Backup dei dati nelle PMI

Il ripristino rapido e il più completo possibile dei dati aziendali in caso di perdita per dolo, incidente o casualità è una parte imprescindibile della protezione di base di una PMI, che richiede un processo di backup ben strutturato.

Punti principali per le aziende:

- Stilate un inventario dei vostri sistemi IT e dei dati e per ogni elemento definite il massimo grado di perdita o avaria sopportabile.
- Sulla base di tale elenco, stabilite alcune classi di protezione per gli elementi che presentano lo stesso livello di rischio e per ciascuna classe studiate uno schema di backup.
- Definite e implementate nella vostra PMI un processo di backup dei dati.
- Controllate periodicamente che le operazioni di salvataggio avvengano secondo lo schema e che i dati si possano ripristinare.

Il processo di backup dei dati

La crescente digitalizzazione si accompagna a un aumento costante, anche nelle PMI, del numero di sistemi IT utilizzati e della quantità di informazioni elaborate. Di conseguenza, le aziende dipendono sempre più dalla possibilità di accedere ai loro sistemi e dati senza alcuna limitazione.

Grosse perdite di dati, derivanti p. es. da attacchi informatici, difetti tecnici, eventi naturali o anche solo da banali cancellazioni accidentali, possono mettere a rischio la sopravvivenza di una piccola o media impresa. La possibilità di ripristinare i dati aziendali da un backup nel modo più rapido e completo è quindi un pilastro della protezione di base.

Occorre perciò stabilire un processo che garantisca la corretta realizzazione delle copie di sicurezza secondo uno schema studiato. Di pari importanza è che il processo preveda anche la verifica periodica dell'effettiva ripristinabilità dei dati.

Le classi di protezione

I vari sistemi IT e dati di una PMI hanno un impatto diverso sulle procedure aziendali; di conseguenza, deve essere differenziata anche la valutazione di quanto sia importante salvaguardarli. Un inventario completo e aggiornato dei sistemi IT e dei dati è il primo passo per avere una panoramica e inserire le varie componenti nella giusta classe di protezione (CdP).

Esempio di assegnazione a una classe di protezione in base a criteri

CdP	Denominazione	Rischio	Perdita/avaria max. sopportabile	Tempo di ripristino	Periodi di conservazione
I	Esigenza di protezione normale	Basso	> 1 giorno	< 1 settimana[/av_cell]> 1 settimana	
II	Esigenza di protezione elevata	Medio	1 giorno	1 giorno	> 1 mese
III	Esigenza di protezione assai elevata	Elevato	< ½ giorno[/av_cell]> 1 anno		

Oltre al pericolo rappresentato dalle situazioni citate, l'attenzione va posta anche su altri criteri, tra cui da un lato la stima del massimo grado sopportabile di avaria per i sistemi IT o di perdita quantitativa per i dati e, dall'altro, i periodi di conservazione necessari.

Una valutazione di questo genere permette di ripartire in classi di protezione i sistemi IT e i dati che presentano esigenze di salvaguardia analoghe. Per ogni classe di protezione vengono poi stabiliti i requisiti che deve soddisfare lo schema di backup.

Lo schema di backup dei dati

Lo schema di backup dei dati fissa i dettagli organizzativi e tecnici con cui si creano le copie di sicurezza per le varie classi di protezione. Tra i dettagli organizzativi vi sono in particolare:

1. entità (*scope*) delle copie di sicurezza
2. periodicità del backup (giornaliero, settimanale, mensile, ...)
3. tempistica del backup (a fine giornata, fine settimana, fine mese, ...)
4. periodi di conservazione dei set di backup (principio delle generazioni)
5. tempi di ripristino richiesti (massima avaria sopportabile)

Da questi derivano i dettagli tecnici, in particolare:

1. metodo di backup dei dati (completo, differenziale, incrementale)
2. supporto per il backup (disco rigido, nastro, ...)
3. conservazione dei supporti (on-premise, fisicamente delocalizzati, cloud, ...)

Grosse perdite di dati – dovute p. es. ad attacchi informatici, difetti tecnici, eventi naturali o cancellazioni accidentali – possono mettere a rischio la sopravvivenza di una PMI.

Uno schema ragionato di backup può ridurre al minimo simili rischi e consentire un ripristino rapido e possibilmente completo dei dati perduti.

Ulteriori informazioni

L'**entità delle copie di sicurezza** (*scope*) determina quali dati (e quali loro origini) sono effettivamente inclusi nel backup. Un'archiviazione ben ragionata e strutturata può contribuire notevolmente a garantire che non vengano trascurati elementi importanti. Inoltre, è opportuno verificare se i dati (e le loro origini) da replicare sono effettivamente disponibili al momento della copiatura (p. es. se i dispositivi in questione sono spenti durante il fine settimana).

Per quanto riguarda la **periodicità del backup**, intervalli ravvicinati assicurano sì che vadano perduti meno dati, a fronte però di operazioni ben più impegnative tra cui l'eventuale rallentamento della rete laddove si vogliano salvare ogni giorno grandi quantità di informazioni. È opportuno, allora, valutare attentamente le esigenze di protezione.

La **tempistica del backup** dipende dai processi aziendali. L'attenzione va posta su quanto sarebbe rischioso subire una perdita nell'arco di tempo compreso tra due operazioni di salvataggio. Spesso le copie di sicurezza vengono create a fine giornata, così da non disturbare le attività diurne e sfruttare le risorse inutilizzate di notte.

In genere, in caso di perdita dei dati si ripristina l'ultimo set disponibile. Per vari motivi, tuttavia, a volte può anche rendersi necessario recuperare dati storici, meno recenti. Per questo tipo di informazioni vanno specificati i **periodi di conservazione dei set di backup**. Uno schema a rotazione (principio delle generazioni) ragionato e adeguato alle quantità di dati e alle esigenze di protezione della PMI permette di soddisfare queste esigenze minimizzando il fabbisogno di supporti. Per fare un esempio, se si configura una periodicità giornaliera (lun–ven) possono essere sufficienti 20 supporti per ripristinare i set degli ultimi quattro giorni feriali (lun–gio), degli ultimi 13 fine settimana (ven), degli ultimi due fine mese e dell'ultimo backup di fine anno.

I **tempi di ripristino richiesti** rappresentano la quantità di tempo necessaria per recuperare i dati dopo che se ne è constatata la perdita. Ridurre il periodo massimo sopportabile per l'assenza di dati fa crescere i requisiti organizzativi e tecnici per il backup. Tra le operazioni da considerare per calcolarne la durata vi sono l'identificazione degli elementi da recuperare, la loro localizzazione nei vari set di backup, l'accesso ai supporti necessari e l'effettiva rigenerazione delle informazioni.

Può accadere che il tempo disponibile (p. es. le ore notturne) non sia sufficiente per eseguire il backup completo dei dati di una determinata classe di protezione con la periodicità richiesta. Questo problema può essere mitigato scegliendo il giusto **metodo di backup** (completo, differenziale, incrementale). Il backup **completo** crea sul supporto una copia integrale di tutto ciò che rientra nello *scope*: si tratta della procedura più esigente in termini di spazio di archiviazione e tempi. Con il metodo **differenziale**, invece, vengono salvati solo i dati che hanno visto modifiche o rilevano differenze rispetto all'ultimo backup completo. Con questa procedura si riduce notevolmente il volume dei dati, poiché per i documenti non modificabili, in particolare, è sufficiente un'unica copia di sicurezza. Se si adotta questo metodo, il ripristino avviene in due fasi, cominciando con l'ultimo backup completo disponibile prima di passare a quello differenziale. Il metodo **incrementale** riduce ulteriormente il volume dei dati da salvare, poiché vengono salvati soltanto quelli modificati rispetto all'ultimo backup, indipendentemente dal metodo utilizzato per crearlo. L'eventuale ripristino dovrà quindi considerare l'ultimo set completo, l'ultimo differenziale e tutti i successivi incrementi.

Per «**supporto per il backup dei dati**» si intende il sistema che accoglie una determinata serie di copie di sicurezza. Nel caso più semplice, può trattarsi di un semplice file con uno specifico formato, oppure anche di un supporto fisi-

co (disco rigido, supporto ottico, nastro magnetico ecc.) che fa parte di un sistema di backup dedicato. La scelta del supporto giusto dipende principalmente dai requisiti organizzativi (entità, periodicità, periodi di conservazione e tempi di ripristino). Soprattutto per la memorizzazione a lungo termine (archiviazione) di grandi quantità di informazioni si prediligono i nastri magnetici.

I supporti di backup e la loro **conservazione** rivestono la massima importanza per l'intero processo di protezione dei dati. La valutazione del rischio non può prescindere da fattori quali la sicurezza fisica, le condizioni di conservazione, la disponibilità, l'accessibilità ecc. In generale, i backup dovrebbero essere il più possibile preservati e isolati dagli influssi esterni. Per esempio, l'esistenza del ransomware rende necessario garantire che queste forme di attacco non possano raggiungere le copie di backup – in altre parole, occorre conservarle offline.