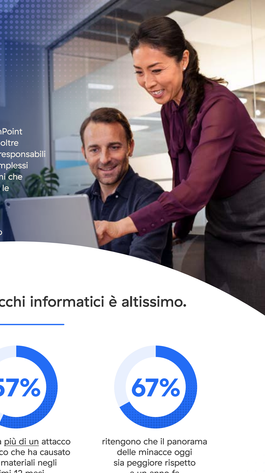


Il report dei CISO

La prospettiva dei CISO

Redatto da CISOs Connect in collaborazione con AimPoint Group e W2 Communications, il Report dei CISO va oltre i titoli delle testate per rivelare i principali timori dei responsabili della sicurezza informatica di oggi, i problemi più complessi che i loro team devono affrontare e le priorità e i piani che stanno mettendo in atto per difendere con successo le proprie organizzazioni.

Una conclusione fondamentale: l'implementazione di un modello di sicurezza zero trust è al primo posto tra le priorità dei CISO di oggi.

Il rischio di subire attacchi informatici è altissimo.

75%
colpite da almeno un attacco informatico che ha causato danni materiali negli ultimi 12 mesi

57%
colpite da più di un attacco informatico che ha causato danni materiali negli ultimi 12 mesi

67%
ritengono che il panorama delle minacce oggi sia peggiore rispetto a un anno fa

Le minacce informatiche più preoccupanti

- Ransomware
- Phishing/ spear phishing
- Attacchi alla catena di approvvigionamento

I punti deboli e le conseguenze che preoccupano maggiormente i CISO

Le principali vulnerabilità

N° 1
Punti deboli di terzi nella sicurezza (ad esempio i partner collegati)

N° 2
Software/ sistemi senza patch

N° 3
Lacune nella sicurezza sul cloud

Conseguenze di un attacco riuscito

N° 1
Esposizione di dati personali/dati dei clienti

N° 2
Tempo di inattività di infrastrutture/servizi critici

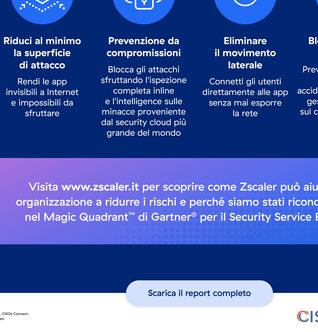
N° 3
Danno al marchio o alla reputazione

Le conseguenze esterne sono quelle che preoccupano maggiormente i CISO, perché sono quelle con gli effetti di più ampia portata, che vanno oltre le mura di un'organizzazione.

La strategia migliore

In risposta a una superficie di attacco in espansione e a un panorama di minacce in costante evoluzione, la maggior parte delle organizzazioni sta attualmente adottando un modello di sicurezza zero trust.

Qual è la condizione della tua organizzazione in relazione a un modello di sicurezza zero trust?



96,5%
Percentuale di CISO che punta su un modello di sicurezza zero trust per migliorare il profilo di sicurezza della propria organizzazione

L'identità è il nuovo perimetro

Con il crescente utilizzo del cloud e il lavoro a distanza, le app, i sistemi e gli utenti si stanno spostando dall'interno all'esterno dell'azienda fisica. Questa tendenza ha eroso il perimetro di rete legacy, rendendolo inefficace come confine per l'attribuzione dell'attendibilità. Un risultato importante, nonché un principio cardine dello zero trust, è che l'identità sta diventando il nuovo perimetro. I CISO stanno adottando varie misure per tenere conto di questa nuova realtà, tra cui:

- **Investimenti in soluzioni volte a ridurre il rischio di esposizione delle credenziali e delle informazioni sull'identità**
- **Incremento dell'ispezione dei dispositivi degli utenti prima che venga concesso l'accesso**
- **Investimenti nell'autenticazione a più fattori di nuova generazione, che offre un'esperienza utente senza ostacoli**
- **Accelerazione dell'implementazione di un modello di sicurezza zero trust**

I principali investimenti tecnologici

Percentuale di intervistati che intendono investire in ciascuna delle seguenti tecnologie nei prossimi 12 mesi:

63%
rete/ microsegmentazione

56%
piattaforma SSE (Security Service Edge)

53%
Piattaforme di protezione delle applicazioni native del cloud (CNAPP)

41%
deception / difesa attiva

Cosa può fare Zscaler

Zero Trust Exchange di Zscaler consente una trasformazione cloud sicura, e protegge utenti, applicazioni e carichi di lavoro indipendentemente dalla loro posizione. Grazie al security cloud più grande del mondo, Zscaler blocca le minacce sfruttando un approccio a quattro livelli:

Riduci al minimo la superficie di attacco
Rendi le app invisibili a Internet e impossibili da sfruttare

Prevenzione da compromissioni
Blocca gli attacchi sfruttando l'ispezione completa inline e l'intelligence sulle minacce provenienti dal security cloud più grande del mondo

Eliminare il movimento laterale
Connetti gli utenti direttamente alle app senza mai esporre la rete

Blocca la perdita di dati
Previeni il furto di dati e l'esposizione accidentale su dispositivi gestiti e non gestiti, sul cloud pubblico e sui servizi SaaS.

Visita **www.zscaler.it** per scoprire come Zscaler può aiutare la tua organizzazione a ridurre i rischi e perché siamo stati riconosciuti leader nel Magic Quadrant™ di Gartner® per il Security Service Edge (SSE).

Scarica il report completo

CISOs CONNECT