LOGISTICA EFFICIENTE

TDI, cybersecurity e affidabilità per la continuità operativa

Anche in Italia, il settore dei trasporti si sta evolvendo e comincia a comprendere il valore intrinseco della digitalizzazione. La sicurezza informatica diventa quindi l'elemento fondamentale per la continuità operativa delle aziende, con l'obiettivo di rilevare e neutralizzare le minacce in tempo reale.

Un attacco o un malfunzionamento dei sistemi possono bloccare interi processi, generando perdite economiche e danni reputazionali difficili da recuperare. Per questo motivo, TDI ha adottato un sistema di cybersecurity avanzato, oltre a una struttura capace di rispondere in pochi millisecondi e garantire la ripartenza immediata dell'attività dei suoi clienti grazie a tecnologie innovative e server ridondanti.

Uno degli aspetti chiave per garantire la continuità operativa è proprio l'implementazione di server ridondanti. Questi sistemi duplicano in tempo reale i dati e le operazioni, permettendo di mantenere attivo il lavoro. Grazie alla ridondanza, un server secondario può subentrare immediatamente a quello principale, assicurando una ripartenza istantanea senza perdita di dati o interruzioni nei servizi.

Il *BCP (Business Continuity Plan)* di TDI garantisce una latenza minima, ovvero una risposta in pochi millisecondi, per impedire che eventuali malfunzionamenti, possano interrompere o rallentare il normale flusso di lavoro.

"Con l'obiettivo di proporre qualità e per certificarne l'affidabilità, abbiamo recentemente effettuato una fase di test della nostra soluzione BCP (Business Continuity Plan). Implementata dal 2023, questa struttura sicura ci consente di garantire il funzionamento permanente e continuo delle tecnologie di TDI e l'accesso immediato ai dati dei clienti, nonostante la perdita parziale o totale di un sito di produzione. La sua attività si basa sulla distribuzione della produzione in due data center remoti attivi, in modo che venga effettuato uno switch over istantaneo e automatico al secondo sito, in caso di malfunzionamento del primo. Abbiamo inoltre effettuato test tecnici e volontari per disattivare la fibra che collega i due data center di TDI, che ha avuto l'effetto di creare una perdita totale di accesso ai dati sul secondo sito. Risultato? Non sono stati dimostrati effetti negativi sull'attività dei clienti! Questa operazione, effettuata al di fuori dell'ambiente produttivo, ha permesso di corroborare la fattibilità, la reattività e l'efficienza del sistema BCP. Infatti, di fronte all'interruzione della trasmissione, l'attività ha immediatamente ripreso, consentendo la manutenzione e il funzionamento delle nostre soluzioni, senza alcuna perdita di dati per i nostri clienti". Commenta **Matteo Moretto, Country Manager Italia di TDI.**

I vantaggi del BCP *(Business Continuity Plan)* di TDI

Il BCP garantisce il mantenimento dell'attività operativa in caso di perdita parziale o totale di un sito di produzione aziendale. Più in particolare, la qualità del servizio viene mantenuta grazie all'infrastruttura completamente ridondante su due data center e consente di:

- Ridondare il data center originale per garantire uno switch over sicuro, istantaneo e automatico ad un secondo sito in caso di malfunzionamento
- Garantire l'accesso ai servizi senza interruzioni grazie alla replica degli IP pubblici in caso di perdita del collegamento internet principale
- Ottenere una configurazione attivo/attivo con la produzione distribuita in modo equilibrato e intelligente tra i due data center
- Mantenere un'infrastruttura iperconvergente, efficiente e sicura

La sicurezza firmata TDI

L'obiettivo principale del **BCP** di TDI, è garantire la continuità dell'attività per i propri clienti. Questa è la vera garanzia di qualità e affidabilità, in grado di assicurare la disponibilità del servizio al 100% con un'elevata sicurezza dei dati.

Relativamente alla **cybersecurity**, per difendersi è importante sapere che la maggior parte degli attacchi informatici prende di mira gli utenti e non direttamente i sistemi. TDI ha quindi implementato una serie di misure integrate:

- **SentinelOne** è installato su tutte le postazioni di lavoro. Questa soluzione avanzata di rilevamento raccoglie i log e li invia a un **SOC (Security Operations Center)** per l'analisi.
- TDI, grazie al partner **Almond** specialista in cybersecurity, verifica e gestisce 24/7 la sicurezza informatica. In caso di comportamenti sospetti, un team altamente specializzato analizza gli allarmi in tempo reale e interviene immediatamente, contattando se necessario la sede di TDI.
- TDI esegue audit annuali con **Advens** per garantire la sicurezza dei siti esposti, ottenendo le più aggiornate certificazioni di sicurezza.

"Grazie all'uso di server ridondanti e tecnologie all'avanguardia, oltre alla combinazione tra SOC e SentinelOne che rappresenta un vero investimento in sicurezza garantendo un monitoraggio preciso e proattivo delle postazioni di lavoro e dei server, con TDI è possibile ridurre al minimo i rischi e assicurarsi un ambiente di lavoro digitale più che affidabile. La protezione dei dati e la resilienza informatica non sono più un optional, ma pilastri fondamentali per il successo di ogni impresa che vuole avvicinarsi alla digitalizzazione dei trasporti e migliorare le sue performance da subito". Conclude Matteo Moretto.

https://www.tdi-group.com/it/

Sponsor TDI