CISCO
SECURE

5 metodi collaudati per migliorare la cybersecurity

Le sfide della cybersecurity continuano. Ogni giorno il nostro mondo diventa sempre più connesso e complesso. E per i team di cybersecurity, la complessità comporta maggiori responsabilità.

Fortunatamente, le aziende possono adottare misure concrete per rafforzare la sicurezza. Nel nostro report Studio sui risultati della sicurezza, 2a edizione abbiamo raccolto i dati provenienti da oltre 5.100 professionisti del settore IT e sicurezza di 27 paesi. Da questi dati emergono cinque procedure che favoriscono il successo dei programmi di cybersecurity. Eccole elencate di seguito.

Aggiornare la tecnologia

Il 39% delle tecnologie di sicurezza usate dalle aziende è considerato obsoleto.

Non aspettare che si verifichi un incidente per valutare la tua infrastruttura informatica. Adotta una strategia di aggiornamento della tecnologia più proattiva.

> Quasi il 40% delle aziende usa tecnologie di sicurezza obsolete, perciò il deficit di sicurezza è un problema concreto. Ma la cosa positiva è che le aziende con architetture cloud moderne e consolidate conseguono un alto livello di aggiornamento tecnologico adottando una strategia tecnologica proattiva: la soluzione per il problema.
>
> Richard Archdeacon, Advisory CISO, Cisco

Integrare per ottenere maggiore visibilità

Il 77% delle aziende preferisce acquistare soluzioni già integrate anziché occuparsi dell'integrazione.

Fortunatamente, il crescente successo delle soluzioni basate sul cloud rende le integrazioni più accessibili, offrendo ai team di sicurezza maggiore visibilità sui propri sistemi.

> Le tecnologie IT di sicurezza moderne e ben integrate contribuiscono al successo complessivo dei programmi di sicurezza, più di qualsiasi altra procedura o controllo.
>
> Helen Patton, Advisory CISO, Cisco

Ampliare il team

Le organizzazioni con i team di sicurezza più numerosi hanno il 20% di probabilità in più di essere efficienti nel rilevamento e negli interventi di risposta alle minacce.

L'ampliamento del team non è possibile? Valuta la possibilità di rafforzare le competenze del personale esistente. La formazione è sempre un investimento intelligente.

> Scegliere le persone più qualificate per il tuo team di SecOps è più importante che il numero di persone nel team. L'automazione può sopperire alle carenze del personale inesperto, permettendo di conseguire gli stessi risultati ottenibili con personale più esperto.
>
> Wendy Nather, Head of Advisory CISOs, Cisco

Lavorare in modo più efficiente con l'intelligence sulle minacce

Le aziende che usano l'intelligence sulle minacce hanno il doppio delle probabilità di essere efficienti nel rilevamento e negli interventi di risposta.

A prescindere dalla possibilità di ampliare il team, utilizza tutti gli strumenti di intelligence disponibili per sopperire a eventuali carenze. Lavora in modo più efficiente per ottenere risultati migliori.

> Quando le aziende impiegano persone competenti, processi efficienti e tecnologie efficaci, raggiungono capacità avanzate di rilevamento e risposta se sono integrate da una solida intelligence sulle minacce.
>
> Dave Lewis, Advisory CISO, Cisco

Creare problemi intenzionalmente

Le aziende che adottano tecniche di ingegneria del caos hanno il doppio di probabilità di migliorare la continuità delle attività aziendali.

L'interruzione regolare e intenzionale dell'infrastruttura IT preparerà la tua azienda a gestire le minacce reali. Usa il caos per prepararti a risolverlo.

> Le aziende che conducono test regolari di vario tipo hanno probabilità 2,5 volte maggiori di mantenere la continuità operativa in caso di emergenza. Si possono ottenere risultati ancora migliori adottando l'ingegneria del caos.
>
> Wolfgang Goerlich, Advisory CISO, Cisco

L'adozione di queste misure collaudate ti metterà sulla buona strada per ottenere una migliore postura di cybersecurity. Ma non limitarti a crederci sulla parola: scopri tutti i dati del nostro studio leggendo il report completo.

Scarica il report

CISCO The bridge to possible