Tecno - *Cyberattacchi, il backup non basta più: i criminali informatici puntano alle copie dei dati, ecco perché serve la "cyber resilience"*

Roma - 02 lug 2026 (Prima Notizia 24) **Secondo l'analisi di Infinidat, ransomware e malware prendono sempre più di mira i sistemi di backup. Oggi la vera sfida non è solo conservare i dati, ma riuscire a ripristinarli rapidamente dopo un attacco.**

Per anni è stato considerato la principale garanzia contro la perdita dei dati. Oggi, però, il semplice backup non basta più. L'evoluzione degli attacchi informatici ha cambiato profondamente le strategie dei cybercriminali, che non si limitano più a colpire server e reti aziendali, ma prendono direttamente di mira le copie di sicurezza. È questa l'analisi contenuta nel nuovo News Blog di Infinidat, società del Gruppo Lenovo specializzata nello storage enterprise, firmato da Donato Ceccomancini, Country Manager Italia dell'azienda. Secondo l'esperto, la capacità di recuperare rapidamente dati e applicazioni critiche è diventata oggi il vero elemento che determina la sicurezza di un'organizzazione. Perché gli hacker attaccano anche i backup Il motivo è semplice: compromettere i sistemi di backup significa impedire alle aziende di ripristinare rapidamente la propria operatività dopo un attacco ransomware. In questo modo aumenta il potere di ricatto dei criminali informatici, che possono costringere le vittime a pagare per riottenere l'accesso ai propri dati. Quello che un tempo rappresentava soltanto uno strumento di protezione è diventato quindi uno degli obiettivi principali degli attacchi cyber più sofisticati. In Italia gli attacchi crescono del 42% Lo scenario italiano conferma questa evoluzione. Secondo il Rapporto Clusit 2026, citato nell'analisi, nel corso del 2025 gli attacchi informatici gravi contro organizzazioni italiane sono aumentati del 42%. Anche l'Agenzia per la Cybersicurezza Nazionale continua a indicare ransomware, phishing e compromissione delle infrastrutture digitali tra le principali minacce per imprese e pubbliche amministrazioni. Numeri che, secondo Infinidat, impongono un cambio di prospettiva. Dalla protezione dei dati alla cyber resilience Fino a pochi anni fa l'obiettivo principale era conservare una copia dei dati aziendali. Oggi la priorità è diversa: bisogna garantire che quelle copie rimangano integre, non possano essere modificate dagli attaccanti e siano immediatamente disponibili quando serve ripristinare i sistemi. È questo il concetto di cyber resilience, sempre più centrale nelle strategie di sicurezza informatica. Non si tratta semplicemente di conservare i dati, ma di assicurare la continuità operativa anche durante un attacco, limitando i tempi di fermo e riducendo i danni economici. Come sono cambiati gli attacchi ransomware Secondo l'analisi, molte infrastrutture di backup oggi ancora in uso sono state progettate per affrontare eventi accidentali, come guasti hardware o errori umani. I ransomware moderni, invece, seguono una logica completamente diversa. Prima di cifrare i dati, cercano deliberatamente di compromettere snapshot, repository e copie di sicurezza, eliminando qualsiasi possibilità di recupero autonomo da parte

dell'azienda. Per questo motivo le strategie tradizionali di data protection risultano sempre meno efficaci. Le caratteristiche richieste ai nuovi sistemi di backup Anche il modo di valutare le infrastrutture di storage sta cambiando. Oggi, spiega Infinidat, non conta soltanto la capacità di archiviare grandi quantità di dati. Sempre più importanti diventano elementi come: l'immutabilità delle copie di backup; l'isolamento dei dati dai sistemi di produzione; il rilevamento tempestivo di comportamenti anomali; la velocità di ripristino delle informazioni critiche. Sono queste caratteristiche che consentono di ridurre realmente l'impatto di un attacco informatico. Lo storage diventa parte della difesa informatica L'evoluzione delle minacce sta modificando anche il ruolo dello storage aziendale. Sempre più imprese cercano piattaforme capaci di integrare direttamente funzionalità di protezione informatica all'interno dell'infrastruttura, riducendo così la superficie di attacco e aumentando la disponibilità dei dati anche nelle situazioni più critiche. Secondo Donato Ceccomancini questa è ormai una richiesta comune in aziende appartenenti ai settori più diversi. Le imprese cercano infrastrutture semplici da amministrare, ma soprattutto in grado di garantire continuità operativa anche durante eventi imprevisti o attacchi cyber. Il vero interrogativo per le aziende Secondo Infinidat, la domanda che ogni organizzazione dovrebbe porsi oggi non è se possieda un sistema di backup. La vera domanda è un'altra: quel sistema sarà realmente in grado di rendere disponibili i dati quando tutto il resto avrà smesso di funzionare? È proprio questa la differenza tra una strategia di backup tradizionale e un'infrastruttura progettata secondo i principi della cyber resilience. Il ripristino rapido è la nuova priorità La conclusione dell'analisi è chiara. Il valore di una moderna strategia di protezione dei dati non si misura più dal numero di copie archiviate, ma dalla rapidità e dall'efficacia con cui dati e servizi essenziali possono essere ripristinati dopo un incidente. In uno scenario in cui gli attacchi informatici sono considerati sempre più inevitabili, la capacità di recuperare rapidamente l'operatività rappresenta oggi uno dei principali elementi di competitività e sicurezza per qualsiasi organizzazione.

(Prima Notizia 24) Giovedì 02 Luglio 2026

Sede legale : Via Costantino Morin, 45 00195 Roma
E-mail: redazione@primanotizia24.it