DELL Technologies

Panoramica del servizio

SERVIZI DI CYBER RECOVERY

Sviluppa la tua strategia di cyber recovery e implementa il programma di ripristino

CARATTERISTICHE PRINCIPALI

Servizi di Dell Technologies Cyber Recovery:

- Creazione dell'azienda minima vitale nel vault di Cyber Recovery, capace di ripristinare le funzioni aziendali essenziali in seguito ad attacchi informatici
- Consigli per la strategia di ripristino e i punti di integrazione con piani di risposta agli incidenti per tutta l'organizzazione
- Integrazione di una soluzione di ripristino che elabori piani per un'ampia varietà di vettori di minaccia, in linea con il framework per la sicurezza informatica del NIST
- Sviluppo e test di piani e procedure di ripristino

Sfida aziendale

Gli attacchi informatici sono diventati comuni e sono causa di downtime prolungati, interruzione delle operazioni aziendali per giorni e persino settimane e milioni di spese. Oltre alla preoccupazione legata all'esposizione di informazioni sensibili o di dati proprietari, i fatti dimostrano che sempre più frequentemente gli attacchi informatici sono ideati specificamente per la distruzione o la codifica dei dati con lo scopo di trattenerli per chiedere il riscatto. Molti dei recenti attacchi ransomware hanno danneggiato notevolmente i sistemi di produzione, i sistemi informatici ospedalieri, i sistemi bancari e i governi locali. Tali attacchi riescono ad aggirare i tradizionali controlli di sicurezza presenti al perimetro, così gli autori procedono inosservati per mesi o talvolta anche anni, con ripercussioni sulla maggior parte dei sistemi e indebolendo ulteriormente la preparazione dell'azienda per il ripristino. Oltre ai malintenzionati al di fuori dell'organizzazione, la triste realtà è che sono in crescita gli attacchi informatici che vedono coinvolto il personale interno ed è necessario che i dirigenti siano pronti a proteggere il business da qualsiasi tipo di minaccia. Questi fattori hanno spinto i dirigenti aziendali di tutti i settori a richiedere garanzie di ripristino da eventuali attacchi informatici.

Poiché gli attacchi diventano sempre più sofisticati e devastanti, le aziende sono chiamate a considerare nuovi use case per la protezione dei dati e la sicurezza informatica: "l'ultima linea di difesa" per assicurarsi di essere in grado di sopravvivere agli attacchi informatici distruttivi.

Descrizione del servizio

L'approccio più recente sottolinea l'importanza di disporre di una copia dei dati critici (ad esempio, applicazioni, dati e proprietà intellettuale essenziali) isolata dalla rete di produzione e separata dai sistemi di backup di produzione. Senza connessione di rete diretta e diversi punti di roll-back disponibili, hai la certezza di disporre della "gold copy" integra e pronta per il ripristino.

Grazie a Dell EMC PowerProtect Cyber Recovery ottieni il vault di protezione dei dati air-gapped e, in combinazione con Dell Technologies Services, acceleri l'adozione della tecnologia e dei processi, così da aumentare la sicurezza nelle tue capacità di ripristino dagli attacchi informatici. I nostri servizi sono incentrati su due aree principali: consulenza e implementazione.

La fase di consulenza mira a fornire consigli per l'integrazione e l'ottimizzazione di Cyber Recovery nell'ambiente di protezione dei dati. Tali risultati si ottengono analizzando lo stato attuale e futuro dell'azienda al fine di creare strategie su misura per la preparazione al cyber recovery, assicurando l'allineamento perfetto con le esigenze aziendali di protezione e ripristino.

Componenti chiave nella fase di consulenza, la sessione informativa e il workshop servono a raccogliere dati sulle applicazioni e comprendere quanto sono essenziali per le normali operazioni aziendali. Sulla base di queste considerazioni è possibile fornire consigli su cosa proteggere nel vault di Cyber Recovery e creare così l'azienda minima vitale, composta dalle applicazioni e dai dati critici da utilizzare innanzitutto per ricostruire le funzioni principali e per rimettere in marcia l'attività.

La fase di implementazione consiste nell'integrazione della soluzione Cyber Recovery nell'ambiente di protezione dei dati. In questa fase sfruttiamo le informazioni raccolte in fase di consulenza per adattare ulteriormente la soluzione alle esigenze specifiche. Inoltre, è possibile integrare tecnologie e funzionalità aggiuntive nell'ambiente di Cyber Recovery, ad esempio:

- Deployment dell'infrastruttura vault
- Deployment delle analisi CyberSense per esaminare i dati e identificare per tempo gli indicatori di compromissione
- Modifica dei backup di produzione per il supporto dei requisiti del vault di Cyber Recovery
- Consolidamento dell'infrastruttura di produzione aggiuntiva di Dell Technologies
- Integrazione del vault e delle funzionalità di Cyber Recovery negli ambienti mainframe
- Creazione del vault di Cyber Recovery con più piattaforme, tecnologie eterogenee, policy e applicazioni di retention
- Sviluppo di procedure operative dettagliate (runbook di ripristino) per eseguire il ripristino al fuori del vault
- Supporto per la creazione di runbook di ripristino estesi e scenari di test aggiuntivi

Riepilogo dei vantaggi

Dato il proliferare degli attacchi informatici, la domanda non è se l'organizzazione verrà colpita, ma quando. Ciascuna azienda ha aspirazioni, obiettivi e requisiti di IT esclusivi da soddisfare mediante strategie di cyber recovery e di risposta agli incidenti informatici. Gli esperti di consulenza collaborano con te per sviluppare processi e procedure in grado di proteggere e ripristinare il business in caso di attacchi informatici distruttivi.

Dell Technologies Services offre:

- Soluzione vault air-gapped di Cyber Recovery e consigli per creare l'azienda minima vitale nel vault ed essere in grado di ripristinare il business in caso di attacchi informatici.
- Supporto per raggiungere gli obiettivi di conformità con le pressioni normative sempre più stringenti, proteggendo e dimostrando le capacità di ripristino delle applicazioni principali specifiche.
- Integrazione di strategie di ripristino in linea con il framework per la sicurezza informatica del NIST nei piani di risposta agli incidenti