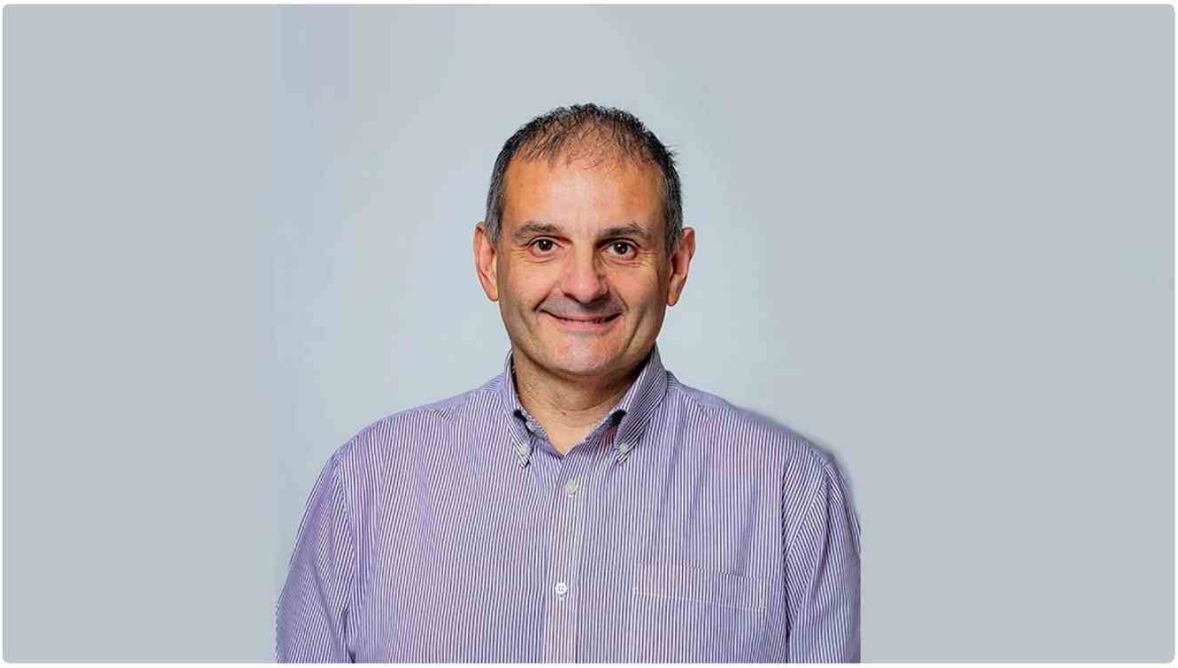
Il parere di Achab

Risponde Claudio Panerai, Chief Portfolio Officer di Achab



Perché è importante il backup e con quale cadenza bisognerebbe aggiornare le copie di sicurezza?

Il backup è un'attività fondamentale, anche per la piccola azienda, perché i dati sono l'unico vero bene delle imprese. Tant'è vero che quando in tutte le aziende, a maggiore ragione le PMI, si verifica un attacco ransomware, si apre una crisi profonda. Alcune restano molto tempo in down time, alcune perdono molti soldi, altre addirittura falliscono. È lì che si capisce la criticità e l'importanza di un dato disponibile. Il backup serve a proteggere il dato, perché senza il dato non si fa più nulla. Il backup è solo una parte del lavoro, perché l'altra vera sfida è occuparsi del restore: siamo capaci di tornare indietro, e quanto tempo ci vuole?

Prima di dire ogni quando va fatto un backup bisognerebbe rispondere a un'altra domanda: quale tipo di dato tratto (personale, di fatturazione, listini, etc) e quanto posso vivere senza quel dato? Tecnicamente i parametri da valutare sono due: RPO (Recovery Point Objective) e RTO (Recovery Time Objective). In altre parole, quanti dati puoi permetterti di perdere, e quanto puoi stare senza lavorare. Il primo parametro determina la frequenza del backup. Se un cliente ha fatto il backup 24 ore fa e improvvisamente perde i dati lo reputa accettabile? O può permettersi di perdere solo i dati delle ultime 8 ore, o delle ultime 2 ore? Il secondo parametro determina che tipo di backup (quindi di business continuity) serve, ossia quanto tempo un'azienda può restare senza lavorare. In altre parole: dal momento in cui si verifica un blocco, per quando tempo l'azienda può restare ferma?

Come valutate l'attenzione delle PMI al problema della protezione costante dei dati?

Negli ultimi tempi qualcosa si sta muovendo, anche se a rilento. Sia per la pressione di chi eroga servizi IT, sia perché i media parlano sempre di più degli attacchi alla cyber security. Fino a poco tempo fa la risposta standard delle aziende era: "tano a noi non succede". Oggi c'è un barlume di interesse, però siamo ancora lontani dalla consapevolezza che possa succedere realmente a tutti. E che la perdita dei dati non è dovuta necessariamente a un ransowmare. Può essere dovuta alla rottura di un disco.

Quali sono le soluzioni che proponete?

Sono tre. Datto è la nostra soluzione di disaster recovery e business continuity. Include anche il backup, ed è indicata per i sistemi e servizi veramente critici. Ha tanti punti di forza, fra cui la certezza matematica che i backup funzionano o non funzionano, perché effettua un test di ripartenza automatico. Consente di ripartire istantaneamente in ogni circostanza, perché la soluzione all inclusive include hardware e virtualizzatore. Tutto il sistema è replicato nel cloud di Datto. Il cliente ha a disposizione un data center as a Service a cui collegarsi.

Ci sono poi una serie di sistemi e servizi che si usano tutti i giorni, per i quali basta un eccellente backup. In questi casi consigliamo Altaro, un prodotto recentemente introdotto. È un backup di ambienti virtuali che ha dalla sua soprattutto la facilità d'uso e la grande capacità di compressione dei dati. Nonostante il volume di dati sia in costante aumento, lo storage occupato non è mai tantissimo. Inoltre, a chi eroga servizi IT, offre una console di gestione molto semplice che permette di tenere sotto controllo tutti i backup di tutti i clienti.

Poi abbiamo un sistema entry level che si chiama Backup Assist, indirizzato alle piccole e medie imprese, dedicato a Windows. È il classico buono strumento di backup che abbiamo a listino da moltissimo tempo. Il suo punto di forza è che dispone di molti pluging, quindi a seconda dell'esigenza del momento si possono aggiungere nuove funzioni.