Acronis

#CyberFit

Come adottare una strategia di disaster recovery efficace

Sommario

Introduzione

Potrebbe sembrarvi che il backup sia sufficiente. Potreste non comprendere l'importanza di dati, sistemi e applicazioni finché non vengono compromessi. Il disaster recovery è quel passaggio ulteriore che vi consente di tornare operativi in tempi rapidi dopo un'interruzione dell'attività. Molte aziende credono che non ne avranno mai bisogno. Ma è davvero così?

Che cos'è il disaster recovery?

Per essere efficace, una soluzione di disaster recovery deve essere supportata dal backup. Il disaster recovery include le copie più recenti dei dati e funzionalità di elaborazione in una piattaforma che offre la disponibilità automatica delle risorse più critiche: dati, applicazioni e sistemi.

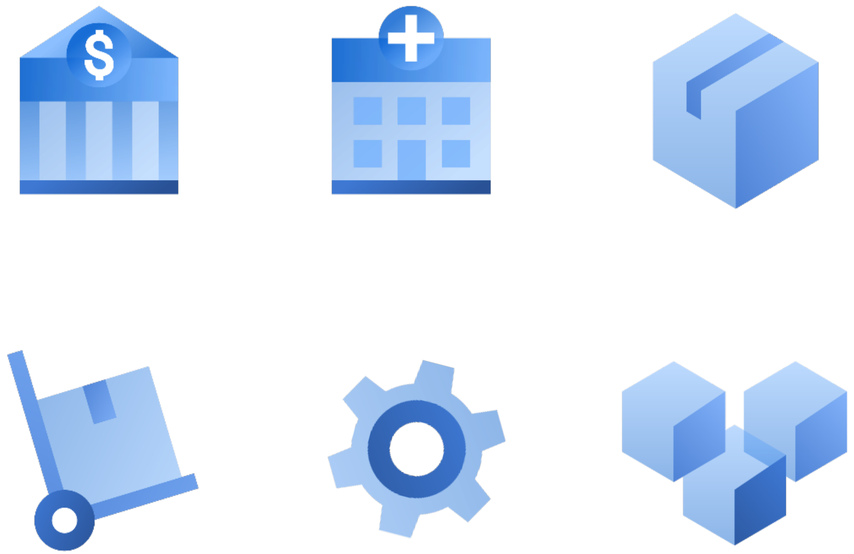
Assicura che i processi interdipendenti vengano ripristinati nell'ordine corretto, nel punto di ripristino corretto e al momento giusto.

La vostra azienda è pronta?

Chi ha bisogno del Disaster Recovery as a Service (DRaaS)? Tutti. Eventi avversi possono colpire qualsiasi azienda. Potreste trovarvi in aree soggette a calamità naturali o non avere le risorse tecniche o l'esperienza necessaria per implementare un programma di disaster recovery.

Settori come i seguenti si basano su applicazioni e dati mission-critical o rischiano di incorrere in pesanti multe in caso di mancata conformità alle normative:

- Servizi finanziari
- Healthcare
- Settore giuridico
- Trasporti
- Telecomunicazioni
- Produzione industriale
- Settore edile
- Settore energetico
- eCommerce
- Servizi
- Supply chain e logistica



Non è solo una questione di IT

Tornare operativi in tempi rapidi non è solo un problema legato all'IT. Le interruzioni possono riguardare anche altri reparti, come quello delle risorse umane, l'ufficio finanziario o quello legale, coinvolgendo l'intera azienda.

IT

- Backup e ripristino
- SLA interni ed esterni
- Soddisfazione dei dipendenti
- Audit
- Conformità e normative

Alta dirigenza

- Piani di continuità operativa
- Percezione del mercato
- Produttività dei dipendenti
- Conformità e normative
- Assicurazione

Finanza

- Conformità e normative
- Protezione dei dati sensibili
- Gestione delle operazioni commerciali
- Fiducia economica e dei mercati
- Audit

Risorse umane

- Pianificazione del personale e della forza lavoro
- Formazione
- Produttività dei dipendenti
- Protezione dei dati sensibili

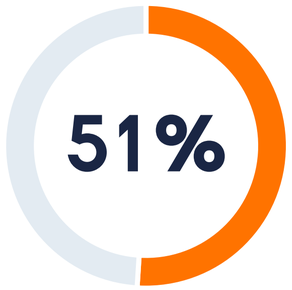
Settore giuridico

- Conformità e normative
- Protezione dei dati sensibili
- Assicurazione

La realtà

Eventi avversi possono colpire in qualsiasi momento e in vari modi. Siamo qui per impedire che queste statistiche riguardino anche la vostra azienda.

Violazioni dei dati del 2019 che sono state causate da cancellazione o sovrascrittura accidentale di file o cartelle[1]



Violazioni dei dati del 2019 che sono state causate da attacchi malevoli e criminali[1]

Organizzazioni che probabilmente subiranno un'interruzione dell'attività entro il 2022 in seguito alla perdita di dati non ripristinabili[2]

Aziende che hanno subito un attacco negli ultimi tre anni[3]

2,2 giorni

Durata media di un'interruzione dell'attività[2]

$ 5.600

Costo medio al minuto[2]

$ 3,92 MLN

Costo totale medio di una violazione dei dati[2]

1) Ponemon Institute, 2019. 2) Gartner, 2019. 3) IDC, 2019

Le minacce

Quali minacce dovreste prendere in considerazione? Alcune aziende ritengono che le interruzioni dell'attività siano dovute soltanto a calamità naturali che bloccano l'erogazione di energia elettrica ai sistemi hardware. In realtà, occorre prendere in considerazione anche il software e le persone. Parallelamente allo sviluppo della tecnologia, si assiste all'aumento delle minacce interne ed esterne.

Calamità naturali

Uragani, tornado e incendi possono causare gravi interruzioni dell'attività che interessano le strutture e le infrastrutture.

Quello che la maggior parte delle aziende potrebbe non comprendere è che solo il 6% delle interruzioni è causato da calamità naturali.

Pandemie

Questo tipo di minaccia colpisce le persone di un'organizzazione e, nel caso del telelavoro, richiede la gestione di una serie di scenari di pianificazione che i reparti IT potrebbero non avere considerato in precedenza.

Esiste un rischio maggiore quando i dati e i dispositivi escono dalla consueta infrastruttura IT.

Guasti all'hardware e danneggiamento del software

Un guasto all'hardware può essere causato da un'interruzione di corrente. Il software può danneggiarsi in seguito ad aggiornamenti non funzionanti o a una formattazione non corretta delle unità.

Errore umano intenzionale o meno

È successo a molti di noi di avere accidentalmente cancellato o sovrascritto dati o cartelle.

Ma un dipendente insoddisfatto potrebbe colpire intenzionalmente la propria azienda danneggiando dati e sistemi.

Attacchi informatici

La compromissione del sistema di un solo dipendente può rendere vulnerabili intere reti.

Gli attacchi possono avvenire abbastanza rapidamente tramite l'individuazione di password deboli, campagne di phishing e link dannosi.

Il disaster recovery si è evoluto

Anni '90

Data center aziendale o housing in data center

- Hardware obsoleto
- Networking
- Licensing
- Piattaforme di replica
- Enormi quantità di storage

Anni 2000

Approccio ibrido

- Opzioni di licensing costose
- Complesso
- Copertura limitata

Anni 2010

Disaster recovery moderno ibrido in cloud

- Economicamente conveniente
- Facile da usare
- Pronto all'uso

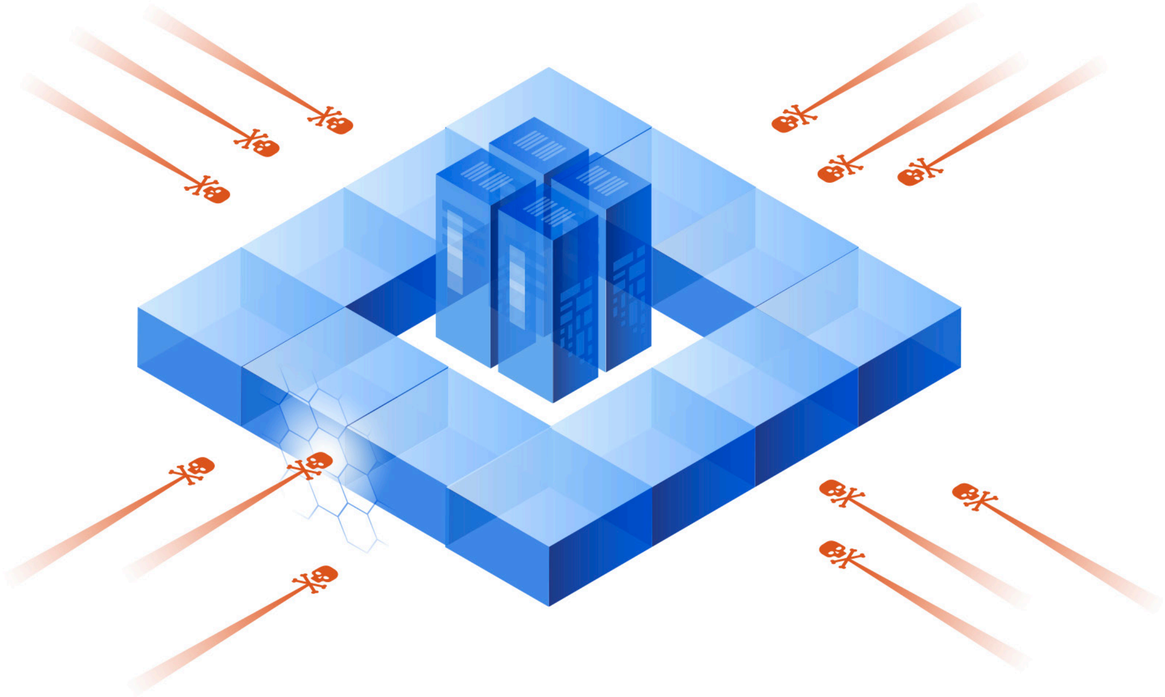
10 motivi per cui dovete investire nel disaster recovery

Sono numerose le ragioni per cui dovreste non limitarvi al backup e adottare invece una strategia di disaster recovery.

- Usufruite di costi mai stati così **ridotti**
- **Riducete al minimo l'impatto** di qualsiasi evento avverso
- Garantite la **produttività continua dei dipendenti**
- Soddisfate i requisiti di **conformità e normativi**
- Eseguite **ripristini istantanei**
- **Riducete i tempi di interruzione** dell'attività
- **Contenete** potenziali **perdite economiche**
- **Riducete gli** obblighi in materia di responsabilità
- **Riducete al minimo il rischio** di esposizione negativa
- **Agevolate** la gestione delle crisi

Vista la varietà di fattori interni ed esterni che possono avere un impatto negativo sui vostri sistemi e sui vostri dati...

il problema non è se subirete una perdita di dati, ma quando.



Calcolate il costo delle interruzioni dell'attività

Questi fattori possono essere applicati alla vostra organizzazione: utilizzate i costi e i dati dei vostri reparti per calcolare il costo orario effettivo delle interruzioni dell'attività. In sintesi: le interruzioni dell'attività hanno costi ingenti.

Perdita di profitti + perdita di produttività + costi di ripristino + costi intangibili = costo delle interruzioni dell'attività (all'ora)

Perdita di profitti

Questo elemento è abbastanza semplice da comprendere. Se la vostra azienda è ferma, non potete generare profitti.

Utilizzate il fatturato annuale lordo per calcolare i profitti mancati di ogni funzione aziendale per ogni ora di interruzione dell'attività.

Perdita di produttività

Il costo delle interruzioni dell'attività aumenta quando i vostri dipendenti non sono in grado di lavorare o sono costretti a svolgere attività che non generano profitti. Gli stipendi o le retribuzioni orarie rappresentano un costo fisso e devono essere pagati indipendentemente dalla produttività dei dipendenti.

Costo del ripristino

Spesso non si pensa ai costi associati al ripristino e alla ripresa delle normali operazioni aziendali. In genere, i costi riguardano:

- servizi e tempo dei dipendenti necessari per ripristinare i dati persi
- strumenti fisici/dispositivi che devono essere riparati o sostituiti
- dati persi

Costi intangibili

Qualsiasi danno alla reputazione o al marchio comporta una perdita economica. Anche la minima interruzione dell'attività può gettare un'ombra pesante sulla vostra azienda e il modo in cui tale interruzione viene gestita può determinare la ripresa o il fallimento.

Opzioni per un programma di disaster recovery

Quando si gestisce un programma di disaster recovery, è necessario:

- **Personale per:**
  - Valutazioni
  - Progettazione
  - Test
  - Implementazione
  - Gestione
- **Formazione**
- **Documentazione**
- **Rapporti**
- **Infrastruttura di ripristino**

Se scegliete un partner Acronis certificato avrete a disposizione:

- **La nostra pluriennale esperienza nel campo del disaster recovery**
- **Servizi di disaster recovery attivabili in modo rapido e semplice**
- **Un modello di erogazione continuo ed efficiente**
- **Supporto 24/7**
- **Funzionalità di test semplificate**
- **Monitoraggio e gestione**
- **Risorse integrate di cloud storage e calcolo**
- **Spese operative contenute**

Mantenere sempre operativa l'azienda non è mai stato così facile

Immaginate di utilizzare un unico agente. Una singola console. Un solo cloud.

Protezione dei dati

+

Cyber Security

+

Disaster Recovery

Backup e ripristino

Obiettivo primario:

- Prevenzione della perdita di dati importanti
- Dati situati su server, workstation e dispositivi mobile

Gestione e sicurezza degli endpoint

Obiettivo primario:

- Rilevamento e deviazione degli attacchi malware
- Vulnerability assessment e gestione delle configurazioni
- Filtraggio degli URL
- Patch management

Disaster Recovery

Obiettivo primario:

- Disponibilità elevata delle applicazioni critiche
- Ripristino rapido per evitare costose interruzioni dell'attività

Acronis

#CyberFit

Grazie.

Contattateci oggi stesso per discutere di come possiamo aiutarvi a tornare operativi in tempi rapidi dopo un evento avverso.

www.acronis.com | dr@acronis.com