PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5327 di Venerdì 10 febbraio 2023

Come sensibilizzare dipendenti e collaboratori sulla sicurezza informatica

I programmi di sensibilizzazione e formazione su temi di sicurezza informatica vengono spesso assai poco apprezzati da dipendenti e collaboratori: come è possibile rendere più coinvolgente un programma di formazione su questi aspetti critici?

Una recente indagine, condotta negli Stati Uniti e nel Regno Unito, ha rilevato che, anche se l'85% dei dipendenti partecipa a corsi di sensibilizzazione ed addestramento sulla sicurezza informatica, il 64% pone a questi temi un'attenzione distratta e il 36% ritiene addirittura noiosa tale formazione.

Si tratta evidentemente di una situazione assai preoccupante, perché è opinione comune di tutti gli esperti di sicurezza informatica che un elevato livello di protezione si raggiunga solo quando tutti i dipendenti e collaboratori prestano adeguata attenzione a questi temi.

Ci si domanda quindi come sia possibile creare una cultura di sicurezza informatica per l'organizzazione, superando l'atteggiamento distaccato, per non dire annoiato, che i dipendenti tendono ad assumere.

Questa preoccupante situazione è confermata dal fatto che, ad esempio, il 30% degli intervistati ritiene di non avere un ruolo diretto nella sicurezza informatica aziendale, mentre il 45% non sa esattamente a chi riferire un possibile incidente informatico.

Alla luce della gravità delle sanzioni, applicabili nel caso la violazione si riferisca a dati personali, appare evidente che la situazione è oltremodo preoccupante.

L'esperienza che ha mostrato che, nella maggior parte dei casi, la formazione su questi temi viene offerta mediante presentazioni PowerPoint, che spesso utilizzano linguaggi pressoché incomprensibili per la media dei partecipanti.

Anche in questo caso, lo studio critico delle presentazioni, spesso utilizzate in questi corsi, mette in evidenza come il contenuto delle presentazioni sia spesso mirato maggiormente a gratificare il docente, piuttosto che a trasferire informazioni fondamentali ai partecipanti.

Una tecnica che si è dimostrata assai coinvolgente e fruttifera viene chiamata, con termine anglosassone, "gamification". In pratica, si tratta di introdurre, nel programma di formazione, delle tecniche giocose, che accrescono l'interesse dei partecipanti e facilitano l'assorbimento delle nozioni di base.

Le tecniche di gamification fanno leva sulla naturale propensione dei partecipanti alla socialità, alla acquisizione di nuove conoscenze, allo stimolo a competere nei confronti degli altri partecipanti, il tutto operando in una situazione, che viene presentata come un gioco.

La frequente introduzione di scenari, ai quali si può dare diversa risposta, accresce il livello di partecipazione dei presenti.

Anche solo la suddivisione dei partecipanti in gruppi, messi in competizione fra di loro, garantisce un elevato livello di coinvolgimento.

Nell'esperienza di chi scrive, la suddivisione in gruppi dei partecipanti a corsi di formazione, assegnando dei test a soluzioni variabili, conferma la vivacità della partecipazione, lo scambio di conoscenze tra i partecipanti e l'elevato livello di memorizzazione dei risultati dell'esperienza competitiva.

Un classico test di scenari competitivi prevede, ad esempio, il verificarsi di un evento di violazione della sicurezza informatica, a fronte del quale i vari gruppi possono offrire modelli di comportamento diversi e fra loro confrontabili.

Infine, un aspetto fondamentale di un percorso di formazione riguarda la somministrazione di un test a risposte multiple, alla fine del corso.

Tutti i partecipanti devono essere informati tempestivamente del fatto che dovranno compilare questo test e l'esperienza mostra come il livello di attenzione possa crescere rapidamente.

Un ultimo consiglio che viene offerto da chi scrive riguarda il fatto che, volta compilato il test finale, è bene correggerlo tutti insieme. L'obiettivo del corso non è infatti quello di promuovere o bocciare i partecipanti, ma di accertarsi che tutti i partecipanti abbiano correttamente assimilato i temi illustrati.

Non per nulla, l'Università di Roma, pone come condizione per il rilascio di un attestato di partecipazione ad un corso, sostenuto dall'Università stessa, la somministrazione di un test finale di almeno 20 domande.

In poche parole:

- la formazione in sicurezza informatica è fondamentale per tutta l'azienda;
- questa formazione può essere somministrata in vari modi, alcuni dei quali più gradevoli ed altri più distaccati;
- infine, è indispensabile effettuare un test finale di validazione della formazione.

Buon lavoro a tutti i docenti di sicurezza informatica!

Adalberto Biasiotti

www.puntosicuro.it