

Promuovere la resilienza operativa con il supporto e i servizi IT

Punti salienti

Supporto infrastruttura

Visibilità e assegnazione delle priorità dei rischi IT

Gestione del rischio con servizi di supporto proattivo

Gestione del rischio con una strategia di supporto consolidata per i data center

Test di resilienza operativa

In seguito al continuo aumento degli incidenti di cybersecurity, non sorprende il fatto che stia emergendo una legislazione sulla resilienza operativa nel settore finanziario. Che si tratti del Digital Operational Resiliency Act (DORA) nell'Unione Europea, di indicazioni normative come la SR 20-24, Sound Practices to Strengthen Operational Resilience negli Stati Uniti, o la Operational Risk and Resilience Guidance in Canada, queste normative stanno aumentando le aspettative nei confronti degli istituti finanziari per quanto riguarda la governance, l'identificazione e la gestione dei rischi, nonché la resilienza operativa e la gestione dei rischi di soggetti terzi. Naturalmente, l'obiettivo finale è quello di garantire che le organizzazioni finanziarie siano dotate delle giuste strategie per mettere in atto misure di prevenzione e di ripristino in caso di attacchi informatici, corruzione dei dati, guasti catastrofici al sistema o altri tipi di incidenti. In molti casi, la non conformità e/o il guasto possono comportare pesanti sanzioni finanziarie per le aziende coinvolte.

IBM offre una gamma di servizi e soluzioni per consentire alle entità finanziarie di gestire la sicurezza e la resilienza operativa. IBM Consulting fornisce servizi per la valutazione del rischio, la governance e i controlli del rischio, nonché per la gestione del rischio ICT di terze parti. Le soluzioni software IBM riducono fino al 90%¹ il tempo necessario per automatizzare il rilevamento dati e la governance, contribuendo alla conformità e al reporting. IBM Data Security aiuta a proteggere i dati e ad automatizzare la verifica della conformità. IBM Security offre assistenza nella segnalazione e nella gestione degli incidenti, IBM Security X-Force offre servizi per il rilevamento e il recupero dagli incidenti e per il rilevamento e la risposta gestiti, mentre IBM Control Desk con Maximo aiuta l'organizzazione a gestire e segnalare gli asset critici.

Oltre a questi servizi e soluzioni, IBM ritiene che il supporto e i servizi IT possano rappresentare un elemento importante nel panorama in continua evoluzione dei requisiti di resilienza operativa. IBM TLS offre ai clienti servizi e soluzioni di supporto che consentono di identificare e correggere in modo proattivo i potenziali problemi prima che si verifichino.

Supporto infrastruttura

La resilienza operativa dipende da un funzionamento regolare e sicuro dell'infrastruttura. Ciò significa trovare costantemente un equilibrio tra i costi e le risorse associati all'implementazione di nuove tecnologie, come il cloud ibrido o la containerizzazione, e la necessità di mantenere contratti di assistenza, almeno di base, per l'hardware e il software in produzione. Secondo IDC, "le imprese dovrebbero dare priorità ai servizi di supporto IT in base alla criticità dei workload, considerandoli come un investimento per preservare il valore aziendale di tali sistemi, affidandosi ai fornitori per ottimizzare le prestazioni". Il report rileva inoltre che le imprese intervistate stanno attualmente risparmiando 290 ore di tempo di inattività con contratti di assistenza per server, storage e networking; più precisamente, stanno prevenendo 79 ore di tempo di inattività non pianificato grazie a strumenti predittivi e di supporto proattivo.² Apparentemente, quanto più critico è il workload, tanto più dovrebbe essere preso in considerazione un supporto proattivo.

Per gestire efficacemente oltre sei milioni di ticket di assistenza all'anno, IBM si affida a un'infrastruttura di supporto globale che comprende strumenti basati sull'AI come Call Home, Remote Technical Support (RTS) e Cognitive Support Platform (CSP). Il supporto da remoto di IBM è progettato per connettersi automaticamente, eseguire analisi diagnostiche e recuperare/risolvere la maggior parte dei problemi, spesso entro un'ora. I team di supporto remoto di IBM risolvono il 74% dei problemi di hardware e di software.³ I Client Availability Leader e i Technical & Project Escalation Manager assicurano una gestione tempestiva delle situazioni critiche sia da remoto che in loco. L'approccio differenziato del supporto IBM con IBM Expert Care e IBM Multivendor Enterprise Care consente ai clienti di scegliere il livello di supporto migliore in base alle proprie esigenze.

Visibilità e assegnazione delle priorità dei rischi IT

Una delle domande fondamentali che le organizzazioni dovrebbero porsi è come monitorare e valutare in modo proattivo i rischi IT per quantificare e dare priorità a quelli più critici. La visibilità della struttura può rivelarsi complessa, mentre i rischi informatici cambiano di frequente. Anche in questo caso, la visibilità da sola non è sufficiente. I rischi devono essere compresi, valutati e classificati in ordine di priorità, nonché tradotti in piani d'azione tempestivi che gestiscano efficacemente e prontamente i rischi più critici.

IBM Support Insights, incluso nei contratti di assistenza e manutenzione in garanzia dell'infrastruttura IBM, fornisce visibilità sull'intera struttura IT, oltre a comunicare le potenziali criticità e le azioni consigliate per determinati fornitori. Questo servizio basato sul cloud agisce come un unico pannello di controllo, che unifica l'esperienza di supporto in tutta l'infrastruttura IBM e multivendor, fornendo insight basati su analytics, gestione dell'inventario e raccomandazioni di manutenzione preventiva. L'abbonamento IBM Support Insights Pro offre un valore aggiuntivo con insight prioritari sulle vulnerabilità nella sicurezza e sul ciclo di vita, sistemi operativi consigliati e livelli di firmware, oggi incentrati su insight per IBM Power e CISCO.

Support Insights fornisce avvisi per diversi fattori di rischio, che includono le vulnerabilità nella sicurezza, la copertura del supporto, i rischi del sistema operativo/firmware e i rischi legati all'hardware. Oltre agli avvisi continui, lo strumento fornisce punteggi di rischio con una panoramica riepilogativa delle potenziali minacce all'ambiente IT.

Le categorie dei punteggi di rischio sono calcolate utilizzando dati e insight provenienti da diverse fonti e analisi:

- Sicurezza: vulnerabilità ed esposizioni comuni (CVE, Common Vulnerabilities and Exposures) per sistemi operativi noti e livelli di firmware
- Copertura: eventi di scadenza del contratto e della garanzia
- Firmware: eventi di fine supporto/fine del ciclo di vita del software e diversità del sistema operativo/firmware
- Hardware: eventi di fine supporto/fine del ciclo di vita del software (solo per l'infrastruttura IBM) e avvisi ai fornitori (solo per CISCO)

Questo aiuta a comprendere i rischi e fornisce le informazioni e gli approfondimenti necessari per individuare e attenuare efficacemente i possibili esiti negativi associati agli asset in questione. Gli avvisi includono un punteggio di rischio (alto, medio, basso) determinato in base al tipo, alla priorità e all'orizzonte temporale (immediato o previsto) del rischio. Ciò consente alle organizzazioni di stabilire rapidamente le priorità degli interventi di mitigazione in base ai livelli di rischio. Gli avvisi sono inoltre corredati da raccomandazioni specifiche per la mitigazione, che includono suggerimenti e opzioni specifiche per risolvere il problema in oggetto. A seconda della categoria di rischio, le raccomandazioni possono includere informazioni sulle patch da applicare, sulle versioni da aggiornare, sulle opzioni di sostituzione dei servizi di consulenza e altro ancora. Non tutti gli avvisi contengono raccomandazioni specifiche, ma in genere forniscono indicazioni sulle best practice da seguire per contribuire a ridurre i rischi derivanti dall'avviso.

Gestione del rischio con servizi di supporto proattivo

La visibilità del rischio informatico è il punto di partenza, ma sta poi al personale IT delle organizzazioni, già sotto pressione, seguire gli avvisi e intraprendere le azioni di mitigazione appropriate in modo tempestivo. Nel 2022, XForce ha individuato 23.964 vulnerabilità nella sicurezza.⁴Una volta che gli avvisi sono stati pubblicati, le organizzazioni sono tenute ad analizzarli, dare priorità a quelli da gestire per primi e avviare quindi le azioni di mitigazione. L'integrazione del personale IT con un supporto proattivo da parte del fornitore può consentire alle organizzazioni di dare priorità alle azioni di manutenzione quotidiane, che spesso possono subire ritardi a causa di problemi imprevisti e di progetti IT strategici.

IBM collabora con i clienti per personalizzare i servizi di assistenza e fornire soluzioni sia reattive che proattive. Alcuni esempi di diversi servizi di supporto che IBM può eseguire al posto del personale IT includono:

- Un unico punto di contatto per i problemi di gravità 1 e 2
- Determinazione del problema, identificazione dell'origine del problema e risoluzione dello stesso
- Piani di supporto personalizzati che includono processi operativi e di manutenzione, attuale struttura di supporto, applicazioni critiche, scenari di interruzione critici e ambiente
- Report che riassumono l'attività di assistenza per i problemi segnalati con suggerimenti proattivi
- Documentazione e mantenimento dei requisiti di disponibilità
- Analisi delle prestazioni e raccomandazioni per migliorarle
- Esecuzione di servizi di prevenzione

Puoi affidarti a IBM Technology Lifecycle Services per mantenere sempre operativi i tuoi sistemi mission-critical, 7 giorni su 7, 24 ore su 24

Gestione del rischio con una strategia di supporto consolidata per i data center

Secondo IDC, la proliferazione di fornitori nel data center ha un impatto diretto sul tempo di inattività riscontrato.² A ogni nuovo prodotto e fornitore corrispondono rischi di interoperabilità esponenziali. Con contatti separati per ogni fornitore, diventa sempre più difficile individuare una singola area che influisca sulle prestazioni. Anche il tempo che il personale IT dell'organizzazione dedica all'assistenza dei fornitori è per molti motivi di grande preoccupazione, dal momento che viene sottratto ad altre attività più strategiche. Infine, ogni persona che ha accesso fisico al data center rappresenta un potenziale rischio per la sicurezza.

Unificare il supporto fornitori con un fornitore di fiducia è uno dei modi in cui le organizzazioni possono affrontare la resilienza operativa in tutto il data center. La collaborazione con IBM come fornitore di fiducia per il supporto unificato dei data center ha dimostrato di rispondere adeguatamente alle criticità sopra riportate. Di fatto, i clienti hanno ottenuto una riduzione del tempo medio impiegato per la risoluzione dei problemi, una riduzione del tempo dedicato all'assistenza di hardware e alla gestione dei fornitori, la prevenzione di interruzioni e una riduzione dei costi.⁵ Leggi il report Forrester [The Total Economic Impact of IBM Hybrid IT Support](#) per maggiori dettagli su una strategia di supporto consolidata con IBM e sui benefici associati.

Test di resilienza operativa

Eseguire dei controlli regolari dell'infrastruttura atti a individuare potenziali punti deboli è un altro elemento fondamentale per garantire la resilienza. Le organizzazioni devono individuare i potenziali singoli punti di vulnerabilità che potrebbero causare o prolungare le interruzioni. È opportuno programmare un'analisi dei log, dei record e delle tendenze delle macchine per isolare i problemi cronici e sviluppare piani d'azione che evitino o riducano al minimo l'impatto di interruzioni non pianificate. IBM è in grado di fornire controlli rapidi sullo stato di salute dei prodotti nel data center. Oltre a questi controlli, è possibile eseguire valutazioni più dettagliate per adattare le prestazioni a un livello ottimale o approfondire le vulnerabilità nella sicurezza.

Data l'attuale presenza di molteplici prodotti e fornitori singoli in gran parte dei data center, eseguire test di resilienza a livello di prodotto non è sufficiente. Sia che un'organizzazione abbia appena subito un grave incidente, sia che voglia essere più proattiva nel mantenere alti livelli di disponibilità, una valutazione dell'ambiente nel suo complesso può aiutare a individuare le dipendenze e i fattori che ostacolano la disponibilità e proporre le best practice per garantirla. L'IBM High Availability Center of Competency può offrire assistenza nelle valutazioni e nelle revisioni post-incidente, nonché nella condivisione di best practice e conoscenze.

Conclusioni

La resilienza operativa dipende da un'infrastruttura efficiente ed efficace. Mantenere aggiornata l'infrastruttura, ottenere visibilità sui rischi potenziali e intraprendere azioni aggressive per ridurli è fondamentale per ottenere risultati positivi. Le organizzazioni hanno bisogno di un partner fidato che comprenda le loro esigenze di business e che adotti un approccio olistico al supporto e ai servizi, con particolare attenzione alla resilienza.

Perché IBM Technology Lifecycle Services?

IBM Technology Lifecycle Services collabora con le organizzazioni per dare forma a un approccio che soddisfi le loro esigenze di resilienza operativa. IBM vanta oltre 35 anni di esperienza nella fornitura di manutenzione e supporto multivendor per circa 22.000 dispositivi e prodotti software IBM e di terze parti. Con una presenza globale in più di 130 paesi, puoi dormire sonni tranquilli sapendo che le risorse saranno disponibili quando ne avrai bisogno. Infine, come indicato nel report [IDC Marketscape 2022 Worldwide Support Vendor Assessment](#), i principali punti di forza di IBM come fornitore di assistenza globale sono la sua presenza internazionale e le funzionalità multivendor, le sue capacità di assistenza proattiva e le relazioni con i vertici aziendali, che le consentono di comprendere le esigenze di business dei propri clienti⁶.

© Copyright IBM Corporation 2022

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)

Italia
IBM Corporation
New Orchard Road
Armonk, NY 10504

Prodotto negli Stati Uniti d'America,
gennaio 2024

IBM e il logo IBM sono marchi o marchi registrati di International Business Machines Corporation, negli Stati Uniti e/o in altri Paesi. Altri nomi di prodotti e servizi potrebbero essere marchi registrati di IBM o di altre società. Un elenco aggiornato dei marchi registrati IBM è disponibile all'indirizzo ibm.com/it-it/trademark.

Le informazioni contenute nel presente documento sono aggiornate alla data della prima pubblicazione e possono essere modificate da IBM senza preavviso. Non tutte le offerte sono disponibili in ogni Paese in cui opera IBM.

LE INFORMAZIONI RIPORTATE NEL PRESENTE DOCUMENTO SONO DA CONSIDERARSI "NELLO STATO IN CUI SI TROVANO", SENZA GARANZIE, ESPLICITE O IMPLICITE, IVI INCLUSE GARANZIE DI COMMERCIALIZZABILITÀ, DI IDONEITÀ A UN PARTICOLARE SCOPO E GARANZIE O CONDIZIONI DI NON VIOLAZIONE.

I prodotti IBM sono coperti da garanzia in accordo con termini e condizioni dei contratti sulla base dei quali vengono forniti.

1 ["IBM Cloud Pak for Data enhances DataOps services to deliver business agility with cost savings and risk reduction"](#), Aliye Ozcan, maggio 2020.

2 [IDC Perspective: The Cost of Downtime in Datacenter Environments: Key Drivers and How Support Providers Can Help](#), Doc # US50240823, marzo 2023

3 Dati interni IBM

4 [X-Force Threat Intelligence Index 2023](#)

5 [The Total Economic Impact for IBM Hybrid IT Support](#), uno studio di Forrester commissionato da IBM, gennaio 2023.

6 [IDC Marketscape 2022 Worldwide Support Vendor Assessment](#), IDC, marzo 2022

