

SECURITY MIND ► L'AZIENDA TORINESE SI OCCUPA DI CYBER SECURITY AWARENESS IN MODO MULTIDISCIPLINARE UNENDO CYBERSECURITY, PSICOLOGIA COMPORTAMENTALE E COMUNICAZIONE

La consapevolezza digitale si crea con metodo

Immaginare un mondo privo di rischi informatici sembra impossibile oggi. Eppure, ci sono aziende impegnate in prima linea nell'incrementare la consapevolezza di persone e imprese. È il caso di Security Mind, società di Torino specializzata nella Cyber Security Awareness che adotta un approccio innovativo e completo per proteggere le organizzazioni dalle minacce digitali. Per farlo, mette in campo una metodologia caratterizzata dall'adozione di un approccio multidisciplinare che integra cybersecurity, psicologia comportamentale e comunicazione. A guidarla i due co-fondatori Veronica Patron e Lorenzo Patron, affiancati da Federico Incoronato, Board of Advisors.

I PUNTI FORTI

L'approccio di Security Mind consente, oltre a descrivere le tecniche di attacco più utilizzate dai cybercriminali, anche di analizzare le leve emotive che sfruttano, i bias cognitivi e i processi decisionali che possono indurre in errore esponendo di conseguenza a potenziali rischi. La sicurezza informatica, per l'azienda, dipende anche dalla consapevolezza degli utenti, alla luce del fatto che oltre il 90% degli attacchi ha successo per un errore umano. Un punto critico da tenere in considerazione è proprio il ruolo del fattore umano, e il team di Security Mind aiuta le aziende a gestirlo nel modo giusto. Lo fa nell'implementazione di strategie su misura, integrando formazione continua, simulazioni di attacchi, analisi dei comportamenti e mettendo alla prova la gestione dei rischi, con l'obiettivo di trasformare i comportamenti e creare una cultura aziendale resiliente, capace di affrontare con sicurezza le sfide digitali odierne. I motivi per scegliere Security Mind sono: dalla pluriennale esperienza nell'awareness training con competenze in cybersecurity (oltre a com-

Per la società un aspetto da tenere sempre in mente è il ruolo del fattore umano nella gestione dei rischi



VERONICA PATRON, CO-FOUNDER



FEDERICO INCORONATO, BOARD OF ADVISORS



LORENO PATRON, CO-FOUNDER



petenze in psicologia, tecniche di formazione e comunicazione efficace) fino all'e-learning coinvolgente attraverso video formativi efficaci e stimolanti (ma anche in aula), passando per contenuti chiari e comprensibili anche a persone inesperte. E ancora l'analisi di stati emotivi e fattori cognitivi che i cybercriminali potrebbero sfruttare, l'accessibilità dei contenuti (in qualsiasi momento e su qualsiasi dispositivo), monitoraggio e reportistica grazie a strumenti avanzati per tracciare i progressi dei partecipanti ai corsi. Il tutto adattando la formazione alle esigenze specifiche di ogni azienda e proponendo contenuti in costante evoluzione per restare sempre al passo con le nuove minacce.

CACCIATORI DI IDEE

In Security Mind le persone sono veri e propri cacciatori di idee innovative, fiduciosi nelle possibilità date dalle nuove tecnologie quali motori dello sviluppo aziendale, della qualità della vita e del valore aggiunto che può dare ogni essere umano. Il tutto senza dimenticare che nessuno meglio delle persone che vivono quotidianamente le imprese può conoscere meglio le esigenze specifiche della propria realtà. Ecco perché il modello operativo di Security Mind è per loro: cooperare condividendo competenze e conoscenze.

Per informazioni:
www.securitymind.cloud

SERVIZI ► L'OBIETTIVO È CAMBIARE IN MEGLIO L'APPROCCIO ALLA SICUREZZA INFORMATICA

La piattaforma al centro di un percorso di consapevolezza completo

Come si affrontano le sfide digitali? Il modo migliore è affidarsi ad esperti in grado di fornire una preparazione completa e un supporto a 360 gradi. Security Mind, società di Torino specializzata nella Cyber Security Awareness, lo fa fornendo numerosi servizi alle imprese. In primis grazie a Security Mind Awareness, più di una piattaforma di formazione è un vero e proprio percorso per cambiare il modo in cui aziende e individui affrontano la sicurezza informatica. È stata pensata, infatti, per coinvolgere tutta l'organizzazione in un percorso di apprendimento stimolante e dinamico, con l'obiettivo di trasformare i comportamenti delle persone ed evitare che diventino dei complici inconsapevoli di un atto malevolo. Il programma è completo, accessibile e costruito con un linguaggio divulgativo chiaro e coinvolgente. Nello specifico, si tratta di un percorso formativo strutturato in moduli auto-consistenti, pensati per coprire ogni aspetto della sicurezza informatica, dal phishing alle minacce emergenti. Grazie



Tra le soluzioni offerte trovano spazio programmi fatti non solo di nozioni ma anche di esperienze

ad un percorso sequenziale, ogni modulo deve essere completato prima di passare al successivo, garantendo un apprendimento graduale e strutturato. Questo metodo flessibile consente di assimilare le nozioni in modo naturale, trasformando la sicurezza informa-



tica in un'abitudine quotidiana. Infine, i contenuti della piattaforma sono progettati per essere brevi e coinvolgenti, permettendo agli utenti di apprendere in pochi minuti a settimana, in qualsiasi momento della giornata.

SEMPRE ALL'AVANGUARDIA

Tra le soluzioni offerte dall'azienda, c'è anche la Security Mind Phishing Campaign, un programma di allenamento che riproduce le stesse tecniche utilizzate dai cyber criminali, permettendo agli utenti di riconoscere, contrastare gli attacchi informatici in modo efficace e di passare dalla conoscenza alla pratica. Il metodo impiegato è quello del "Learning by Doing", che combina teoria e pratica per far acquisi-

re competenze da testare immediatamente attraverso simulazioni di attacchi phishing mirati. Un'altra opzione è rappresentata dal percorso CyberAgility, un servizio di consulenza e coaching basato sulle competenze di personale specializzato. Il suo obiettivo è aumentare la resilienza del personale aziendale e la conoscenza dei possibili rischi. Infine, l'azienda offre una Cyber Experience che va oltre le semplici questioni tecniche, poiché la sicurezza informatica è una sfida che coinvolge persone, processi e consapevolezza. Per questo, la formazione va oltre il semplice trasferimento di nozioni: è un'esperienza che cambia il modo di percepire il rischio e rafforza la resilienza delle persone.