Bitdefender

10 in 10

2020

I responsabili della sicurezza devono sempre essere un passo avanti ai malintenzionati. Ciò ha portato a una cultura dell'avversione al rischio ed elenchi di controlli di sicurezza compulsivi. Allo stesso tempo, le aziende e le tecnologie coinvolte sono in costante mutamento, più che mai nel 2020. È tra cambiamenti rapidi e procedure rigorose che si trova la sfida della sicurezza.

Lo studio 10 in 10 di Bitdefender mette in luce il divario tra il modo in cui i responsabili della sicurezza vedono l'attuale panorama della sicurezza e i cambiamenti che sanno di dover apportare.

C'è la necessità di cambiare il settore dall'interno

75%

75% ritengono che sia necessaria una **serie di competenze più diversificate** tra coloro che affrontano incarichi di sicurezza informatica

17%

Il 17% dei professionisti della sicurezza informatica italiani ritiene che **una maggiore neurodiversità** nel settore aiuterebbe a combattere la guerra informatica

43%

Il 43% ritiene che la neurodiversità renderebbe più forti le **difese della sicurezza informatica**

30%

Il 30% ha svelato che una forza lavoro più neurodiversa **livellerà lo scenario** contro i malintenzionati

20%

20% ritengono che se la mancanza di abilità continuerà per altri cinque anni, ciò **comprometterà definitivamente la propria attività**

In definitiva, la ricerca ha svelato che c'è una forte convinzione sulla necessità di diversità nel settore.

La comunicazione è essenziale

In relazione a ciò che i professionisti della sicurezza informatica ritengono debba cambiare maggiormente in termini di modalità di comunicazione del settore della sicurezza in futuro, gli intervistati hanno svelato che:

54%

54% dei professionisti della sicurezza informatica italiani concordano sul fatto che per aumentare gli investimenti nella sicurezza informatica, il modo in cui si **comunica sulla sicurezza** deve cambiare profondamente.

48%

Il 48% ritiene che per eliminare i rischi più rapidamente, **deve cambiare e migliorare soprattutto la condivisione delle conoscenze**, in pratica come il settore della sicurezza comunicherà in futuro

37%

Il 37% crede che utilizzare **un linguaggio meno tecnico** aiuterebbe il settore a comunicare meglio, in modo che l'intera organizzazione possa comprendere i rischi e come proteggersi

Un cambiamento nella comunicazione è fondamentale se i professionisti della sicurezza informatica devono reagire alla velocità necessaria per proteggere le proprie organizzazioni e ottenere investimenti.

La guerra informatica è una preoccupazione molto seria

I rischi della guerra informatica sono in aumento e, sebbene preoccupati, alcuni professionisti della sicurezza informatica non sono ancora preparati adeguatamente.

Il 53% prevede che l'aumento della guerra informatica sarà dannoso per l'economia entro i prossimi 12 mesi

53%

47%

Il 47% dei professionisti italiani ritiene che lo stato di guerra informatica sia una minaccia per la propria organizzazione.

Malgrado le preoccupazioni, almeno **il 32% non ha una strategia** per proteggersi dalla guerra informatica

32%

Secondo più di un terzo (33%), una migliore comprensione del panorama delle minacce (33%) o investire in più difese di sicurezza informatica (38%) sono i modi migliori per combattere la guerra informatica.

L'ascesa e il declino (e la nuova ascesa) dei ransomware

Gli attacchi ransomware sono di nuovo in aumento, ma la sicurezza contro questo tipo di incidenti non è migliorata allo stesso ritmo.

44%

Il 44% concorda sul fatto che stanno assistendo a una recrudescenza degli attacchi ransomware, ma la protezione contro di essi non è progredita molto negli ultimi 5 anni.

46%

Il 46% è preoccupato che un attacco ransomware possa far chiudere l'attività entro i prossimi 12-18 mesi, se non si aumentano gli investimenti in materia di sicurezza

35%

Più di un terzo (35%) ritiene che se la propria attività subisse un attacco ransomware, **il riscatto verrebbe pagato**

La realtà è che i ransomware sono qui per restare e occorre trovare, creare e investire in difese migliori.

Tutti sono connessi ma non protetti

Il 34% dei professionisti della sicurezza italiani e **40% a livello globale** ritengono che sia facile per gli hacker ottenere il controllo dei dispositivi IoT, utilizzati dai dipendenti a casa per scopi lavorativi

Il 64% dei professionisti della sicurezza informatica italiani ritengono che, come risultato del maggiore utilizzo di dispositivi IoT, le conoscenze sulla sicurezza su come proteggere questi dispositivi **siano migliorate** all'interno della loro attività

Tuttavia, il 23% afferma che i dispositivi IoT continueranno a diffondersi più velocemente di quanto possano essere protetti nei prossimi 12-18 mesi

Il ritmo con cui i dispositivi IoT vengono utilizzati, è più rapido della sicurezza messa in atto per proteggere gli utenti.

Metodologia

Sono stati intervistati 6.274

professionisti della sicurezza informatica

Gli intervistati vengono da **Stati Uniti, Regno Unito, Australia/Nuova Zelanda, Germania, Francia, Italia, Spagna, Danimarca** e **Svezia**, e rappresentano le risposte di utenti con un ruolo lavorativo o un'influenza decisionale sulla sicurezza informatica in aziende con 100 o più dipendenti. Oltre 10.000 imprese in un'ampia varietà di settori, tra cui finanza, governo ed energia.

Lo scenario globale delle minacce è in costante evoluzione.

Scopri come puoi restare sempre un passo avanti