BACK UP DAY: Evoluzione, strategia e rinnovamento per garantire resilienza al business delle aziende.
A cura di Andrea Guerra, Technical Expert VEM sistemi

Una delle sfide che il mondo IT sta affrontando in questo periodo riguarda l'ingresso nel mondo hybrid Cloud.
Le esigenze di business, infatti sono cambiate: l'utilizzo di architetture on-premise per l'erogazione di servizi che non richiedono particolari fattori di dinamicità e scalabilità, si affianca all'utilizzo di risorse "a consumo" sul public cloud.

L'avvento dell'Hybrid ha spinto le aziende ad adottare un modello diverso rispetto al passato, spostando il paradigma di "gestione delle infrastrutture" a quello di "gestione delle applicazioni". Questo nuovo paradigma application-centric ha allargato la visione, spingendo le aziende ad adottare strategie MultiCloud per l'erogazione dei servizi aziendali, posizionando dati e applicazioni sull'hyperscaler più congeniale.
Nel 2023 il backup day porta con sé sfide nuove e diverse: Hybrid e MultiCloud sono diventati uno standard de facto, hanno ottimizzato performance e disponibilità dei servizi ma allo stesso tempo hanno frammentato la gestione del dato, rendendone più difficoltosa la protezione. In Italia gli attacchi informatici nel 2022 sono cresciuti del 169% rispetto all'anno precedente come rileva il Rapporto Clusit e la minaccia ransomware è una piaga che sta diventando più difficile da contrastare e sempre più crescente. Basti pensare che il Cybersecurity Ventures stima che entro il 2031 un device subirà un attacco ogni 2 secondi.

Oggi l'obiettivo è proprio quello di creare sinergia tra disponibilità dei servizi e sicurezza del dato e VEM identifica 3 step distinti per farlo: Evoluzione, Strategia e Rinnovamento.

- **Evoluzione**
  - Si intende proteggere i propri workload in maniera moderna, sfruttando meccanismi di Machine Learning e intelligenza artificiale. L'analisi del dato di backup è diventata molto importante perché permette di ridurre gli impatti di un attacco e di accelerare i tempi di ripristino del servizio, escludendo tutti quei dati non più integri o che potrebbero nascondere minacce
- **Strategia**
  - La strategia deve essere incentrata su un modello "zero trust" basato sul principio del "non fidarsi mai" in quanto tutti i device sono da considerarsi inaffidabili e attaccabili. La strategia quindi deve prevedere la conservazione delle copie di backup su una soluzione con file system immutabile, che lavori in modalità append-only e che non esponga protocolli di rete aperti. Inoltre diventa fondamentale la gestione delle utenze in grado di accedere ai sistemi di backup: su questo tema è necessario dotarsi di soluzioni in grado di gestire in maniera granulare ruoli e permessi utenti, che integrino MFA e che prevedano un "quorum" di amministratori per l'approvazione di una qualsiasi modifica (per esempio la correzione di una policy di backup)
- **Rinnovamento**
  - Il rinnovamento riguarda l'adozione di soluzioni next-gen per l'archiviazione dei backup, soluzioni che permettano di gestire l'archiviazione dei dati in storage ad oggetti immutabili e opportunamente isolati (air-gap). Una soluzione di Object storage prevede due modalità di implementazione: ibrida o SaaS.

- La modalità ibrida prevede l'introduzione di uno storage ad oggetti on-premise che possa scalare infinitamente in termini di spazio/performance. La scalabilità può estendersi verso il public cloud, mantenendo il controllo dei dati su tutto lo stack.
- La modalità cloud-based prevede l'utilizzo di servizi SaaS basati sul protocollo S3. Una volta archiviati i dati, il sistema SaaS è in grado di isolarsi, realizzando di fatto un air gap logico che non espone dati se non al solo sistema di backup durante la fase di archive.

È evidente quindi come il back-up non sia più solo una copia del dato di produzione ma è gestione dell'informazione a 360 gradi, garantisce sicurezza e resilienza al business delle aziende, assicurando un futuro in cui i dati continueranno a guidarne il rinnovamento.