

BLOCCO DEI SISTEMI ED INTERRUZIONE DEL BUSINESS. ECCO COME LIMITARE I DANNI

Oggi, grazie alle varie possibilità di connessione e alla quantità crescente di dispositivi e tecnologie, i dipendenti delle aziende si aspettano di poter accedere sempre, facilmente e da ogni luogo ai dati e alle applicazioni su cui stanno lavorando e questo rende fondamentale garantire la continuità del servizio

di Claudio Panerai

CTO Achab sulla nuova tecnologia Datto e il problema della business continuity

“DATTO”: LA BUSINESS CONTINUITY SEMPLICE E PROFESSIONALE PER LE AZIENDE

Lo scenario lavorativo attuale è profondamente cambiato rispetto ad anni fa, quando la tecnologia non era ancora una presenza fissa in ufficio. Oggi, grazie alle varie possibilità di connessione e alla quantità crescente di dispositivi e tecnologie, i dipendenti delle aziende di ogni dimensione, tipo e settore, si aspettano di poter accedere sempre, facilmente e da ogni luogo ai dati e alle applicazioni su cui stanno lavorando senza nessuna interruzione, sia con il PC sia in mobilità tramite tablet e smartphone. Tutti i reparti di un'azienda, dal customer care al reparto vendite, dall'ufficio acquisti al marketing, devono poter accedere immediatamente e in ogni momento ai dati aziendali per portare avanti l'attività e vendere servizi e prodotti.

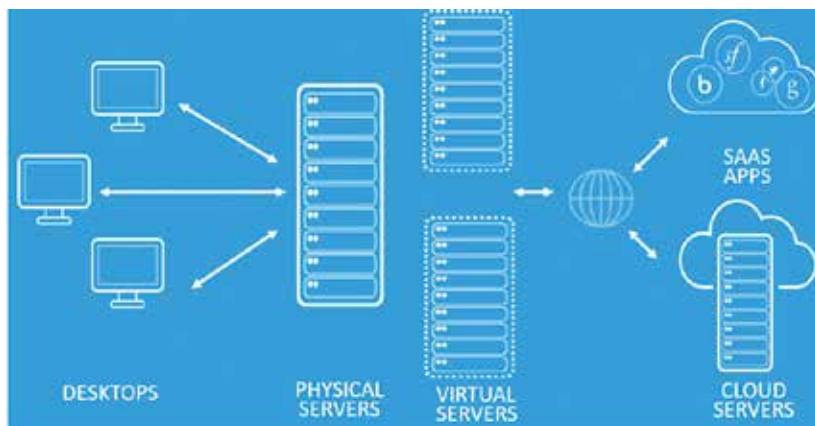
Il cambiamento delle esigenze aziendali si rispecchia anche nella complessità strutturale dei sistemi informatici. Un

tempo in azienda era presente solo un server e qualche desktop, oggi invece la situazione è completamente trasformata: si trovano server fisici, desktop, server virtuali, on premise, server dei data center, cloud server e applicazioni SaaS.

In questo scenario anche il lavoro del reparto IT è profondamente mutato diventando critico per tutte le tipologie

di aziende, dagli studi professionali alle aziende più grandi, che devono avvalersi di professionisti in grado di mantenere e assicurare il perfetto funzionamento di tutto il sistema informatico dell'azienda.

Se per qualche motivo, per esempio un blocco dei sistemi, non si riescono a controllare le mail per dodici secondi o il sistema gestionale si ferma non effettuando la stampa in pdf di quella im-



“

Per i business attuali, sempre connessi e in cui la velocità è tutto, non sono ammissibili down delle applicazioni e irraggiungibilità dei dati. Non poter lavorare, non poter rispondere alle richieste via mail, non poter accedere ai sistemi equivale ad avere la porta dell'azienda chiusa e non far entrare i clienti

”

”

portantissima fattura urgente, ecco che il dipendente si preoccupa e va in allerta. Viene contattato immediatamente il reparto IT, o il fornitore IT, per capire che cosa è successo, per risolvere e sbloccare la situazione e, auspicabilmente, cercare di evitare che possa accadere nuovamente in futuro. Ma perché tutta questa agitazione per un blocco anche se minimo? La ragione è semplice: per i business attuali, sempre connessi e in cui la velocità è tutto, non sono ammissibili down delle applicazioni e irraggiungibilità dei dati. Non poter lavorare, non poter rispondere alle richieste via mail, non poter accedere ai sistemi equivale ad avere la porta dell'azienda chiusa e non far entrare i clienti.

Questa situazione ci porta però a fare alcune riflessioni su quello che andava bene anni fa e che forse adesso è diventato obsoleto e non più sufficiente: il backup. La richiesta da parte delle aziende di dati e applicazioni sempre disponibili e accessibili spinge verso la necessità di soluzioni che vanno ben oltre il backup: ovvero soluzioni che possano assicurare la continuità dell'attività, senza interruzioni in qualsiasi condizione.

Per fare un esempio concreto, se i dipendenti di un'azienda vanno in agitazione perché non possono controllare la posta elettronica per qualche minuto a causa di un blocco del server, in caso di problemi, forse un backup tradizionale non riesce a far ripartire l'attività velocemente. Un'azienda deve pertanto chiedersi: quanto tempo posso permettermi di stare ferma? Quanto tempo mi serve per ripartire e per essere nuovamente operativa? Quanti dati posso permettermi di perdere?

Le aziende hanno quindi bisogno di approcciare un nuovo paradigma, ovvero iniziare a ragionare non più solo sul backup, ma valutare la necessità di inserire all'interno della loro infrastruttura IT soluzioni di **disaster recovery & business continuity**.

Quando si parla di disaster recovery & business continuity è bene precisare che non significa trovare soluzioni in grado di far fronte solo a **disastri dovuti a calamità naturali**, come alluvioni, trombe



d'aria, incendi e terremoti, situazioni forse sentite poco vicine o non percepite come una reale minaccia. In realtà, per un'azienda **basta molto meno** per trovarsi in mezzo a un vero e proprio **disastro!** Pensiamo a un dipendente maldestro o distratto che cancella uno o più ordini. Oppure un collaboratore che vuole recare un **danno intenzionale all'azienda**, oppure ancora un dipendente che lascia l'azienda e cancella dati e informazioni importanti su cui stava lavorando. Ma anche **virus e malware** che possono attaccare i sistemi dell'a-

zienda rappresentano una reale minaccia per il business, come le recenti infezioni trasmesse tramite finte bollette che includevano un link per visualizzare fantomatici dettagli dei costi: una volta cliccato sul link tutti i dati venivano infettati e criptati e solo il pagamento di un riscatto poteva restituire i file originali.

Tutti questi scenari, che possono facilmente capitare, sono in grado di arrecare un danno enorme all'attività dell'azienda, sia in termini di immagine sia

monetari.

Ma quante sono le aziende che sono adeguatamente protette e in grado di far fronte a un blocco dei sistemi grazie a soluzioni di disaster recovery & business continuity? Secondo una ricerca di Symantec il 50% delle piccole e medie imprese americane non ha un piano di business continuity, possiamo quindi pensare che la percentuale italiana si aggiri su numeri simili se non decisamente più alti.

Se i danni per calamità naturali, come alluvioni e terremoti, non sono fortunatamente così ricorrenti, sono sicuramente più frequenti i **danni causati da errori umani, i problemi tecnici di hardware e software** o le infezioni da virus. Per salvaguardare la propria attività, è importante che le aziende prendano coscienza di quali rischi corrono se non adeguatamente protette per far fronte a un blocco dei sistemi e quali sono i costi di inattività del proprio business. Prendiamo ad esempio una piccola media impresa italiana di 10 dipendenti con un milione di euro di fatturato che sta riscontrando un blocco dei sistemi o altri problemi che possono causare interruzione temporanea dell'operatività. Durante il **periodo di downtime** il personale non può accedere ai propri sistemi, a file, documenti, email e applicazioni: in questo frangente temporale non sta lavorando e quindi per l'azienda il **lavoratore è improduttivo**, ma rappresenta un costo perché viene comunque pagato. Nello stesso momento l'azienda, oltre al fermo dei dipendenti, potrebbe subire ingenti perdite monetarie causate dalla mancata vendita di prodotti o servizi e può incorrere anche in un pesante **danno di immagine** poiché l'azienda è irraggiungibile, i dipendenti non possono rispondere nei tempi a richieste di supporto o di informazioni dei consumatori arrivate via mail perché il mail server non è disponibile e ancora perché si mancano deadline fissate con fornitori o clienti.

Se vogliamo provare a quantificare il danno monetario in una situazione del genere, per un'azienda di questo tipo magari con circa 250 GB di dati critici, ipotizzando che dopo un blocco riesca a ripartire in 4 ore e 48 minuti, avrebbe

dei costi pari a circa 3.700 euro. A questi costi vanno poi aggiunte tutte le spese vive legate alla ripartenza, i costi per eventuali nuovi software e hardware da acquistare e le varie consulenze esterne per ripartire. (Si possono fare altre stime con il calcolatore automatico www.achab.it/RTOfcalculator).

Le aziende devono quindi adottare **misure di protezione in grado di assicurare il minor danno possibile** al business in caso di blocco dei sistemi, devono scegliere soluzioni di disaster recovery & business continuity che consentano di ripartire, limitando i danni e i costi legati all'inattività.

Per proteggersi è necessario adottare una soluzione di protezione locale che permetta all'azienda di ripartire in poco tempo: per esempio una soluzione che effettua in modo costante e frequente immagini complete del sistema operativo, delle varie configurazioni dei sistemi, delle applicazioni e dei dati. L'azienda deve procurarsi una soluzione che con un solo click possa far ripartire l'intero sistema all'interno della rete locale. Ma questo non basta per assicurare una protezione completa dell'attività dell'azienda. Poiché i disastri sono imprevedibili, è necessario essere preparati anche in caso di indisponibilità totale delle reti, delle sedi fisiche e dei server e quindi anche dei backup effettuati in locale. Ogni azienda per essere protetta e limitare i danni e costi in caso di blocco dovrebbe adottare sistemi di disaster recovery & business continuity che abbiano repliche dei **propri sistemi offsite in cloud**, in modo da avere un'alternativa se il backup locale non è raggiungibile, è corrotto o è inutilizzabile. Anche per la **replica offsite**, non sono solo i dati a dover essere salvati e replicati, è necessario che l'intero sistema informativo, e quindi tutto il server, il sistema operativo e le applicazioni, venga replicato nel cloud, questo consentirà all'azienda di ripartire velocemente. Pertanto, un sistema di disaster recovery & business continuity per essere considerato tale deve includere sia una protezione in locale sia in cloud offsite, che possa quindi garantire in caso di blocco dei si-

stemi o di qualsiasi tipo di disastro una ripartenza istantanea con un solo click e di eliminare, o comunque limitare il più possibile il downtime. Le aziende hanno necessità di dotarsi di una soluzione che permetta di ripartire senza dover contare troppi danni e perdite, minimizzando RPO e di RTO. Con RPO si intende **Recovery Point Objective**, ovvero il parametro con cui si misura la quantità di dati che un'impresa può perdere a causa di un guasto ai sistemi informatici e con RTO il **Recovery Time Objective**, ovvero il parametro che misura la quantità di tempo che un'azienda può permettersi di stare ferma in caso di guasto.

Sono numerose le soluzioni di backup, disaster recovery e business continuity presenti sul mercato IT. Esistono in commercio degli ottimi sistemi che però funzionano solo su macchine virtuali e solo su determinati sistemi operativi. La vera difficoltà è trovare una soluzione di business continuity multipiattaforma (Windows, Mac e Linux) e che sia in grado di funzionare in

m o d o



eccellente e indipendentemente da dove siano ubicati i sistemi da proteggere: fisici, virtuali, on premise, all'interno di un data center o presso un fornitore esterno consentendo di ripartire immediatamente. Quello che mancava fino ad oggi nel mercato IT è un sistema standardizzato di disaster recovery & business continuity. Infatti, per un fornitore IT non

“

un sistema di disaster recovery & business continuity per essere considerato tale deve includere sia una protezione in locale sia in cloud offsite, che possa quindi garantire in caso di blocco dei sistemi o di qualsiasi tipo di disastro una ripartenza istantanea con un solo click e di eliminare, o comunque limitare il più possibile il downtime”

”

è complicato creare un sistema di disaster recovery ad hoc con un budget di 50.000 euro o magari anche di 100.000 euro, ma non tutte le aziende dispongono di questi budget. Ecco quindi che la difficoltà per il consulente IT che fornisce servizi a un'impresa è industrializzare questa piattaforma, in primo luogo per una questione legata ai costi, e poi perché diventa critico creare dieci, venti o anche cinquanta architetture di disaster recovery, personalizzate per i vari clienti, da gestire e da mantenere manualmente. Se però sul mercato si affaccia una piattaforma standard che permette di ripartire istantaneamente, già completamente industrializzata, che protegge i dati e applicazioni sia in locale sia in cloud, che funziona su qualsiasi sistema operativo e con qualsiasi dimensione della rete da proteggere, ecco che il consulente di servizi IT può fare un salto in avanti verso la

Italia di soluzioni IT innovative.

ARCHITETTURA DELLA BUSINESS CONTINUITY DI DATTO

In caso di blocco, crash dei sistemi o calamità naturali, l'azienda sarà immediatamente operativa, il fermo dei sistemi e dell'attività sarà di pochi istanti. In questo modo il downtime sarà minimo, così come i costi e le perdite legate all'inattività dei dipendenti. Il produttore stima tempi di ripartenza di circa 6 secondi, ma anche se fossero minuti sarebbe, comunque un'ottima tempistica per recuperare il lavoro e ripartire.

Oltre alla protezione di dati e applicazioni, con la funzione Backup Insights di Datto è possibile ricercare file e dati modificati tra due backup, si possono quindi identificare cartelle cancellate o i file infettati da un virus e recuperare così i dati necessari in poco tempo. Tutti i dati che transitano nel sistema Datto, anche in cloud, sono inoltre protetti dalla crittografia AES 256 che garantisce una sicurezza completa di tutto il sistema senza doversi preoccupare della divulgazione di informazioni sensibili. Il sistema permette anche di crittografare i dati localmente secondo le policy proprie di ogni azienda.

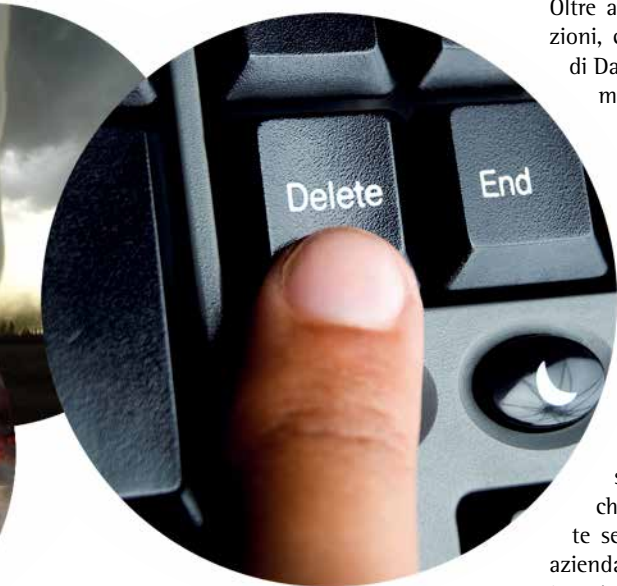
Le aziende però non sono tutte uguali e non hanno le stesse necessità e richieste, le esigenze del piccolo studio professionale differiscono completamente da quelle di una grande multinazionale con più sedi. Una delle caratteristiche chiave di tutta l'offerta Datto è la possibilità di adottare il dispositivo più adatto alle esigenze di ciascuna azienda, esistono configurazioni che soddisfano le richieste in termini di dimensioni, esigenze di protezione, numero di postazioni da

proteggere e struttura del sistema informatico. La famiglia Datto è infatti composta da una gamma completa di soluzioni per rispondere alle esigenze di ogni azienda.

Per le aziende con esigenze professionali è dedicata la soluzione Datto SIRIS 2 che assicura il minor downtime a seguito di un disastro o di un crash, garantendo la ripartenza immediata e, con un solo dispositivo, si possono proteggere fino a 60TB di dati e applicazioni. SIRIS 2, la fascia professionale di Datto, include anche una versione del software di sync&share ownCloud, grazie al quale il service provider è in grado di costruire per sé stesso e per i suoi clienti una sorta di "Dropbox privato". Potrà infatti costruire un sistema di condivisione di documenti all'interno e all'esterno dell'azienda senza dover ricorrere a soluzioni cloud, ma gestendo tutto in casa.

ownCloud on SIRIS archivia file e dati direttamente sul dispositivo all'interno dell'infrastruttura locale senza necessità di affidarsi a un servizio cloud pubblico. Questa soluzione è molto sicura poiché è possibile definire in autonomia le restrizioni per utente secondo le policy aziendali specifiche di ogni azienda. Per garantire protezione e accessibilità, tutti i dati che passano attraverso ownCloud sono replicati anche nel cloud di Datto. Per le piccole e medie imprese la soluzione più adatta è Datto ALTO XL, un sistema scalabile e facile da usare che assicura protezione contro il downtime in caso di perdita di dati o di disastro, un singolo dispositivo può proteggere fino a 24 TB di dati e applicazioni.

Per le micro-imprese o studi professionali c'è Datto ALTO 2, una soluzione di disaster recovery & business continuity entry level, ma completa, ad un prezzo aggressivo.



semplice moltiplicazione dell'offerta di disaster recovery & business continuity per tutti i suoi clienti: lato service provider questo si traduce in costi più sostenibili, certezza di funzionamento e un processo industrializzato per l'azienda che decide di adottare un sistema del genere: un sistema come Datto, appena introdotto in Italia da Achab, distributore italiano specializzato nello scouting e nell'introduzione in

Datto NAS è la soluzione di storage che si connette al cloud di Datto portando così le performance di un NAS a un livello superiore grazie alle “fotografie” e alla sincronizzazione nel cloud. Tutti i

Datto è una soluzione di backup, recovery e business continuity che permette alle aziende di essere immediatamente operative anche in caso di perdita totale di dati, crash del sistema o di disastro. Datto protegge dati, server e applicazioni localmente replicandoli in automatico nel cloud. Il server, e quindi tutta l'attività dell'azienda, è pronto a ripartire in pochi istanti, anche in caso di inaccessibilità fisica dei sistemi, e le perdite dovute al downtime saranno ridotte al minimo.

All'interno di ogni rete che si desidera proteggere è necessario installare un device Datto, uno “scatolotto” di dimensioni contenute e non invasivo, e ogni macchina deve avere installato il software fornito in dotazione con il device Datto e salvare i backup sul dispositivo stesso. Ogni backup è un'immagine completa e avviabile del sistema.

Per una sicurezza maggiore i sistemi protetti sono replicati automaticamente all'interno del cloud di Datto, o all'interno del cloud privato, in questo modo una copia del sistema e dei dati si trova al di fuori della rete, e sarà disponibile in caso di inaccessibilità alla copia presente sulla rete locale.

Punto di forza della soluzione Datto è la virtualizzazione istantanea in locale o da remoto. In caso di crash di un server, tramite il dispositivo Datto è possibile avviare in pochi istanti e con un solo click un server uguale all'originale. In questo modo l'azienda potrà riprendere immediatamente la propria attività. Nel caso in cui tutta la rete fosse inutilizzabile e anche il device Datto risultasse irraggiungibile perché magari distrutto o danneggiato, è possibile riattivare i propri server direttamente dal cloud di Datto.



dati che vengono immagazzinati all'interno del dispositivo di storage Datto NAS sono sincronizzati automaticamente con il cloud di Datto. I file memorizzati su Datto NAS saranno quindi sempre accessibili, anche in caso di disastro o di irraggiungibilità del dispositivo.

NODE permette di implementare la tecnologia Datto all'interno del cloud privato dell'azienda o del fornitore di servizi IT, permette quindi di salvaguardare l'investimento se hai un data center di proprietà.

Le soluzioni di business continuity Datto possono essere acquistate anche come dispositivi virtuali mantenendo tutte le caratteristiche e i vantaggi propri del dispositivo fisico, come replica nel cloud e virtualizzazione istantanea del sistema per una ripartenza immediata in locale o da remoto.

Oltre alla tecnologia Datto che assicura una protezione completa, le aziende che decidono di adottare questa soluzione sapranno a priori quanto andranno a spendere, senza avere costi variabili o nascosti. Lo storage nel cloud è infatti illimitato e i costi sono legati al tempo per cui si vuole lasciare i dati disponibili off site (1, 3 o 7 anni) e non allo spazio reale occupato. Questo consente di non dover fare conti o stime sullo spazio cloud da acquistare e i costi saranno

certi fin dall'inizio.

I vantaggi offerti dalla soluzione sono numerosi anche per i fornitori di servizi IT che decidono di avvalersi di un sistema come Datto per gestire e proteggere le reti dei clienti. Una volta installato il dispositivo Datto all'interno della rete clienti, il service provider ha accesso a una console online in the cloud che permette di tenere sotto controllo, monitorare e gestire da remoto tutti i dispositivi installati presso le reti dei clienti.

La gestione dell'infrastruttura di disaster recovery & business continuity Datto avviene tramite un unico pannello centralizzato che mostra in modo semplice, chiaro ed immediato lo stato di tutti i sistemi protetti, delle repliche effettuate nel cloud e tutte le informazioni necessarie e utili per tenere sotto controllo la protezione dell'azienda. All'occorrenza, il fornitore di servizi IT può accedere a ogni singolo dispositivo locale senza dover modificare l'architettura delle reti dei clienti e senza doversi spostare dalla propria postazione.

Datto è una soluzione completa, affidabile pronta all'uso di backup, recovery & business continuity che permette di essere immediatamente operativi anche in caso di perdita totale dei dati, crash del sistema o di disastro. ♦

