Enterprise Strategy Group | Getting to the bigger truth.™

WHITE PAPER ESG

Il ruolo dello storage per garantire la resilienza IT

A cura di Scott Sinclair, ESG Practice Director e Senior Analyst
e Monya Keane, ESG Senior Research Analyst

Gennaio 2022

White Paper ESG commissionato da IBM
e distribuito su licenza di TechTarget, Inc.

Indice

Sommario

Il ruolo dei dati come risorsa aziendale strategica sta assumendo sempre più importanza. Grazie all'aumento degli investimenti in sviluppo di applicazioni e moderne pratiche DevOps, all'aumento della domanda di business intelligence, analytics e machine learning, praticamente in tutte le aziende si assiste a un aumento nella creazione e uso di dati. E aumenta il numero di sedi che li utilizzano. Questa proliferazione di dati, combinata con la crescente pressione sul business, ha portato a un aumento di complessità dell'infrastruttura e delle operazioni IT.

Tali fattori espongono le aziende e le loro infrastrutture a un elevato rischio di dover fronteggiare attacchi, errori umani e comportamenti negligenti. Sfortunatamente, le vecchie strategie non sono in grado di fornire un'adeguata garanzia di continuità delle operation aziendali durante e dopo questo tipo di incidenti. Le aziende possono cercare di utilizzare insieme funzionalità di tool diversi nel tentativo di impedire gli attacchi e altre violazioni, ma gap funzionali, scarsa integrazione e complessità di gestione rendono il raggiungimento degli obiettivi di sicurezza un processo difficile e lungo.

Modificare l'approccio organizzativo passando dalla prevenzione alla velocità di risposta agli incidenti, ad es. implementando soluzioni di storage con resilienza IT integrata, è fondamentale per proteggere le risorse di dati critiche ed essere in grado di fornire risposta e ripristino rapidi da ransomware e altre forme di attacchi informatici.

Introduzione

L'IT si trova ad affrontare nuove sfide. Quasi la metà (46%) di coloro che sono stati sottoposti al sondaggio ESG afferma che l'IT è molto più complesso oggi rispetto a due anni fa. Tale aumento di complessità può essere il risultato di continue iniziative di trasformazione digitale (citate dal 29%), volumi di dati superiori (35%), rapida evoluzione del panorama della sicurezza informatica (37%), e/o sforzi di rispettare nuove regolamentazioni in materia di sicurezza dei dati e di privacy (32%).[1]

Allo stesso tempo, le aziende stanno facendo di tutto per affrontare una problematica scarsità di competenze IT. Infatti, il 48% delle aziende che ha partecipato al sondaggio riferisce di non disporre di un sufficiente numero di esperti di sicurezza informatica; è la principale area di debolezza indicata. Inoltre, tali aziende hanno a che fare con una quantità variegata di applicazioni, dispositivi e lavoratori da remoto/in mobilità che estendono l'ambito del perimetro di sicurezza che i team IT hanno il compito di proteggere.[2]

Data la complessità dell'IT, la proliferazione di dati e le minacce di attacchi informatici in costante crescita, i team IT spesso faticano a tenere il passo. Tentare di risolvere la complessità soltanto con personale interno è una battaglia persa. Il successo richiede la modernizzazione della stessa infrastruttura sottostante. Comunque, nel farlo, i decisori devono cercare tecnologie che non si limitino a soddisfare le esigenze applicative o a semplificare le operazioni. Raggiungere il vero successo significa trovare la tecnologia che possa soddisfare tali obiettivi e migliorare la sicurezza IT dell'ambiente applicativo.

Una crescente minaccia di attacchi informatici e ransomware

Le aziende affrontano minacce alla sicurezza informatica in costante crescita, probabilmente alimentate dall'aumento di incentivi economici ai criminali informatici. Ad esempio, le cause avviate da parte del pubblico americano nel 2020 presso l'Internet Crime Complaint Center (IC3) dell'FBI sono aumentate del 69% dal 2019, con perdite dichiarate superiori ai 4,1

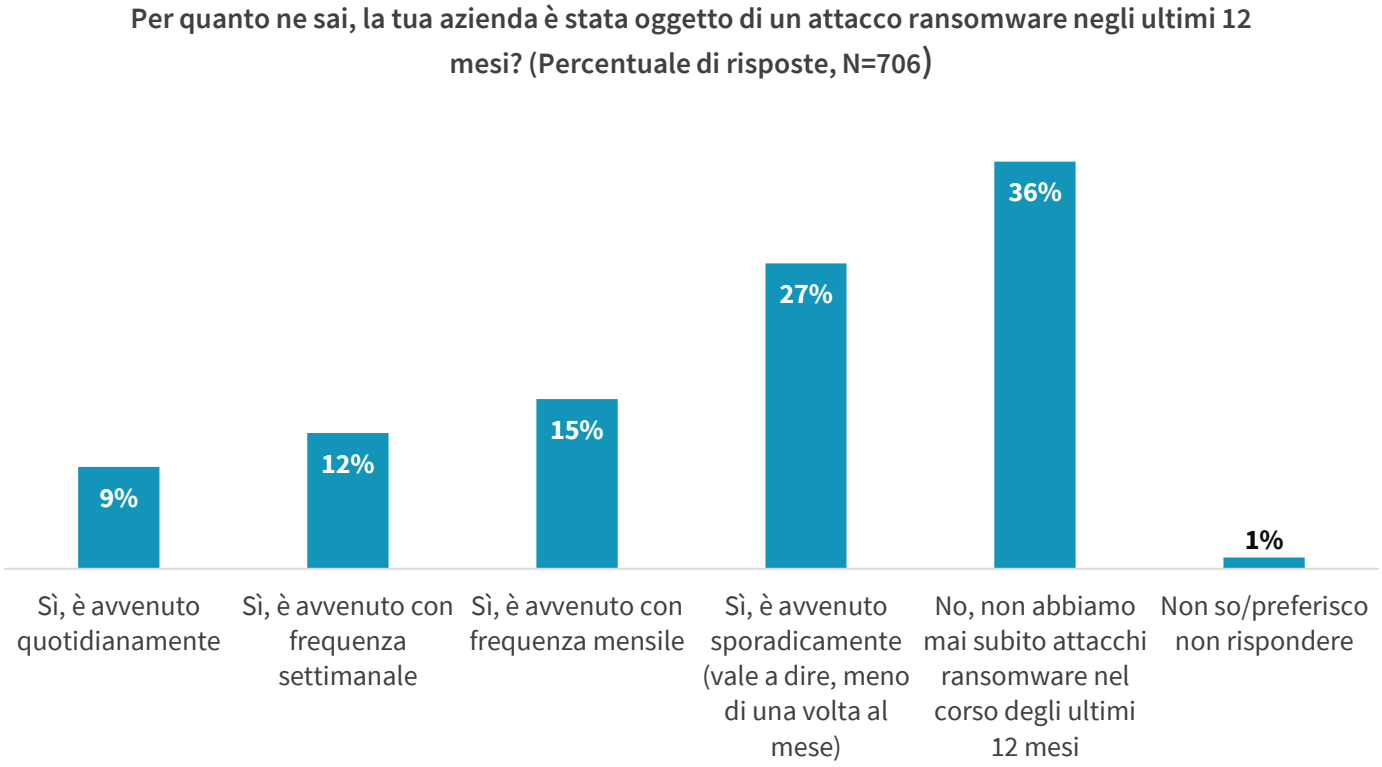
[1] Fonte: Risultati completi sondaggio ESG, *2022 Technology Spending Intentions Survey (Sondaggio sulle intenzioni di spesa tecnologica)*, novembre 2021.
[2] Ibid.

miliardi di USD.[3] Inoltre, negli ultimi cinque anni, l'IC3 riferisce perdite totali combinate pari a 13,3 miliardi di USD.[4] Nel quarto trimestre del 2020, negli USA la durata media dell'interruzione in seguito ad attacchi ransomware alle aziende era di 21 giorni.[5] Ovviamente, l'impatto negativo del ransomware sulle operazioni aziendali è considerevole.

Esiste una forte correlazione tra complessità IT e vulnerabilità agli attacchi informatici. Man mano che l'IT diventa più complesso aumenta la frequenza degli attacchi informatici con costi sempre maggiori.

Il ransomware costituisce una minaccia pervasiva che prende di mira una delle risorse di maggior valore di un'azienda: i suoi dati.

Figura 1. Il 63% degli intervistati è stato vittima di attacchi ransomware nel corso degli ultimi 12 mesi



Fonte: ESG, divisione di TechTarget, Inc.

L'IC3 ha individuato 2.474 incidenti ransomware riferiti nel 2020 ed ESG ha scoperto che il 63% delle aziende sottoposte al sondaggio ha subito attacchi ransomware nel corso dell'ultimo anno. Infatti, il 9% è stato quotidianamente vittima di attacchi ransomware (vedi Figura 1).[6]

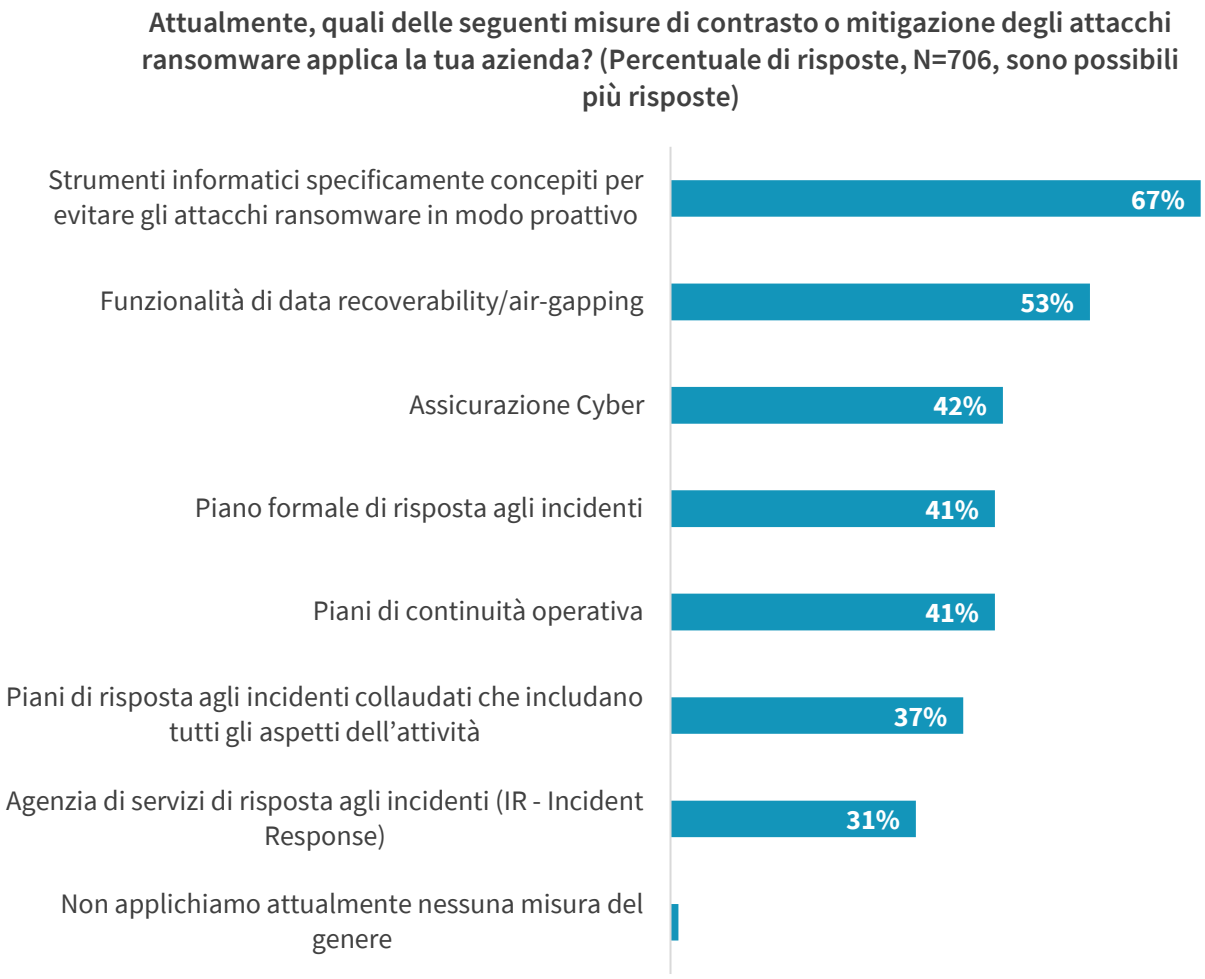
La protezione contro il ransomware richiede una strategia tecnologica che vada ben al di là della tradizionale sicurezza informatica: deve sfruttare i progressi nello storage e nella protezione di dati.

Il ruolo dello storage nella resilienza IT

[3] Fonte: Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*.
[4] Ibid.
[5] Fonte: Blog Coveware, *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, Febbraio 2021.
[6] Fonte: Risultati completi sondaggio ESG, *2022 Technology Spending Intentions Survey (Sondaggio sulle intenzioni di spesa tecnologica)*, novembre 2021.

I sistemi di storage e gli storage administrator rivestono entrambi un ruolo fondamentale nella protezione contro il ransomware. Quando ESG ha chiesto ai decisori IT quali misure avessero adottato le loro aziende per contrastare o mitigare gli attacchi ransomware, il 67% delle persone intervistate ha riferito di utilizzare strumenti informatici di prevenzione proattiva del ransomware per contrastare o mitigare questo tipo di attacchi e il 53% ha indicato le funzionalità di ripristino dei dati come l'air-gapping (vedi Figura 2).[7] Queste due risposte comuni mettono in evidenza l'importanza non solo dell'implementazione di misure per evitare un attacco, ma anche degli investimenti in soluzioni per garantire che l'azienda sia preparata al ripristino quando l'attacco inevitabilmente si verifica. È importante non limitarsi a impostare policy per combattere o mitigare il ransomware. Un simile approccio "parziale" crea un falso senso di sicurezza perché, mentre si lavora per mitigare gli attacchi, non si fa praticamente nulla per introdurre un efficace piano di ripristino *prima* che sia necessario.

Figura 2. Comuni misure utili a contrastare o mitigare il ransomware



Fonte: ESG, divisione di TechTarget, Inc.

È importante ricordare che il "contrasto ad un attacco" differisce abbastanza dal tradizionale ripristino di dati. Le aziende desiderano quasi sempre ripristinare i loro dati utilizzando la copia più recente. Ma con il ransomware, l'IT spesso non sa quale sia la copia "giusta" da utilizzare; quindi, il ripristino è spesso più rischioso e può richiedere più tempo. Alcuni

[7] Ibid.

attacchi ransomware non si limitano solo a prendere di mira i dati ma anche la stessa infrastruttura di backup. E questa è la ragione per cui le funzionalità di storage avanzate sono fondamentali per un efficace ripristino dal ransomware.

Anche se l'adozione delle misure identificate nella Figura 2 ha il suo senso e deve crescere, è necessario che le aziende capiscano che nessuna difesa è di per sé efficace al 100% per il ripristino da un ransomware. È importante considerare gli strumenti che sono specializzati nell'individuazione e nella prevenzione del ransomware oltre che nel ripristino dei dati, che è solo una parte del lavoro. Persino con le migliori difese, è possibile che si verifichi un attacco. Le aziende devono prepararsi a tale eventualità e valutare in quale modo possono minimizzare l'impatto sull'azienda effettuando il ripristino nel modo più rapido possibile. Per ridurre al minimo l'esposizione complessiva al ransomware, le aziende devono trovare il modo di accelerare l'individuazione degli attacchi, la mitigazione rapida di qualsiasi compromissione e la velocità di ripristino.

Ed è questo il punto in cui entrano in gioco le strategie di resilienza IT che prendono in considerazione *tutti i componenti* del trattamento dei dati, vale a dire hardware, software, persone e processi. Nello sviluppo di un approccio di resilienza IT, le aziende devono passare dal chiedersi "Come ci proteggiamo?" a "*Nel caso in cui fossimo colpiti da ransomware, quanto rapidamente potremmo effettuare il ripristino*? *Quanto rapidamente la nostra attività potrebbe tornare alla normalità*?"

Storage e protezione dei dati: sapere su cosa concentrare l'attenzione per minimizzare il rischio di ransomware

Il ripristino dal ransomware è una forma di disaster recovery, ma gli effetti del ransomware sono piuttosto diversi da quelli di un incendio o un'inondazione. Dopotutto, è possibile dire quando un incendio è completamente estinto. Il ransomware somiglia piuttosto a una scintilla nascosta all'interno di una parete che è in grado potenzialmente di riaccendersi. Gli storage administrator devono concentrare la propria attenzione su determinate aree per contribuire a ridurre i rischi associati al ransomware. Poiché la velocità è fondamentale, devono determinare quanto rapidamente la loro azienda può:

- Identificare il rischio.
- Quantificare il danno generato.
- Mitigare il danno individuando una buona copia nota, effettuando il ripristino grazie all'uso di tale copia e, in definitiva, ripristinando le operazioni.

Adottare un approccio del tipo "a noi non accadrà mai" è la cosa più rischiosa. Le aziende devono essere proattive e introdurre una soluzione efficace di storage e protezione dei dati, prima di averne effettivamente bisogno.

Passare dalla sicurezza informatica alla resilienza IT con IBM

IBM, con la sua vasta esperienza nella sicurezza informatica e nel risk management, è leader riconosciuto nel campo della resilienza IT e offre una suite completa di soluzioni avanzate per lo storage e la protezione dei dati, tra cui:

- IBM FlashSystem, IBM Cloud Object Storage e IBM Spectrum Scale, importanti soluzioni di storage dotate di funzionalità di immutabilità e crittografia dati.
- IBM Tape Storage, che supporta anche immutabilità e crittografia dati e fornisce protezione mediante air-gapping.
- Il software IBM Spectrum Copy Data Management gestisce e protegge le copie dei dati.

- IBM Spectrum Protect Suite per maggiore protezione. Lo storage software-defined di Spectrum Protect può memorizzare i dati su flash, disco, object storage e nastro fisico o virtuale. Rileva quindi l'attività malware e ransomware individuando grandi deviazioni dai normali comportamenti di accesso.

- Le soluzioni QRadar e Storage Insights contribuiscono ad accelerare il rilevamento di potenziali minacce grazie a funzionalità di intelligenza artificiale.

Resilienza IT con IBM Cyber Vault

Lo storage ha un ruolo fondamentale nella protezione contro il ransomware. Il software di storage supervisiona gli aggiornamenti dei dati primari e, di conseguenza, si trova in una posizione ideale per individuare quando sta iniziando un attacco. È la tecnologia che sta anche eseguendo e proteggendo copie secondarie, rendendo lo storage di estrema importanza nell'aiutare il ripristino. Tenendo a mente tutto ciò, forse uno degli strumenti più utili di tutti nell'arsenale di resilienza IT di IBM è IBM Cyber Vault.

IBM Cyber Vault è una metodologia di sicurezza per il ripristino rapido in seguito a un attacco informatico. Si basa su IBM Safeguarded Copy, una tecnologia per la creazione regolare di snapshot isolati e immutabili. Cyber Vault analizza questi snapshot cercando modifiche potenzialmente dannose, che potrebbero indicare la presenza di ransomware. IBM Cyber Vault è inoltre integrato con IBM QRadar e IBM Storage Insights per un rilevamento ancor più rapido. La sua convalida di copie immutabili consente agli amministratori di individuare rapidamente una buona copia, testarla e poi effettuare il ripristino a partire da quella.

In termini di velocità, in particolare IBM Cyber Vault aiuta gli storage administrator in:

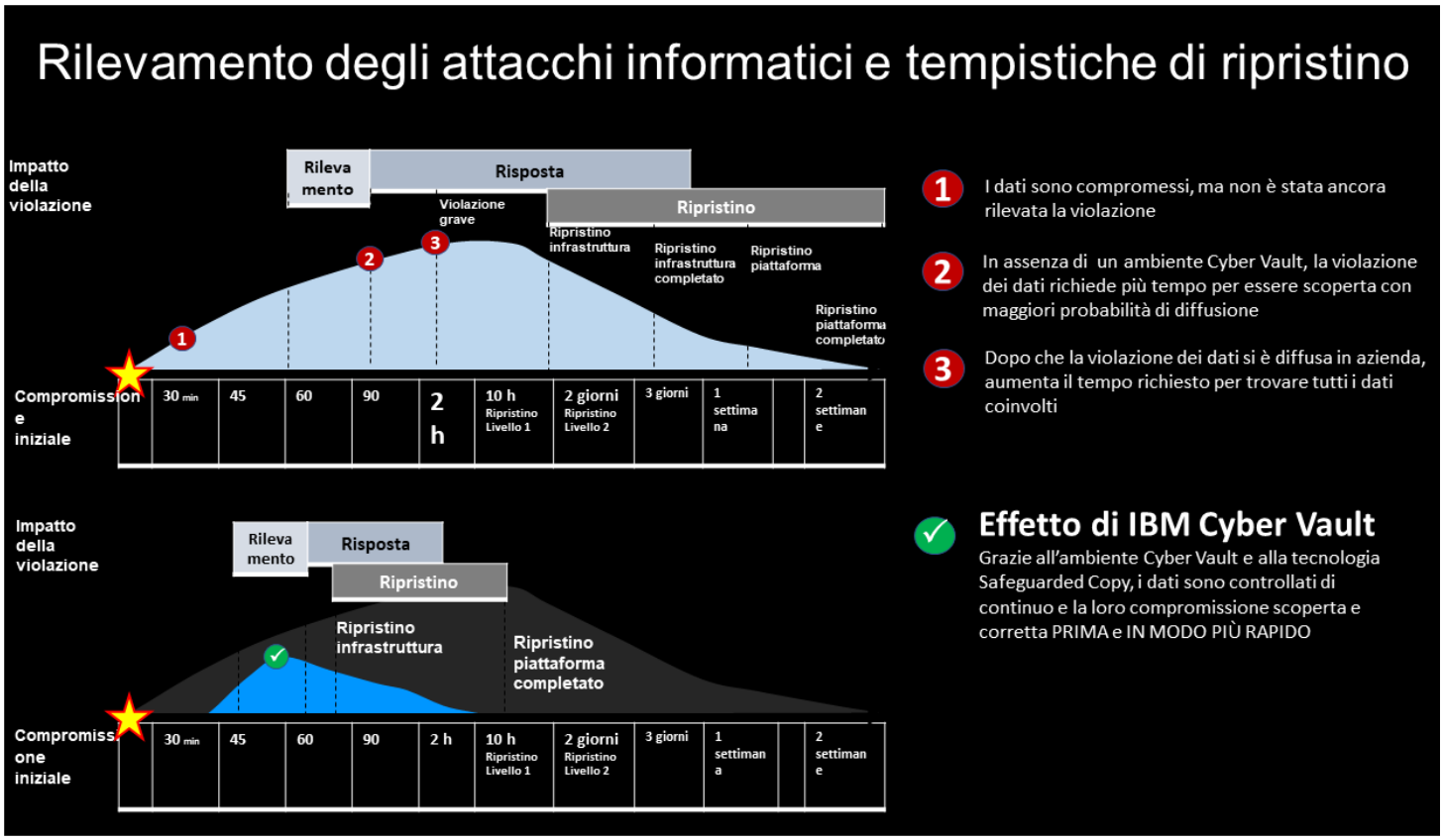
- Individuazione: l'integrazione di QRadar e Storage Insights offre rilevamento e monitoraggio migliori.

- Mitigazione e quantificazione del danno: è un processo automatico. Il rilevamento automatico degli attacchi consente ovviamente un ripristino più rapido.

- Individuazione di una buona copia nota: l'automatizzazione delle copie di dati immutabili si verifica in caso di rilevamento di una minaccia.

- Ripristino delle operazioni: il ripristino rapido è possibile nell'arco di ore, non giorni o settimane (vedi Figura 3).

Figura 3. Come accelera il ripristino informatico IBM Cyber Vault?



Fonte: IBM

La grande verità

Le infrastrutture IT stanno diventando sempre più complesse, con conseguente aumento delle probabilità di errori umani, guasti ai sistemi o negligenza. Allo stesso tempo i malintenzionati, interni ed esterni all'azienda, sono incessantemente alla ricerca di punti deboli da sfruttare.

Senza dubbio, degli incidenti informatici si verificheranno. E ciò dovrebbe imporre un cambiamento nell'approccio organizzativo, che passerebbe da reattivo a proattivo, dall'energico tentativo di impedire un attacco alla preparazione e alla risposta a guasti inerenti alla sicurezza *nel caso in cui* questi si verificassero. Si tratta di ciò che devono garantire le aziende che si occupano di trasformazione e del passaggio da sicurezza a resilienza IT.

Molte aziende stanno creando modelli di strategia di resilienza IT in seguito alle indicazioni fornite dal NIST Cybersecurity Framework secondo cui si devono individuare le risorse nevralgiche, proteggerle, rilevare i guasti e le violazioni, oltre a pianificare la risposta e il ripristino in seguito a incidenti informatici. Aziende leader nel loro settore stanno prestando particolare attenzione alle funzionalità delle infrastrutture IT che possano migliorare la loro resilienza IT mediante data discovery, gestione delle copie, crittografia, controllo degli accessi e storage immutabile, pur mantenendo numerose opzioni di ripristino dati.

Per i responsabili IT e delle aziende, la resilienza IT consiste nel prendere le giuste decisioni tecnologiche e di business, tenendo a mente l'obiettivo di mantenere l'operatività.

Enterprise Strategy Group è una società di tecnologia, analisi, ricerca e strategia integrate che fornisce analisi di mercato, approfondimenti utili e servizi di contenuti go-to-market alla comunità IT globale.

www.esg-global.com contact@esg-global.com 508.482.0188