

Dalla Direttiva al Comportamento: NIS 2 e Psicologia nell'Era Digitale



Nel campo della sicurezza informatica, l'adozione della Direttiva NIS 2 (Network and Information Systems Security Directive 2) rappresenta un passo avanti nell'approccio dell'Unione Europea alla resilienza delle infrastrutture critiche.

Per realizzare i suoi obiettivi la NIS2 ha previsto una serie di azioni tra cui la formazione e sensibilizzazione dei dipendenti sui protocolli ottimali di sicurezza informatica.

La sicurezza informatica oltre ad essere una questione di tecnologia, è anche influenzata dal comportamento umano.

Psicologia Comportamentale e Sicurezza Informatica con la NIS 2

Il comportamento umano è spesso il fattore più imprevedibile nei sistemi di sicurezza informatica. Gli errori umani possono variare dall'utilizzo di password deboli e facilmente indovinabili, al cliccare su link dannosi, ritardo negli aggiornamenti dei software di sicurezza.

Questi comportamenti possono essere influenzati da una vasta gamma di fattori psicologici:

ECCESSO DI FIDUCIA

Alcune persone sopravvalutano la loro capacità di riconoscere ed evitare le minacce online, portandole così a prendere decisioni meno prudenti.

STANCHEZZA E STRSS

La fatica può ridurre l'efficacia del giudizio di una persona e la capacità di seguire le migliori pratiche di sicurezza, rendendo gli errori più probabili.

ABITUDINI

Le persone tendono a preferire soluzioni che minimizzino lo sforzo, anche se in alcuni casi può compromettere la sicurezza.

L'importanza di una formazione innovativa nella prevenzione degli attacchi informatici

Gli attacchi sfruttano le debolezze umane per indurre le vittime a rivelare informazioni confidenziali o a eseguire azioni che compromettano la sicurezza.

E' quindi essenziale una formazione oltre che tecnica anche psicologica, formare i dipendenti a gestire le emozioni che gli attacchi di ingegneria sociale cercano di sfruttare, come l'urgenza o la paura, con l'obiettivo di ridurre la probabilità di successo di tali attacchi.

Incorporando la comprensione psicologica nella formazione sulla sicurezza informatica, le organizzazioni possono sviluppare difese più robuste contro le tattiche di manipolazione, proteggendo meglio le loro infrastrutture e i dati sensibili.



La nostra Missione è passare
dall' **Informazione** alla **Trasformazione**

www.securitymind.cloud

