White Paper

Perché e come proteggere i dati dei PC

DATA IS THE NEW OIL

Il grande sviluppo tecnologico che abbiamo vissuto negli ultimi anni ha completamente trasformato il modo di lavorare delle aziende. Se prima la tecnologia era presente in minima parte e si limitava a svolgere solo alcuni semplici compiti, ora **ogni attività viene eseguita attraverso uno strumento informatico e ogni informazione viene salvata sotto forma di dati**.

Pensa alla tua giornata lavorativa: **quante volte ti servi del PC, dello smartphone o della connettività a internet?**

Ora prova a immaginare la tua giornata lavorativa senza questi strumenti tecnologici e i dati che vi transitano… probabilmente saresti più produttivo stando seduto sul divano di casa tua a sgranocchiare patatine.

Al giorno d'oggi si rende necessario, quindi, che tutti i dipendenti siano in grado di accedere ai dati necessari per lavorare e che questi siano integri. Per questo **è necessario proteggerli attraverso il backup**, qualunque sia l'ambito in cui opera un'azienda.

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.

Ma quali dispositivi e quali dati vanno protetti?

Se è vero che **è naturale preoccuparsi dei server** e dei dati che risiedono in essi, **i dati che risiedono sulle postazioni di lavoro (endpoint) spesso e volentieri vengono trascurati**.

Questo è un errore da non sottovalutare: sia perché, in generale, anche in presenza di strutture con server centralizzati, il personale per comodità tende a salvare i dati sul proprio desktop e nella propria cartella documenti, sia perché l'aumento dei lavoratori in mobilità ha di fatto scardinato il concetto di "perimetro dell'ufficio" e anche i dati, insieme ai computer, si trovano sempre meno spesso all'interno dei confini della rete aziendale.

In effetti il numero di persone che lavora fuori azienda è iniziato a crescere anche prima del COVID-19: tecnici, venditori, personale che "lavora sul campo", ma anche manager, che sul treno o in aeroporto utilizzano i propri portatili.

Con lo scoppio della pandemia questa situazione si è addirittura accentuata, vista l'esplosione del lavoro da casa, anche nel nostro Paese.

I RISCHI PER I DATI

Ti ho parlato di protezione dei dati, ma forse ti starai chiedendo: "**da cosa dovrei proteggerli, esattamente**?"

Forse ti sembrerà un numero pazzesco, ma **ogni anno ci sono milioni di avvenimenti che in qualche modo causano la perdita dei dati aziendali**. I danni possono variare, ma spesso la perdita di dati porta all'impossibilità di lavorare o al dover perdere diverse ore, giorni o settimane a cercare di recuperare il lavoro perduto.

Come si perdono i dati? Nella maggior parte dei casi in modi abbastanza banali.

- **Guasti hardware**: i dati aziendali sono sempre memorizzati su delle unità di memoria, sia che si tratti di server che di computer. Se i dati sui server sono spesso già protetti da backup, i dati salvati sui computer sono spesso in pericolo. I guasti dei dischi su cui i dati vengono conservati sono all'ordine del giorno, anzi, con il passare del tempo le possibilità che qualcosa si rompa diventano sempre più concrete**.**
- **Problemi software**: le applicazioni sono il pane quotidiano di ogni azienda, immagino sia lo stesso per la tua. Ogni giorno si utilizzano applicazioni su cui transitano i dati più svariati. Per quanto sono sicuro che vorresti che queste funzionassero sempre in modo perfetto, si tratta pur sempre di software. E il software è "bacato" per definizione. Come conseguenza il crash o il malfunzionamento di un'applicazione potrebbe portare a corrompere i file su cui stai lavorando, rendendoli inaccessibili.
- **Cancellazione accidentale**: l'essere umano tende a distrarsi, a svolgere alcune attività sovrappensiero o, quando stressato, a commettere errori. Quando questi errori portano alla cancellazione di un file, di una cartella o di alcuni dati, le conseguenze possono essere davvero spiacevoli. Immagina di aver perso un file sul quale hai a lungo lavorato o su cui erano salvate informazioni importati per svolgere le tue attività… oltre a maledire te stesso e la sorte, l'unica cosa sensata da fare è proteggere questi file con un backup.
- **Virus e ransomware**: avendo ben chiaro in mente quanto importanti i dati siano, i criminal hacker cercano di sviluppare e diffondere virus che puntano a rubare, cancellare o bloccare i dati aziendali. Molto spesso, come nel caso dei ransomware, i dati vengono resi illeggibili finché l'azienda non paga una cospicua somma in bitcoin per "riscattare" i propri dati.

E l'elenco potrebbe andare avanti ancora a lungo.

COME PROTEGGERE I DATI

Hai quindi visto che è necessario proteggere gli endpoint con opportuni sistemi di backup.

Da dove cominciare a proteggere i dati?

Impostare un sistema di backup non è qualcosa che si può lasciare all'improvvisazione, si rischia usare soluzioni poco adatte o troppo costose per i sistemi da proteggere.

Ecco perché dovresti **affidarti a un consulente o una società che eroga servizi IT per farti consigliare** la soluzione più adatta alla tua azienda.

Ci sono numerose soluzioni e diversi metodi per eseguire il backup. **Vediamo, nel prossimo paragrafo, quali sono le tecniche più utilizzate oggi per proteggere i dati**.

Backup di file

Il backup di file è la modalità più tradizionale e **si occupa di salvare file e cartelle con l'obiettivo di ripristinarli in caso di necessità**.

È una forma di backup estremamente semplice ed è utile per chi salva i propri dati su file e cartelle. Se, invece, la tua necessità è quella di proteggere anche i dati che passano dalle applicazioni o gli interi sistemi utilizzati in azienda, ci sono soluzioni più adatte.

I backup di questo tipo si dividono normalmente in due categorie:

- **backup eseguiti in rete locale**, all'interno dell'azienda, per cui è necessario prevedere un server o dello spazio disco su cui memorizzare i dati;
- **backup eseguiti direttamente nel cloud**, in questo caso i dati lasciano gli endpoint e, con opportuna cifratura, vengono trasferiti direttamente presso qualche fornitore di storage (spazio) nel cloud.

Il backup dei file è estremamente comodo se capita di dover recuperare qualche file e cartella cancellati per errore e per i quali è necessario andare a trovare una versione "vecchia": in questi casi bastano pochi minuti per ripristinare i file.

Tuttavia, qualora si dovesse ripristinare da zero una macchina, si dovrebbe innanzitutto installare e configurare il sistema operativo, le applicazioni (queste due operazioni sono manuali e portano via diverso tempo) e, solo alla fine, si può precedere al recupero dei file e delle cartelle che erano state salvate.

Backup per immagini

I file e le cartelle presenti sui PC non sono l'unico elemento da proteggere. **Gli endpoint**, infatti, **sono costituiti da un sistema operativo su cui vengono eseguite configurazioni, salvate applicazioni e infine memorizzati dati**.

Il backup per immagini serve a salvare l'insieme di questi elementi all'interno di una "fotografia", un'istantanea dei sistemi.

In caso di problemi che dovessero rendere completamente indisponibili la macchina, **è possibile ripristinare l'intera immagine** e ricominciare a lavorare sui sistemi ripristinati.

Il backup per immagini porta con sé alcune conseguenze, tra le quali la grande necessità di spazio su disco per salvare i backup.

Occorre notare che spesso e volentieri questo tipo di backup per immagini "incorpora" anche il precedente backup per file: quindi da una fotografia statica di un certo PC è possibile recuperare anche i singoli file.

Backup con replica fuori sede

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.

Alcune soluzioni presenti sul mercato **comprendono più tipologie di backup**.

Può succedere, per esempio, che una soluzione di backup “per immagini” non ti consenta solo di salvare in cloud queste immagini, ma anche di far riaccendere presso la struttura cloud i computer che stavi proteggendo. Questo vuol dire che ad esempio, nel caso in cui un PC dovesse essere inutilizzabile, è possibile sfruttare la potenza del cloud per avviare in poco tempo il sistema danneggiato su un altro PC. Questo può garantire a te, o ai manager, di continuare a lavorare finché un nuovo PC non sarà pronto.

CONCLUSIONI

Ormai ti sarà chiaro che **il backup degli endpoint è una necessità di ogni realtà lavorativa**.

Ma con una varietà così grande di possibilità, da dove cominciare?

Per prima cosa puoi **confrontarti con il tuo fornitore di servizi IT per stabilire qual è la migliore strategia** da utilizzare per i tuoi backup e, ora che hai una maggiore consapevolezza di quali sono i rischi e quali le possibili soluzioni, potrai valutare con più attenzione le sue proposte.

Una volta valutate le possibilità e scelta la strategia di backup per la tua azienda non ti resta che passare all’implementazione. Tranquillo, tu non dovrai fare niente. Ci penserà il tuo fornitore, mentre tu potrai continuare a lavorare **consapevole che i tuoi dati sono al sicuro**.