Sababa Awareness

Trasforma "l'anello debole" nella difesa più forte

L'Errore umano è la prima fra le cause di incidenti di cyber security. Il personale e i colleghi che non si occupano di sicurezza IT, spesso non sono in grado di riconoscere gli attacchi di phishing, ignorano l'importanza di usare password complesse e non hanno una consapevolezza adeguata dei rischi informatici, tutto ciò rappresenta un potenziale rischio per l'azienda.

Sababa Awareness è una piattaforma di training per insegnare a tutti i colleghi le basi della security awareness e far loro acquisire o migliorare capacità pratiche così da riconoscere e fronteggiare i cyber-attacchi. A differenza delle altre piattaforme di formazione, Sababa Awareness è una piattaforma di apprendimento adattivo, costruita su una tassonomia proprietaria di attacchi di social engineering che adatta il programma del corso a ciascun dipendente, in base al suo livello individuale, al ritmo dei progressi e alle aree di miglioramento. L'aggiornamento continuo delle competenze nel corso dell'anno rende i dipendenti maggiormente consapevoli e riduce al minimo i rischi per la sicurezza informatica, causati da errori umani, nell'intera organizzazione.

Approccio scientifico alla formazione

La piattaforma Sababa Awareness è stata disegnata insieme ad un team di psicologi che hanno sviluppato una matrice di tassonomia di 432 possibili tipi di attacco, simulati con la piattaforma.
Tali attacchi sono classificati in base a:

- 6 vettori di attacchi digitali: e-mail, siti Web, social network, messenger, dispositivi mobili, nonché strutture per ufficio e lavoro

- 6 vettori di attacco psicologico: paura, irritazione, mancanza di attenzione, curiosità, avidità e desiderio di aiutare
- 2 catalizzatori di attacchi psicologici: autorità o urgenza
- 3 fonti di attacco: esterne, aziendali o personali
- 2 personificazioni di attacco - anonime o mirate

Simulazione degli attacchi informatici più diffusi
Sababa Awareness sviluppa continuamente una serie di scenari di attacco mirati basati sull'attuale panorama delle minacce, sulle tendenze e, soprattutto, sul profilo di rischio individuale dell'azienda. Gli esempi di veri e propri attacchi informatici rivolti alla società vengono utilizzati per simulazioni di attacchi di ingegneria sociale, come phishing, compromissione della posta elettronica aziendale, frodi fake-CEO, USB drop e molti altri.

Miglioramento continuo dei dipendenti - con meno teoria e più pratica
Il programma di formazione Sababa si basa sul metodo PDCA e combina la tradizionale consapevolezza della sicurezza attraverso valutazioni iniziali dei collaboratori, e-learning e test, con una gestione continua delle competenze del personale tramite attacchi simulati. Allo stesso tempo, si concentra fortemente sullo sviluppo di abilità pratiche, evitando troppe teorie e riducendo al minimo il tempo dei dipendenti lontano dal lavoro.

Implementazione e integrazione flessibili
Sababa Awareness può essere installata on- premise o fruita attraverso il Cloud, in base alle esigenze, alle restrizioni e alla legislazione del cliente. L'API REST di Sababa Awareness offre funzionalità di integrazione per vari sistemi, tra cui LMS (eLearning), LDAP, SGRC, SIEM, IDM e molti altri per compilare processi di gestione della consapevolezza e del comportamento in un unico contesto di gestione della sicurezza.

Come funziona

Gestione della piattaforma
Non appena un responsabile della sicurezza accede alla console di Sababa Awareness, può scegliere tra modelli realistici per e-mail di phishing, allegati e siti di phishing imitati, pianificare e avviare attacchi simulati verso gli utenti aziendali. Ogni azione durante l'attacco viene registrata per definire e aggiornare il livello di sicurezza degli utenti in vari dipartimenti e dell'intera organizzazione. Tramite la dashboard di Sababa Awareness è semplice tenere traccia del rating di sicurezza aziendale e generare i report per il management.

Modelli sempre aggiornati
Ogni trimestre Sababa Awareness sviluppa fino a 10 nuovi scenari di attacchi mirati simulati, tipici del settore, dei clienti, dei dipartimenti aziendali e persino dei singoli utenti. Gli scenari coprono tutti i vettori di attacco organizzativo, tecnologico e psicologico e vengono forniti nel formato di e-mail, allegati, siti di phishing e pagine web pronti da utilizzare durante gli attacchi simulati.

Miglioramento costante della sicurezza
Tutti gli utenti hanno accesso alla piattaforma di formazione integrata e ai corsi di formazione on-line durante l'intero periodo di validità della licenza. La formazione copre tutte le principali aree della security awareness, compresa la sicurezza IT per gli utenti, il lavoro sicuro su Internet, tramite e-mail o dispositivi mobili e la sicurezza fisica per comunicare correttamente con il personale predisposto alla sicurezza.

Aggiornamenti regolari inclusi nel costo della licenza
Tutti i corsi esistenti vengono regolarmente aggiornati e arricchiti con nuovi materiali durante tutto l'anno. La formazione può essere personalizzata secondo le linee guida del cliente. Nuovi materiali e moduli lanciati durante il periodo di validità della licenza sono forniti gratuitamente. Sababa Awareness pubblica regolarmente digest informativi dedicati per sensibilizzare gli utenti sui rischi informatici e incrementare la security awareness.

Rilevamento vulnerabilità in programmi e plugins
Oltre al controllo delle competenze, Sababa Awareness esegue la scansione dei browser, dei plug-in, dei client di posta elettronica e delle applicazioni presenti sui dispositivi alla ricerca di vulnerabilità. Se viene rilevata una vulnerabilità, viene elencata tra i software che presentano dei rischi, modificando lo stato dell'utente. Gli aggiornamenti delle regole aiutano a rilevare nuove applicazioni e vulnerabilità in tutte le applicazioni utente

Integrazione con altri sistemi
Sababa Awareness fornisce un'interfaccia di programma (API REST) per l'integrazione, la gestione e la ricezione dei dati da qualsiasi sistema esterno. Sababa Awareness può essere integrato con i sistemi di classe IR / SGRC, inclusi R-Vision e altri

Supporto tecnico

Il supporto tecnico 8X5 è incluso in ogni licenza e include un pacchetto di installazione locale pronto, modelli individuali aggiuntivi per campagne di attacco simulate e consulenza su come installare, configurare e utilizzare il servizio durante l'intera validità della licenza

Licensing

Licensing per-user. Il costo comprende i contenuti e i moduli di formazione, campagne di attacco simulato all'anno e ser