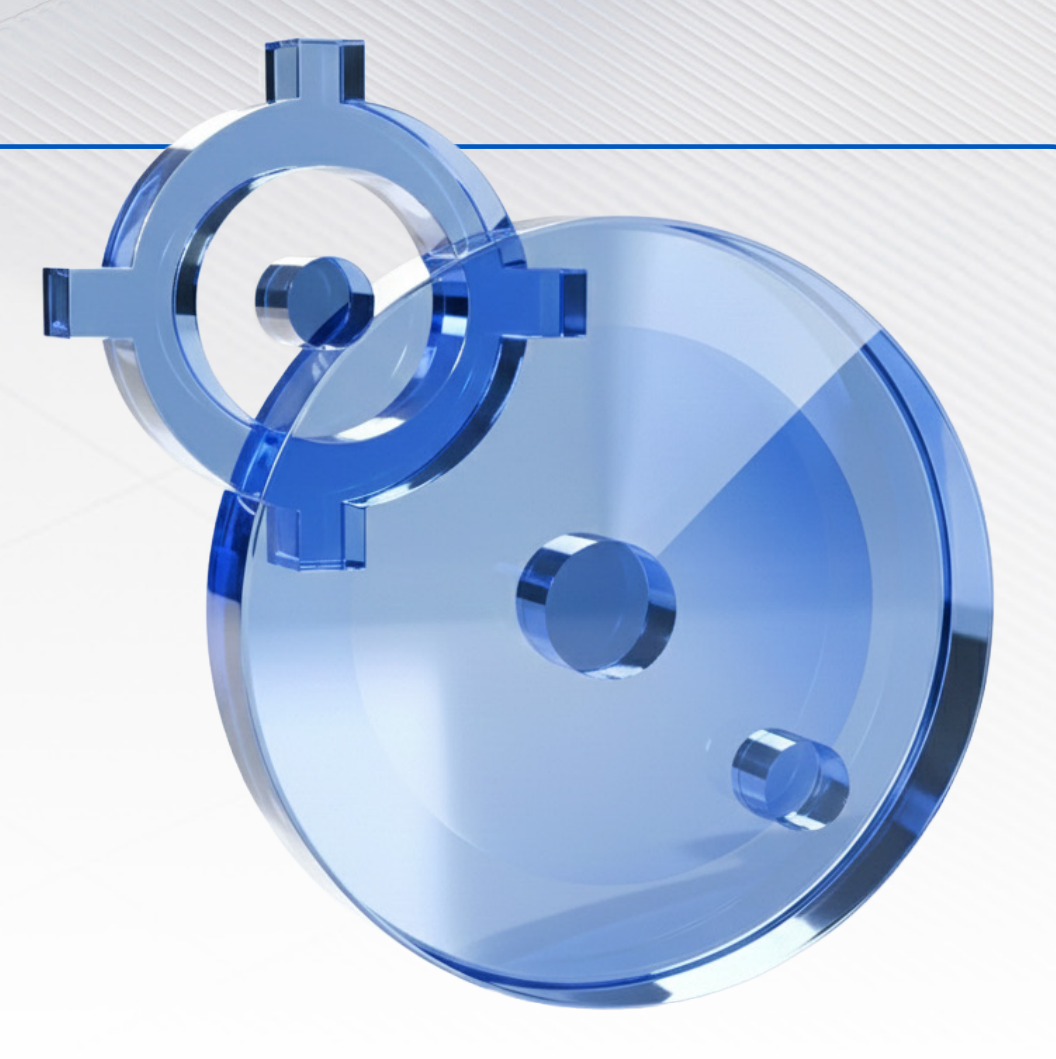
Oltre la Cyber Security: costruire la resilienza digitale per la continuità operativa.

I moderni leader IT devono prevedere le interruzioni operative, non solo prevenirle.

Cyber Security e resilienza digitale a confronto



La Cyber Security si incentra sull'arresto degli attacchi. La resilienza digitale garantisce la continuità operativa aziendale durante e dopo un attacco.

Cyber Security

prevenzione, difesa perimetrale, prevenzione delle violazioni

Resilienza digitale

adattabilità, ripristino, continuità aziendale

L'impatto della continuità operativa nei diversi settori

L'importanza della resilienza digitale nei settori critici

Interruzioni operative e tempi di fermo dovuti agli attacchi informatici colpiscono ogni attività, ma le conseguenze possono variare nei diversi settori.

Sanità

60%

delle organizzazioni sanitarie segnala che gli incidenti informatici interrompono i servizi di assistenza ai pazienti.[1]

Perché è importante

Un'interruzione operativa può ritardare la cura, allontanare i pazienti e compromettere la sicurezza.

Retail

43%

dei retailer ha subito una grave interruzione causata da incidenti informatici lo scorso anno.[2]

Perché è importante

Anche interruzioni di breve durata possono incidere sul fatturato, sulla visibilità dell'inventario e sull'esperienza del cliente.

Servizi finanziari

91%

degli istituti finanziari ha subito almeno un incidente informatico nello scorso anno.[3]

Perché è importante

Un'interruzione operativa può influire sull'elaborazione delle transazioni, sulla fiducia dei clienti e sulla conformità normativa.

Logistica e trasporti[4]

94%

delle organizzazioni afferma che le interruzioni informatiche possono innescare errori a catena nella supply chain.[5]

Perché è importante

Un'interruzione operativa ostacola la tracciabilità delle spedizioni, le operazioni di magazzino e la puntualità delle consegne.

Pubblica amministrazione

60%

delle interruzioni di rete ha un costo di circa 1 milione di dollari in interruzioni operative.[6]

Perché è importante

Le interruzioni incidono sui servizi offerti ai cittadini, sulla risposta alle emergenze e sulla fiducia del pubblico.

L'interruzione operativa sospende la continuità aziendale

L'inattività non incide solo sui sistemi IT, ma sul fatturato, sulle operazioni e sulla reputazione

96%

delle **organizzazioni** ha sperimentato almeno un'interruzione negli ultimi tre anni.

80%

afferma che le interruzioni stanno diventando più gravi.[7]

La ridondanza tradizionale non funziona contro il ransomware

La ridondanza protegge contro i guasti hardware, ma non può nulla contro gli attacchi intelligenti e autopropaganti.

La replica può diffondere l'infezione

Troppi strumenti di disaster recovery e backup creano punti ciechi

La proliferazione degli strumenti aumenta i tempi di ripristino e il rallentamento operativo

La moderna resilienza esige nuovi parametri di ripristino

La velocità, da sola, non è più sufficiente: il ripristino deve essere privo di virus e in linea con gli obiettivi aziendali.

RTO

Tempo massimo per tornare operativi

RPO

Massima perdita di dati accettabile

MTD

Periodo massimo di interruzione tollerabile prima del fallimento aziendale

MTCR

Tempo necessario a ripristinare un ambiente verificato e privo di malware

Il ripristino pulito è oggi un requisito di continuità

La velocità di ripristino è inutile se i sistemi ripristinati sono compromessi.

- Costo medio di una violazione dei dati: 4,45 milioni di dollari.
- L'interruzione operativa è il componente di costo più elevato delle violazioni.[8]

Le priorità dei leader IT aziendali

La resilienza è una decisione economica e operativa.

Azioni prioritarie (ad alto livello)

Allineare la protezione con la criticità delle risorse.

Testare il ripristino in scenari digitali reali.

Verificare i backup prima del ripristino.

Ridurre la complessità con piattaforme unificate.

La resilienza digitale favorisce la continuità, la fiducia e il controllo, anche quando gli attacchi sono inevitabili

Dalla Cyber Security alla resilienza digitale con Acronis

Per la Cyber Security la semplice protezione non basta. Serve la resilienza. Scopri come Acronis può aiutarti ad anticipare le minacce, resistere agli attacchi, riprenderti più velocemente e adattarti al futuro.

Contattaci

---

[1] Dipartimento statunitense per la salute e i servizi sociali, https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute, "Annual Outage Analysis 2023", https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] World Economic Forum, "Global Cybersecurity Outlook 2024", https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] World Economic Forum – Global Risks Report, https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid.

[6] Intelligent CIO, "US government organizations lose millions in an average network outage or breach", https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute, "Annual Outage Analysis 2023", https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM, "Cost of a Data Breach Report 2025", https://www.ibm.com/reports/data-breach