White Paper

Proteggere i dati aziendali con il backup

L'IMPORTANZA DEI DATI 2

I RISCHI PER I DATI 2

QUANTO SI PUÒ STARE SENZA LAVORARE? 3

LE SOLUZIONI POSSIBILI 4

Backup di file 4

Backup per immagini 4

Sistemi di Business Continuity 5

Backup con replica off-site 5

CONCLUSIONI 6

L'IMPORTANZA DEI DATI

Lo scenario lavorativo attuale è profondamente cambiato rispetto a tanti anni fa, quando la tecnologia non era ancora una presenza fissa in ufficio. Un tempo era sufficiente un solo PC per tutta l'azienda. Ordini, richieste di informazioni, corrispondenza, tutto avveniva senza l'utilizzo di strumentazione tecnologica.

Il cuore centrale delle aziende non era il PC o il notebook o il server, e per poter lavorare un dipendente aveva bisogno solo di una scrivania e di un telefono. **In uno scenario del genere, l'azienda poteva sopravvivere tranquillamente in caso di blocco temporaneo del sistema informatico**.

Oggi, grazie alle numerose possibilità di connessione e alla quantità crescente di dispositivi, strumenti e tecnologie, **i dipendenti** delle aziende di ogni dimensione, tipo e settore, **si aspettano di poter accedere facilmente**, da ogni luogo (anche e soprattutto da fuori ufficio), **ai dati e alle applicazioni** su cui stanno lavorando senza nessuna interruzione.

Tutti i reparti di un'azienda devono poter accedere immediatamente e in ogni momento ai dati aziendali per portare avanti l'attività e vendere servizi e prodotti.
I dati sono quindi cruciali per ogni business, compreso il tuo, **ed è necessario proteggerli facendone il backup**.

Detto in parole povere e semplificando**: l'attività di backup consiste nel fare una copia dei dati e riporla in un luogo sicuro**, così da poter ripristinare i file salvati qualora questi venissero danneggiati o cancellati.

I RISCHI PER I DATI

Ma quali sono davvero i rischi per i dati? Quali sono le situazioni che possono davvero portare alla loro perdita?

Se non ti è mai successo di perdere i dati puoi pensare che l'assillo di proteggerli possa essere una inutile fissazione, eppure ogni anno ci sono milioni (sì milioni) di incidenti di vario tipo che causano la perdita di dati aziendali, con danni più o meno elevati legati alla mancata produttività e all'impossibilità di proseguire l'attività lavorativa.

Sicuramente ci sono catastrofi naturali, come terremoti, alluvioni e altri disastri naturali.

Tuttavia, nella maggior parte dei casi, le perdite di dati sono dovute a cause ben più banali e purtroppo anche molto frequenti.

- **Guasti hardware**: i dati sono sempre memorizzati sui dischi dei server o dei computer. Anche se talvolta sembra che i componenti possano durare all'infinito, in realtà hanno tutti un periodo di funzionamento dichiarato ufficialmente dalla casa produttrice. Questo vuol dire che ogni elemento hardware, quindi anche un disco di un computer, prima o poi è soggetto a rottura, e se si rompe un disco…come si accede ai dati che vi erano memorizzati sopra?

- **Problemi software**: sul lavoro si utilizzano quotidianamente diverse applicazioni. Cosa succede se una di queste all'improvviso si chiude sganciando un messaggio di errore e corrompendo il file su cui stavi lavorando, rendendolo inaccessibile? I software sono per definizione imperfetti, presentano bachi e problemi, ma non solo: questi si trovano ad agire all'interno di un altro ambiente, il sistema operativo, non esente da difetti. Ritrovarsi con un file danneggiato e dover recuperare ore, se non giorni, di lavoro e informazioni raccolte non è di certo un bello scenario, non trovi?
- **Cancellazione accidentale**: quante volte ti è capitato di cancellare un file pensando "tanto non mi servirà più", salvo accorgerti due giorni dopo che ne avresti ancora avuto bisogno? Oppure ancora, è mai successo a te o un collega di cancellare per errore un file, una cartella, una fattura o un ordine? Per quanta attenzione si possa porre durante il lavoro al PC, l'essere umano tende a distrarsi, talvolta ad agire sovrappensiero o con la mente poco lucida a causa del troppo lavoro, questo porta a errori a cui è difficile porre rimedio... a meno che tu non abbia un backup dei file!
- **Virus e ransomware**: i dati sono diventati il bene più prezioso per un'azienda, i cyber criminali lo sanno bene e mettono a punto virus in grado di cancellarli o di bloccarli completamente rendendoli indecifrabili.

E l'elenco potrebbe andare avanti ancora a lungo.

Supponiamo (Dio ce ne scampi) che succeda un incidente ai dati aziendali che impedisca a te e ai tuoi colleghi di lavorare.

Quanto tempo può stare la tua azienda senza produrre nulla, erogare alcun servizio e fatturare alcunché prima di subire un danno economico serio?

QUANTO SI PUÒ STARE SENZA LAVORARE?

A fronte di un'interruzione del lavoro o della produzione a causa di un fermo dei sistemi informatici o di perdita di dati, **sono due le domande che puoi porti**.

- Quanto tempo ci mette la tua azienda a ripristinare i dati e a tornare operativa?
- Quando il tuo business è ripartito, da quale punto riparte? Quindi quanti sono i dati che la tua azienda ha perso?

In realtà sono domande a cui è bene avere una risposta ancora prima che si verifichino i problemi. E un colloquio con un buon consulente dovrebbe aiutarti a quantificare i danni che la tua azienda subirebbe in caso di fermo dei sistemi.

In base a queste informazioni è poi possibile valutare quale soluzione è adatta a proteggere i tuoi dati.

In genere, quando si parla di backup, si menzionano spesso due acronimi che è possibile collegare direttamente alle domande riportate poco più alto in questo documento: **RPO e RTO**.

RPO è l'acronimo di Recovery Point Objective ed è l'intervallo di tempo che passa tra il verificarsi di un disastro e a quando risale l'ultimo backup utilizzabile.

Supponiamo che tu faccia il salvataggio a mezzanotte. Se il disastro si verifica alle 10 di mattina, il valore dell'RPO in questo caso è il tempo che intercorre tra la mezzanotte e le 10 di mattina.

L'**RTO, o Recovery Time Objective**, invece, indica il tempo necessario a far ripartire il sistema dopo un incidente. Quindi indica quanto a lungo un'azienda deve rimanere "ferma" in caso di incidente IT.

RTO e RPO sono entrambi parametri vitali per misurare quanto costa un incidente IT o la bontà di un sistema di backup. Minori sono questi due valori e minore è il fermo che il business subisce sia in termini di tempo che ci mette a ripartire sia in termini di quanti dati sono stati persi dopo l'incidente.

Se il tuo business poggia in maniera considerevole sui dati, avrai bisogno di soluzioni che ti permettano di ripristinare i dati in fretta e che facciano dei salvataggi abbastanza frequenti e che quindi ti garantiscano RPO e RTO molto bassi. Viceversa, se la tua azienda utilizza saltuariamente i sistemi informatici, avrai bisogno di una soluzione di backup meno performante nel ripristino e che effettui dei salvataggi meno spesso.

In ogni caso una cosa è certa: **se nella tua azienda c'è almeno un PC, un server o un device su cui vengono salvati dei dati, al giorno d'oggi non puoi fare a meno di una soluzione di backup**.

LE SOLUZIONI POSSIBILI

Naturalmente esistono centinaia di soluzioni di backup e affidarsi a una società che eroga servizi IT è la scelta più saggia per farsi consigliare il sistema adatto alla propria azienda.

Si fa presto a dire backup, infatti, ma nella scelta del backup adatto alla propria azienda concorrono tanti fattori, legati al tipo di infrastruttura, alla quantità di dati, al dove si trovano i dati e all'importanza che rivestono i vari tipi di dati.

Tenendo in considerazione che **ogni azienda ha esigenze differenti**, è impossibile consigliarti la formula magica per proteggerli in modo efficace e al giusto prezzo. A grandi linee però possiamo fare un elenco delle tipologie di backup più diffuse.

Backup di file

È la tipologia di backup "classica". Il suo scopo è quello **di salvare file e cartelle per poterle ripristinare in caso di problemi**. Questo tipo di backup, poiché semplice, immediato e utilizzabile ovunque si trovino i PC, è particolarmente utile per chi conserva informazioni e dati utili al lavoro all'interno di file e cartelle. Se però hai intenzioni di proteggere anche i dati che passano dalle applicazioni o i database con i quali lavori, questo tipo di backup non può aiutarti.

Backup per immagini

Un backup per immagini **si occupa di fare una "fotografia" dei sistemi in un dato momento e di salvarla altrove**. In questa fotografia vengono conservati tutti i dati, il sistema operativo e le applicazioni. Quindi in caso di problemi seri che portano a un crash completo dei sistemi, è possibile ripristinare in qualche ora l'intera immagine del sistema che è stata salvata in precedenza.

Questo tipo di soluzione ti permette di mettere al sicuro tutti i tuoi dati, tenendo conto però anche della frequenza con cui vengono salvate le immagini potresti ritrovarti a perdere il lavoro svolto tra l'ultimo backup e il momento in cui si è verificato il disastro (ricordi l'RPO?).

L'altro aspetto da considerare quando si sceglie una soluzione di questo tipo è che per salvare delle immagini **avrai bisogno di molto più spazio a disposizione** rispetto al backup di file e cartelle. Quindi se questi backup vengono salvati su un server, ad esempio, dovrai verificare la capienza del disco di quest'ultimo ed eventualmente espanderne la memoria.

Sistemi di Business Continuity

Si tratta della forma "più evoluta" di backup. **Un sistema di Business Continuity in genere è in grado di garantire RPO e RTO molto bassi** e di ridurre al minimo l'impatto di un problema IT sul tuo lavoro.

Il termine stesso "Business Continuity" rende chiaro l'obiettivo di questi sistemi: **permettere al tuo business di essere operativo, sempre**.

Ma come fa un sistema di Business Continuity a mantenere RPO e RTO così bassi?

- **Di solito utilizza un sistema di backup particolare**: l'intero sistema viene salvato una sola volta, in seguito vengono salvate solo le modifiche rispetto all'immagine precedente. Questo consente di alleggerire le operazioni di salvataggio, che quindi può avvenire con maggiore frequenza, mantenendo un'immagine del sistema sempre aggiornata.
- Oltre a fare una copia dei sistemi in locale, quindi su un dispositivo "fisico", **questi sistemi eseguono anche una copia nel cloud**. In questo modo anche in caso di incidenti gravi che possono coinvolgere anche la copia locale dei dati, hanno comunque un'immagine dei sistemi salvata altrove.
- Questi sistemi in genere **permettono di virtualizzare un'immagine salvata in precedenza e di farla partire su qualunque macchina in poco tempo**. Quindi se il tuo PC o il server diventassero inutilizzabili per qualsiasi motivo, sarebbe possibile prendere un'altra macchina e avviare una copia del sistema salvato. In questo modo potresti continuare a lavorare senza dover attendere i lunghi tempi di ripristino di tutti i sistemi.

Backup con replica off-site

Il concetto di replica off-site in realtà può essere applicato a qualsiasi sistema di backup; si tratta di **una copia del backup che viene salvata "altrove" rispetto al backup standard**. Questo perché se il backup dei tuoi sistemi viene salvato all'interno di un server situato, ad esempio, nel tuo ufficio, in caso di incidenti anche questo rischierebbe di essere compromesso.

Pensa a un blackout, un incendio o qualsiasi altro tipo di disastro, ma soprattutto pensa a un sempre più comune attacco ransomware, in grado di diffondersi su tutte le macchine collegate a una rete per renderne illeggibili i file.

In questi casi è bene avere un'altra copia dei tuoi backup che si trovi in un posto differente. Molto spesso per le repliche off-site ci si affida a dei cloud provider come Amazon o Microsoft, ma è bene confrontarti con il tuo fornitore di servizi IT per stabilire qual è la migliore strategia da utilizzare per i tuoi backup.

CONCLUSIONI

Se sei arrivato alla fine di questo documento ormai ti sarà chiara una cosa: **il backup è una necessità di ogni realtà lavorativa**.

Ma avrai anche capito che **ci sono tante possibilità** di salvare e ripristinare i tuoi dati e che ogni azienda ha le sue specifiche necessità.

Quali sono i prossimi passi, quindi?

Per prima cosa ti consiglio di individuare un consulente IT affidabile. Una volta fatto, con il tuo aiuto, potrà effettuare un'analisi della tua situazione attuale:

- quanti dati vengono salvati;
- dove si trovano i dati e come vengono salvati;
- quanto sono importanti per il tuo business;
- quali sono i dati critici.

Sulla base di questa analisi potrà consigliarti delle soluzioni di backup con dei parametri RPO e RTO adatti alle tue esigenze e in linea con le tue possibilità di spesa.

In seguito potrà occuparsi lui dell'implementazione della soluzione individuata, mentre tu potrai dormire sogni un po' più tranquilli sapendo che i tuoi dati sono ben protetti.