

Gli operatori finanziari sopravvalutano la propria strategia di resilienza informatica

Un nuovo report di Zscaler, “**Sblocca il Fattore resilienza: perché essere « Resilient by Design » sarà un imperativo nel campo della sicurezza informatica**”, evidenzia la necessità di dare una maggiore priorità e incrementare gli investimenti a supporto di strategie di resilienza informatica per rispondere agli inevitabili scenari di crisi del futuro.



DATI CHIAVE DEL SETTORE FINANZIARIO

Sullo sfondo di minacce crescenti e di ambienti operativi sempre più volatili, la continuità operativa è messa a dura prova

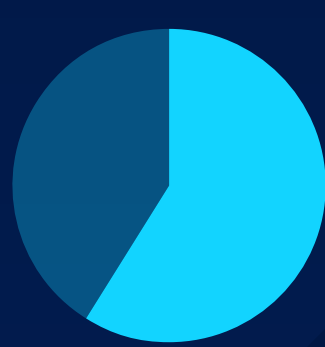
45%

delle organizzazioni ha vissuto una **crisi significativa** nel corso degli ultimi 6 mesi

58%

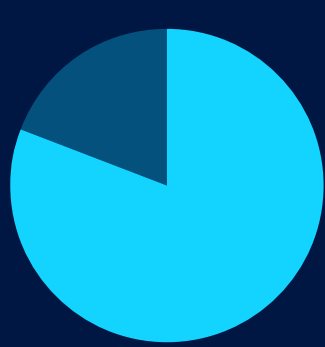
delle organizzazioni prevede di assistere a una crisi significativa entro i **prossimi 12 mesi**

I responsabili IT si sentono all'altezza di rispondere a questi scenari di crisi



59%

dei leader IT ritiene che la propria infrastruttura IT sia **altamente resiliente**



81%

considera l'approccio della propria organizzazione alla resilienza informatica **matturo**



96%

ritiene che le attuali misure di resilienza informatica della propria organizzazione siano **efficaci**

Tuttavia, un esame più attento rivela incongruenze, lacune e inefficienze

SOLO

49%

dei leader IT afferma che la propria strategia di resilienza informatica è **aggiornata** per rispondere al sempre maggiore utilizzo dell'intelligenza artificiale

40%

ammette di **non aver rivisto** la strategia di resilienza informatica negli ultimi 6 mesi

Meno della metà delle organizzazioni utilizza almeno uno dei seguenti strumenti proattivi per la sicurezza informatica



IDENTIFICAZIONE DEI RISCHI

42%



MICRO-SEGMENTAZIONE ZERO TRUST

47%



TECNOLOGIE DI DECEPTION

34%

La mancanza di investimenti da parte della leadership è stata identificata come un ostacolo critico



SOLO il 44%

dei responsabili IT ritiene che la resilienza informatica sia una priorità assoluta per la leadership



Il 46%

concorda sul fatto che il budget assegnato alla resilienza informatica non è allineato con una necessità crescente



SOLO il 44%

afferma che la strategia di resilienza informatica è inclusa nella strategia di resilienza complessiva della propria organizzazione



SOLO il 46%

afferma che il CISO è coinvolto nella pianificazione della resilienza

È necessario un cambiamento di mentalità per superare le principali barriere che ostacolano l'implementazione di una solida strategia di resilienza informatica

Il 61%

dei responsabili IT ritiene che la propria organizzazione attribuisca una priorità eccessiva alla prevenzione nella propria strategia di sicurezza informatica

Il 59%

continua a limitare il concetto di “falla” nella sicurezza informatica al solo accesso iniziale (da parte di un aggressore)

I tre principali ostacoli alla resilienza:

46%

COMPLESSITÀ DELL'IT E DELL'INFRASTRUTTURA DI SICUREZZA

32%

MANCANZA DI RISORSE E COMPETENZE

31%

PROBLEMATICHE RELATIVE ALLA SICUREZZA/INFRASTRUTTURE IT LEGACY

Integrare la resilienza informatica nella strategia aziendale sin dal principio

I responsabili IT sono consapevoli della correlazione tra una solida strategia di resilienza informatica e migliori prestazioni aziendali, ma hanno difficoltà a ottenere risultati tangibili attraverso le misure esistenti.

Il 56%

sta assistendo a una **riduzione della** perdita dei dati

53%

stanno riscontrando un **processo più rapido di** ripristino dagli incidenti

51%

segnala un' **accelerazione delle** procedure di rilevamento e contenimento degli incidenti

Oggi più che mai, le organizzazioni del settore finanziario sono chiamate a prestare maggiore attenzione alla resilienza informatica e a considerarla una priorità, aumentando i relativi investimenti, ottimizzandola e rivedendola periodicamente e alzando le aspettative in questo ambito. È necessario un cambiamento radicale nell'approccio e nella mentalità per rendere la resilienza informatica una parte vitale della strategia di sicurezza fin dal principio. Questa è l'essenza di ciò che definiamo « **Resilient by Design** ».

Scopri di più su come adottare un approccio « Resilient by Design » implementando la piattaforma Zero Trust Exchange, qui. [Leggi il report](#)

METODOLOGIA

A dicembre del 2024, Zscaler ha incaricato Sapio Research di condurre un'indagine che ha coinvolto 1.700 responsabili decisionali nel campo IT (responsabili IT) in 12 mercati (Australia, Francia, Germania, Giappone, India, Italia, Paesi Bassi, Singapore, Spagna, Svezia, Regno Unito e Irlanda, Stati Uniti), 259 dei responsabili IT che sono stati interpellati lavorano in aziende del settore finanziario.

INFORMAZIONI SU ZSCALER

Zscaler accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 160 data center a livello globale, Zero Trust Exchange, basata sull'SSE, è la più grande piattaforma di cloud security inline del mondo.