Il tema della **sicurezza informatica** è sempre più centrale sia nelle grandi aziende come nelle realtà di dimensioni inferiori.

Se in passato il rischio informatico era concentrato su aree quali la violazione dei dati e la responsabilità civile, i moderni attacchi informatici come le infezioni da ransomware provocano danni maggiori.

Gli assicuratori che si occupano di **cyber insurance** hanno reagito all'aumento del rischio e hanno adeguato le proprie offerte, come dimostra una recente analisi di Swiss Re Insurance. La società prevede che i premi totali pagati dalle aziende saranno più che raddoppiati, passando da 10 miliardi di dollari nel 2020 a 23 miliardi di dollari entro il 2025.

Nonostante l'aumento della domanda per le polizze di cyber insurance, ovvero le assicurazioni contro gli **attacchi informatici**, il CEO di Zurich - Mario Greco - ha dichiarato questa settimana in un'intervista al Financial Times che i **cyberattacchi diventeranno presto "non assicurabili"**.

Parlando di copie di sicurezza dei dati, sebbene ne esistano diverse varianti, la strategia del backup 3-2-1 rimane la mossa vincente da porre in campo.

Lo sanno bene quelle realtà aziendali che purtroppo sono state vittime di attacchi ransomware senza disporre di **backup** aggiornati dei dati.

La cifratura dei dati da parte di un ransomware rappresenta infatti soltanto l'ultima fase di un attacco informatico, nato molto prima, e in grado di sfruttare evidenti lacune nella configurazione della rete, nella gestione dei permessi, nella condivisione delle risorse, nella protezione di server, workstation e singoli pc, nella mancata applicazione di aggiornamenti di sicurezza (sistema operativo, browser di navigazione, software installati) nell'utilizzo di dispositivi insicuri, (chiavette usb non opportunamente verificate, vecchi smartphone, e tablet con versioni di Android o IOS deprecate e non

più aggiornabili) nella mancata adozione di strumenti centralizzati per la difesa dell'infrastruttura.
Anche seguendo tutte le linee guida e utilizzando i migliori strumenti per la difesa del **perimetro aziendale**, è tuttavia impensabile avere la certezza di essere protetti al 100%.
Per questo, è essenziale predisporre un efficace piano di **disaster recovery**. In questo senso l'adozione di politiche di backup adeguate fa davvero la differenza.

Backup 3-2-1: la regola che mette al riparo da qualunque incidente informatico

Creare un backup su un dispositivo collegato in rete locale, "vicino" ai sistemi che contengono i dati da proteggere, è del tutto inutile se le risorse sono accessibili da più utenti.
Un ransomware o un qualunque malware che utilizza tecniche per il **movimento laterale** (dopo aver infettato un sistema, il componente dannoso va alla ricerca di altre macchine da aggredire sfruttando, condivisioni di rete e vulnerabilità insite nei vari software) potrebbe facilmente danneggiare anche le copie di backup memorizzate su altri dispositivi.
Come regola generale, quindi, il dispositivo che ospita i backup dovrebbe esso stesso accedere alle risorse condivise in LAN da copiare e mettere in sicurezza, oppure servirsi di "agenti software" che gestiscono la procedura di backup in modo sicuro, senza esporre direttamente le risorse.
Il sistema scelto per il backup dovrebbe inoltre supportare il **versioning**, funzione che dà la possibilità di gestire le varie versioni di uno stesso documento e che tiene traccia delle modifiche effettuate nel tempo.

Dopo un'infezione da ransomware sarebbe davvero disarmante scoprire che il dispositivo di backup ha creato una copia dei dati crittografati dai criminali informatici sovrascrivendo le versioni originali.

Il **backup 3-2-1** prevede che:

- **Vengano create una copia primaria dei dati e due copie accessorie**
- **I backup devono essere salvati su due differenti tipi di supporti di memorizzazione**
- **Sia creata almeno una copia di backup offsite ovvero in un luogo sicuro lontano dalla vostra rete dati, presso terzi**

Per le aziende che utilizzassero un approccio ibrido o avessero deciso di abbracciare l'utilizzo di piattaforme quali **Microsoft 365** o **Google Workspace**, è bene rimarcare come la responsabilità nell'eseguire il backup dei dati sia dell'utente e non del gestore del servizio.

Microsoft, Google e gli altri fornitori si impegnano contrattualmente a mantenere raggiungibili, funzionanti e performanti le rispettive piattaforme cloud, e che le repliche dei dati degli utenti, effettuate automaticamente e in più data center, facciano in modo che le conseguenze di un disastro non si rifletta sull'integrità delle informazioni.

Le funzionalità di versioning che offrono soluzioni come Microsoft 365 e Google Workspace, sono utili in caso di:

- **modifiche avventate sui files**
- **cancellazioni non volute**

ma i ransomware aggrediscono anche le piattaforme cloud, e possono mettere a rischio la disponibilità e l'integrità dei dati dell'azienda che avesse scelto solamente quel tipo di soluzione.