I RIBELLI DELLA CYBER SECURITY

Garantire la resilienza nell'era digitale

Le aziende sono sempre più connesse, esponendosi a un numero crescente di minacce informatiche.

La mitigazione dei rischi richiede l'impegno di ciascuno. Tuttavia, le PMI si rivelano vulnerabili ai cyber attacchi per colpa di dipendenti che non sono in grado di riconoscere le attività ad alto rischio, non comprendono le proprie responsabilità e bypassano i responsabili IT senza considerare le conseguenze.

MANCANZA DI COMPRENSIONE

70% Il 70% dei dipendenti non pensa che utilizzare un **dispositivo non autorizzato** (es. USB) possa rappresentare una minaccia

60% Il 60% non crede che installare un'applicazione **senza i diritti di amministratore** possa costituire un rischio

64% Il 64% non ritiene che **scaricare** musica o film illegalmente comporti dei rischi

COMODITÀ V ACCOUNTABILITY

Le principali ragioni per condurre attività non sicure sono

33% **il risparmio di tempo**

32% **la comodità**

Solo il **44%** si sentirebbe **responsabile** di una violazione di sicurezza causata dal proprio comportamento

Solo il **48%** dei dipendenti **pensa** alle conseguenze per la cyber security delle proprie azioni

I RIBELLI DELLA SICUREZZA INFORMATICA

57% Il 57% dei dipendenti cercherebbe di ottenere i tool (app/dati/accessi) di cui ha bisogno per essere più produttivo **senza il permesso dell'IT**

Questo dato sale al **63%** tra le **figure più senior**

Solo il **32%** installa solamente applicazioni in linea con la policy di sicurezza aziendale

Solo il **42%** aggiorna i software sui propri dispositivi aziendali

Solo il **30%** usa password complesse

UNA FALSA SENSAZIONE DI SICUREZZA

85% L'85% crede che le misure di cyber resilienza della propria azienda siano efficaci

78% Il 78% pensa che la propria azienda si sia adattata abbastanza velocemente per affrontare le minacce informatiche in evoluzione

MA

Solo il **19%** ha ricevuto training di sicurezza informatica dedicati

Solo il **25%** ha notato policy più severe di sicurezza o utilizzo (relativamente all'accesso ai servizi)

Solo il **18%** dei dipendenti ha ricevuto linee guida sulle best practice

È NECESSARIO PASSARE ALL'AZIONE

Cosa possono fare le aziende per migliorare la propria resilienza ai cyber attacchi?

Le basi: un utilizzo adeguato delle password, il backup dei dati e una buona gestione delle licenze software

Formazione costante: il 95% delle violazioni della sicurezza informatica sono dovute all'errore umano. Le aziende devono investire nella formazione dei dipendenti sui comportamenti sicuri

Non aspettare, essere proattivi: può essere difficile investire in qualcosa che non genera direttamente ricavi ma essere preparati ai cyber attacchi permetterà di ridurne le conseguenze

Responsabilità: Ognuno deve essere consapevole delle proprie responsabilità ma avere qualcuno in grado di comprendere i requisiti normativi e legali consentirà di mitigare le conseguenze di una violazione dei dati su larga scala

L'indagine, condotta da Opinium Res