di sicurezza e di risposta agli incidenti le email di phishing sospette con un clic. Questo riduce la durata e l'impatto degli attacchi di phishing attivo, mentre rafforza i comportamenti appresi nel tuo programma di formazione di sensibilizzazione alla sicurezza. La segnalazione di attacchi di phishing (tasso di segnalazione) è un'importante parametro di tendenza per rilevare il comportamento degli utenti finali, nonché la sensibilizzazione alla sicurezza e il coinvolgimento.

Analisi

I risultati della valutazione delle conoscenze, delle campagne di phishing simulate, della formazione e della segnalazione email PhishAlarm forniscono una visione olistica dei livelli di conoscenza degli utenti e della suscettibilità agli attacchi. Con questi dati, puoi identificare le maggiori aree di rischio e creare un piano per potenziare la conoscenza dei dipendenti. Il tuo contatto esaminerà i risultati dopo ogni valutazione e incarico di formazione. I risultati verranno confrontati con i dati storici delle prestazioni per ricavare le tendenze di miglioramento e le aree critiche. Le proprietà incluse nei report (che sono state definite nella sessione di pianificazione iniziale) saranno esaminate ai fini della correlazione del rischio al reparto, alla geografia, al ruolo o al manager. Il tuo contatto fornirà un'analisi di benchmarking del settore e dei modelli, se disponibile.

Report

I report verranno realizzati per ogni attività man mano che il programma procede. Tali report sono a disposizione del responsabile di progetto in qualsiasi momento. Alcuni report possono essere programmati per essere eseguiti periodicamente. Possono anche venirti inviati in modo sicuro tramite email.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **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**.