Attacchi Cyber: La consapevolezza non è più un optional

Cyber Guru

Introduzione

Il fattore umano è oggi l'elemento più cruciale per la sicurezza informatica, utilizzato dal cyber crime per insinuarsi all'interno delle organizzazioni con strategie offensive che si fanno sempre più sofisticate. Sono infatti proprio gli utenti con i loro comportamenti non adeguati alla complessità della sfida, ad aprire inconsapevolmente la porta agli attaccanti.

Analizzando i vari rapporti che riguardano lo stato della Cybersecurity il quadro che emerge è che la crescita degli attacchi Cyber sembra inarrestabile, e che tra le varie tecniche di attacco utilizzate quelle caratterizzate da una maggiore crescita fanno leva principalmente sul fattore umano.

La cronaca è ricca di attacchi Cyber andati a buon fine. Attacchi che hanno colpito organizzazioni di tutti i settori e di tutte le dimensioni. Brand prestigiosi e altri meno conosciuti hanno visto le proprie attività produttive bloccate e la propria reputazione compromessa. Si tratta di una vera e propria guerra cyber che vede gli attaccanti in una posizione di indubbio vantaggio, soprattutto perché la prima linea di difesa è costituita da utenti inconsapevoli che, nella maggior parte dei casi, non hanno neanche la percezione di essere attaccati.

Avviare quindi dei programmi di Cyber Security Awareness efficaci e innovativi, in grado di incidere sui comportamenti umani e trasformare gli utenti nella prima linea di difesa delle organizzazioni, non è più un optional.

Obiettivo della piattaforma di Cyber Security Awareness di Cyber Guru è proprio quello di aumentare la resistenza agli attacchi Cyber, attraverso percorsi di formazione permanente capaci di sviluppare nelle persone la capacità di operare con comportamenti sicuri guidati da una maggiore consapevolezza. Una piattaforma, costantemente implementata, che utilizza le tecnologie, i processi di produzione e le metodologie pedagogiche più avanzate per garantire il massimo coinvolgimento degli utenti e la protezione dai rischi cyber.

Michel Ruefenacht
VP Marketing

Lo scenario

I trend relativi agli attacchi cyber degli ultimi anni mostrano purtroppo una curva in continua crescita. Tra le principali cause c'è senza dubbio il maggiore utilizzo delle tecnologie digitali, considerate il motore trainante per una reale crescita economica, a cui però non è corrisposto un adeguato livello di alfabetizzazione digitale degli utenti. Ad accelerare il trend gli effetti della pandemia, con il massiccio ricorso allo smart working e a un maggior utilizzo di applicazioni e servizi digitali.

Purtroppo, nonostante i considerevoli sforzi fatti dalle organizzazioni in Cyber Security, quello che emerge è che l'anello debole della catena difensiva di qualsiasi organizzazione è ancora oggi rappresentato dal fattore umano, ed in particolare dagli utenti digitali. È infatti ormai accertato che oltre il 90% degli attacchi cyber può essere ricondotto a un errore umano, a un comportamento inadeguato.

Il 90% degli attacchi cyber inizia con un clic su una mail malevola

Barclays Bank

Il 95% degli attacchi Cyber è riconducibile ad un errore umano

IBM Cyber Security Intelligence Index Report

Una catena è forte quanto il suo anello più debole

La resistenza complessiva agli attacchi cyber di un'organizzazione dipende quindi dalla resistenza del Fattore Umano, oggi vero anello debole della catena.

Lo sviluppo della società digitale, con i suoi rischi, costringe tutte le organizzazioni ad investire in modo consistente sul fattore umano, sul livello di consapevolezza delle persone.

Un investimento divenuto necessario per colmare quel gap culturale che gli effetti pandemici e la rapida trasformazione digitale hanno acuito.

Nel 2021 le violazioni dei dati sono costate alle organizzazioni 45 miliardi di dollari

Panda Security

Il numero di attacchi ransomware è aumentato del 13% tra il 2020 e il 2021

Verizon Data Breach Investigations Report

I costi globali della criminalità informatica raggiungeranno 10,5 trilioni di dollari entro il 2025

Cybersecurity Ventures

La metodologia

Avviare quindi dei programmi di Cyber Security Awareness efficaci e innovativi, in grado di incidere sui comportamenti umani per trasformare gli utenti nella prima linea di difesa delle organizzazioni, non è più un optional.

La piattaforma Cyber Guru è stata progettata per massimizzare i processi di apprendimento sviluppando 3 caratteristiche difensive dell'individuo: **la conoscenza, la percezione del pericolo, la prontezza**.

Per fare ciò sono necessari programmi formativi avanzati, basati su metodologie innovative di formazione permanente, allenamento e coinvolgimento, in grado di minimizzare l'impatto sulle funzioni di gestione della formazione del personale e della Cyber Security. Solo così sarà possibile seguire l'evoluzione costante delle strategie di attacco sempre più sofisticate.

3 PERCORSI FORMATIVI

Cognitivo

La conoscenza viene gestita attraverso un processo di formazione cognitiva basato su un approccio principalmente didattico

Induttivo

La percezione del pericolo viene stimolata attraverso una formazione induttiva che tende ad agire sulla componente più emotiva del nostro cervello

Esperienziale

Allenare la prontezza è fondamentale per agire velocemente adottando il giusto comportamento di fronte al manifestarsi di un pericolo

Una piattaforma completa di Cyber Security Awareness

La piattaforma è pensata per trasformare i comportamenti della forza lavoro di qualunque organizzazione pubblica o privata, qualsiasi dimensione o categoria merceologica, grazie a:

3 PERCORSI FORMATIVI FORTEMENTE SINERGICI TRA LORO

Cyber Guru Awareness

Un programma didattico cognitivo erogato su base elearning che garantisce lo sviluppo graduale della consapevolezza attraverso la conoscenza relativa alle minacce della rete e allo schema comportamentale da adottare per prevenire gli attacchi.

Cyber Guru Channel

Un programma di formazione induttiva che genera apprendimento grazie alla forza della narrazione e della produzione video. Seguendo uno schema narrativo tipico delle serie TV, il discente apprende identificandosi nelle situazioni narrate nei diversi episodi.

Cyber Guru Phishing

Un programma di addestramento esperienziale che allena gli individui a resistere agli attacchi phishing nelle loro varie tipologie. Il programma, automatico e adattivo, consente ad ognuno un allenamento personalizzato sulla base delle esperienze individuali e del singolo livello di resistenza agli attacchi.

Cyber Guru Awareness

Cyber Guru Awareness è progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per il suo approccio "a rilascio costante e graduale" (Smart-School). Il percorso è costituito da moduli formativi auto-consistenti, ognuno dedicato ad uno specifico argomento, con attivazione mensile, a copertura di un periodo di 12/24/36 mesi. Ogni modulo è a sua volta costituito da 3 brevi lezioni video di 5 minuti ciascuna. Le principali caratteristiche sono l'appredimento cognitivo efficace, il massimo coinvolgimento del discente e la supervisione ad impatto zero.

- **Moduli formativi auto-consistenti ad attivazione mensile**
- **Impegno settimanale minimo, compatibile con qualsiasi funzione**
- **Micro-lezioni video in formato multimediale**
- **Utilizzo di attori professionisti con funzioni di coach**
- **Linguaggio altamente divulgativo**
- **Approccio interattivo con continua alternanza tra micro lezioni e test**
- **Test di valutazione a risposta multipla**
- **Metodologia di gamification, con organizzazione in team**
- **Piattaforma multilingua**
- **Contenuti aggiuntivi e costantemente attualizzati**

Cyber Guru Channel

La metodologia induttiva utilizzata si basa sull'immersione dell'utente all'interno di una situazione reale e su un processo di auto-identificazione con la minaccia Cyber, che assume così una forma concreta. L'utente assume consapevolezza non attraverso una nozione, ma attraverso una narrazione, la quale agisce, prima, sulla percezione del pericolo, e successivamente sull'elemento nozionistico, superando un retropensiero molto pericoloso: "a me non può capitare". Le tre principali caratteristiche sono l'apprendimento induttivo efficace, il massimo coinvolgimento del discente e la supervisione ad impatto zero.

- **Formazione continua**
- **Produzioni video avanzate**
- **Più formati video con storytelling diversi**
- **Episodi brevi**
- **Ritmo narrativo elevato**
- **Auto-identificazione in situazioni realistiche**
- **Approccio Netflix-Like**
- **Documentazione di approfondimento per ogni episodio**
- **Reportistica esaustiva sul livello di fruizione**
- **Funzioni di student caring automatico, per motivare la partecipazione**

Cyber Guru Phishing

Cyber Guru Phishing è stato progettato per addestrare la forza lavoro a resistere agli attacchi phishing, attraverso campagne di attacchi simulati, che vengono personalizzati sulla base del profilo comportamentale del singolo utente, grazie ad un processo automatico e adattativo, guidato dall'uso di tecnologie di intelligenza artificiale. Il discente aumenta la resistenza agli attacchi attraverso l'esperienza, sia quella negativa dell'errore che quella positiva del riconoscimento dell'attacco. Le tre principali caratteristiche sono l'addestramento esperienziale efficace, l'allenamento personalizzato e la supervisione ad impatto zero.

- **Addestramento esperienziale efficace e continuativo**
- **Allenamento personalizzato tramite processo adattivo**
- **Livelli di difficoltà e simulazioni personalizzate**
- **Campagne di attacco automatizzate**
- **Errore > Formazione istantanea**
- **Procedura di segnalazione**
- **Template pre-caricati**
- **Reportistica analitica e manageriale attraverso una dashboard avanzata**
- **Gruppi di rischio**
- **Politiche di remediation**

Cyber Guru
Security Awareness Training That Works!

Seguici su LinkedIn | Youtube

Scopri di più su Cyber Guru
cyberguru.it

Diventa nostro partner
cyberguru.it/partner/

Sei interessato ad una live demo delle nostre soluzioni?

Prenota un appuntamento di 30 minuti con un Awareness Training Specialist

PRENOTA ADESSO