Complessivamente, l'organizzazione è:

esposta

Ripeti la valutazione

Rilevamento

Per quanto riguarda la protezione proattiva tramite le best practice di rilevamento, l'organizzazione è:

esposta

Guarda il video di riepilogo.

Cannot load video.
This video is unavailable

Risposta

Per quanto riguarda la risposta rapida ed efficace a incidenti informatici per limitare i danni/l'impatto negativo, l'organizzazione è:

esposta

Cannot load video.
This video is unavailable

Guarda il video di riepilogo.

Ripristino

Per quanto riguarda il ripristino dei dati e la ripresa delle operazioni in seguito a incidenti informatici, l'organizzazione è:

esposta

Cannot load video.
This video is unavailable

Guarda il video di riepilogo.

Report personalizzato sulla cyber-resilienza

Grazie per aver eseguito l'autovalutazione della cyber-resilienza di Dell Technologies proposta da ESG. L'obiettivo della valutazione è quello di comprendere il grado di vulnerabilità attuale dell'organizzazione rispetto a ransomware e altri attacchi informatici sofisticati, identificare le aree di vulnerabilità e spiegarti cosa fare per porre rimedio a tali rischi. A tal fine, valutiamo la preparazione dell'organizzazione in tre aree principali: rilevamento proattivo delle minacce, risposta agile alle minacce e completezza delle funzionalità di ripristino.

In base alle risposte fornite per la valutazione in ciascuna di queste aree, classifichiamo l'organizzazione come **esposta**. Questo è il tier di preparazione **minore** della valutazione. Nelle pagine seguenti viene spiegato perché l'organizzazione ha ricevuto tale valutazione e vengono forniti consigli da prendere in considerazione.

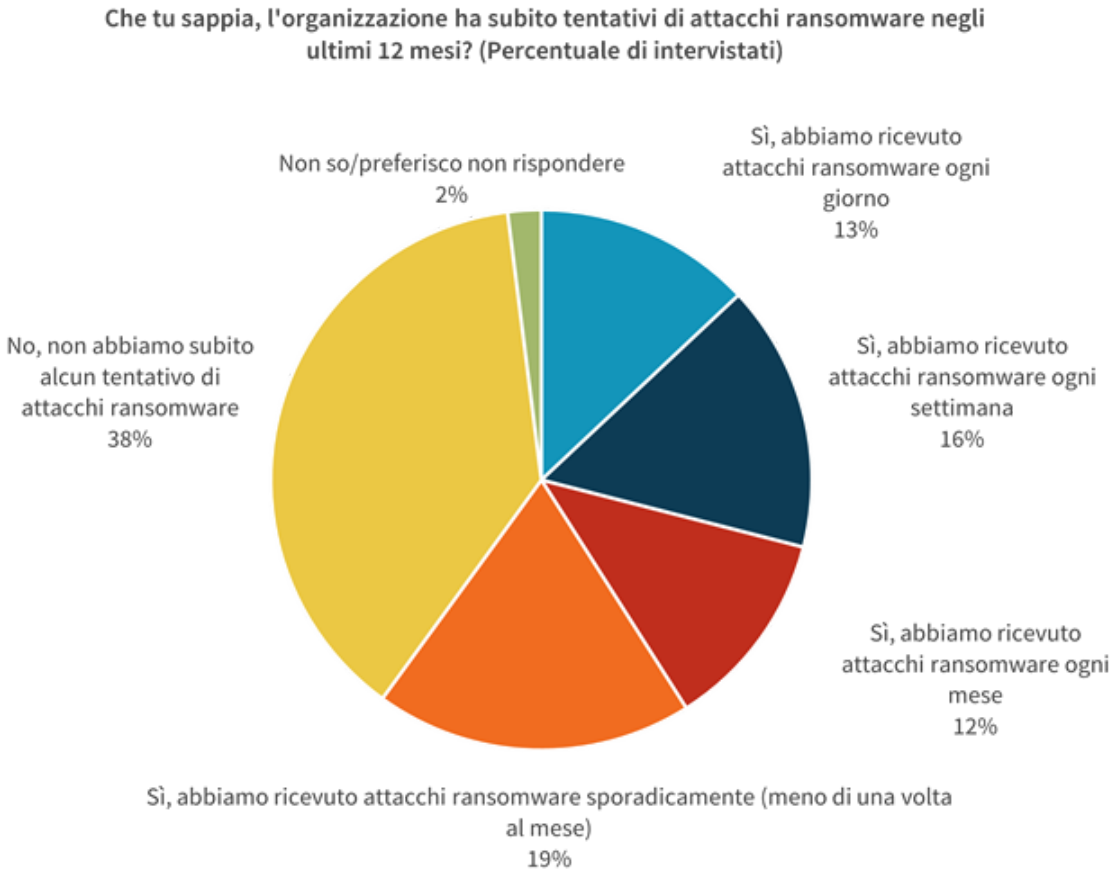
Rilevamento

Il primo pilastro della valutazione è incentrato sul rilevamento proattivo delle minacce, ovvero le tecnologie e i processi utilizzati in azienda per rilevare e prevenire gli attacchi informatici o gli incidenti legati a ransomware. Considerando solo questo

aspetto, l'organizzazione è stata classificata come **esposta**, il tier di preparazione **minore** della valutazione.

- **Per iniziare la valutazione, abbiamo chiesto su quali minacce si concentra il team. Questo è importante perché, come ha dimostrato la ricerca di ESG del 2020 sulle intenzioni di spesa, molte organizzazioni vengono costantemente travolte da ransomware e altre forme di attacchi informatici sofisticati (vedere la figura 1).** Il panorama di minacce diventa sempre più complesso e i criminali sfruttano vettori di attacco multipli per la compromissione e la violazione delle organizzazioni. Mentre la maggior parte delle organizzazioni assegna la priorità a ransomware e attacchi avanzati e in più fasi con movimento laterale, per molti le minacce interne, siano esse intenzionali o meno, sono oggetto di preoccupazione. È estremamente raccomandata l'implementazione di soluzioni per la sicurezza degli endpoint con protezione affidabile da ransomware, oltre a piani di risposta agli incidenti testati e strategie di backup affidabili con funzionalità per la protezione offline, come quelle consigliate da CISA. Se ti affidi a un fornitore di servizi per proteggere l'organizzazione, discutere questi aspetti è altamente consigliato.

Figura 1



Fonte: ESG

- **Inoltre, ti abbiamo chiesto di valutare la capacità dell'organizzazione di soddisfare gli obblighi di conformità.**

- **La valutazione ha affrontato l'utilizzo di framework di rischio nell'organizzazione per guidare il programma di sicurezza.**

- **In seguito, la valutazione ha affrontato la visibilità di endpoint, cloud e rete.**

- **Infine, la valutazione è stata incentrata sull'efficacia dei controlli utilizzati per prevenire attacchi ransomware nello specifico.**

Risposta

Il secondo pilastro della valutazione è incentrato sulla risposta agile alle minacce, ovvero le tecnologie e i processi utilizzati in azienda per rispondere rapidamente agli incidenti di sicurezza o ransomware, limitandone l'impatto. Considerando solo questo aspetto, l'organizzazione è stata classificata come **esposta**, il tier di preparazione **minore** della valutazione.

- **Ti abbiamo chiesto quale sarebbe la tua risposta più probabile in caso di attacco ransomware riuscito.**

- **In seguito, ti abbiamo chiesto quanto tempo, impegno e budget hai predisposto per la protezione delle copie dei dati secondari.**

- **Per quanto riguarda la preparazione alla risposta,**

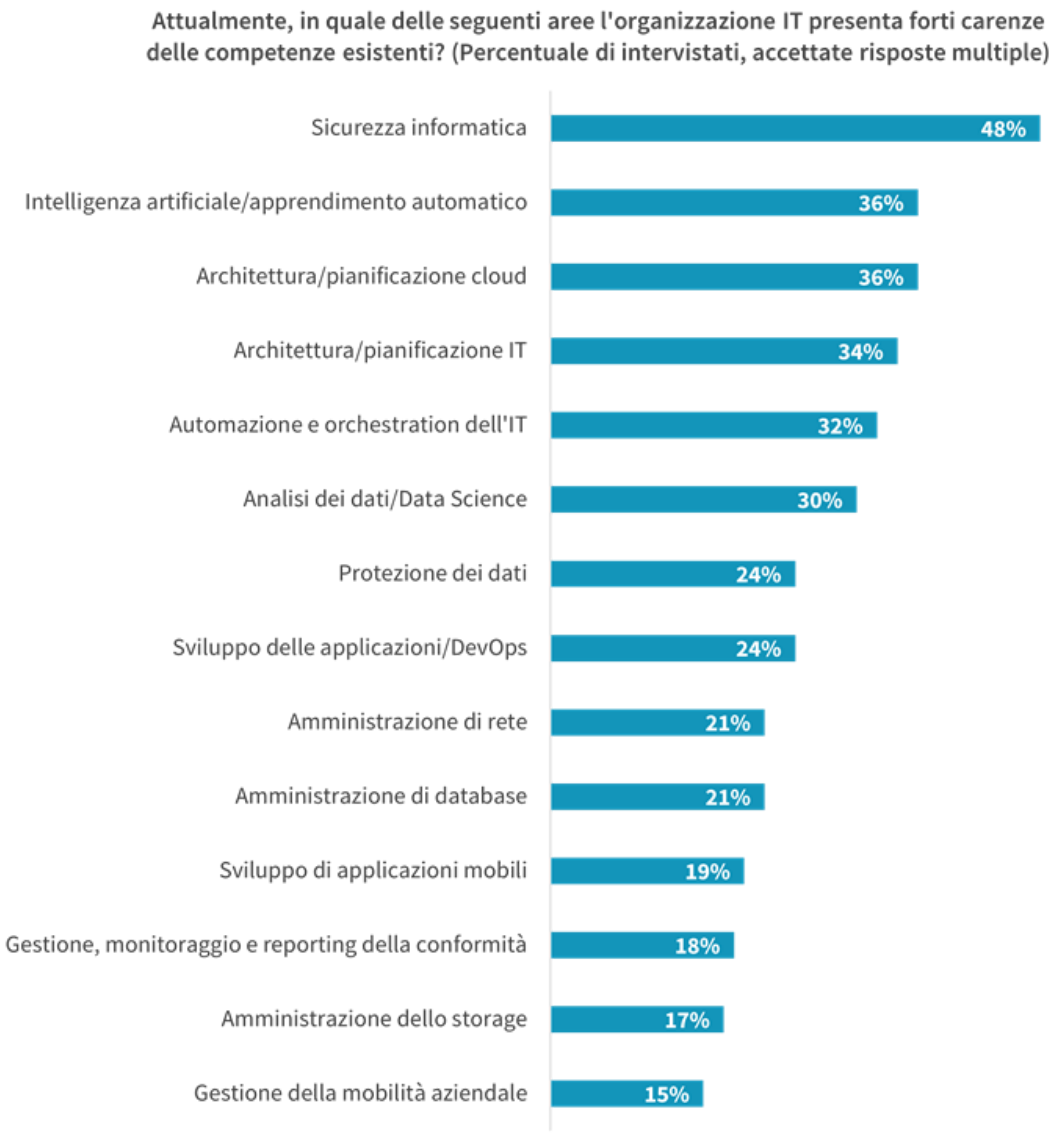
- **Passando alle azioni di preparazione specifiche, la valutazione assegna la priorità ad azioni quali la pianificazione degli incidenti e i test di ripristino.**

Ripristino

Il terzo e ultimo pilastro della valutazione è incentrato sulla completezza delle funzionalità di ripristino, ovvero le tecnologie e i processi utilizzati in azienda per ripristinare tutti i dati e rendere possibile la ripresa delle normali operazioni in modo rapido. Considerando solo questo aspetto, l'organizzazione è stata classificata come **esposta**, il tier di preparazione **minore** della valutazione.

- **Fare affidamento alle persone giuste per ripristinare la situazione in seguito ad attacchi informatici è fondamentale.**

Figura 2



Fonte: ESG

- **Ti abbiamo chiesto quanti dati ritieni di essere in grado di ripristinare in caso di attacco.**
- **La valutazione affronta l'investimento in infrastrutture isolate o air-gapped per le copie di dati critici da parte dell'organizzazione.**
- **Infine, che l'organizzazione disponga di un'infrastruttura isolata o meno, ti abbiamo chiesto in che misura ritieni che occorra proteggere i dati in questo tipo di ambiente.**

In che modo Dell Technologies può essere d'aiuto

Dell Technologies si impegna a consolidare la fiducia e a rendere il mondo sicuro e connesso. Lavoriamo duramente per fare della sicurezza dei dati, della rete, dell'organizzazione e dei clienti la nostra priorità, integrando la cyber-resilienza e la sicurezza end-to-end in tutti i prodotti, soluzioni e servizi. Con le soluzioni di sicurezza degli endpoint di Dell e VMware Carbon Black Cloud, i dispositivi

affidabili Dell e Dell EMC PowerProtect Cyber Recovery, ti offriamo gli strumenti per creare e mantenere la sicurezza e la resilienza dell'organizzazione anche con l'avvento di nuove minacce.

In base alla valutazione e al punteggio attuale, ti forniamo i consigli principali per migliorare la resilienza. Il Centro sicurezza e affidabilità Dell Technologies offre facile accesso a risorse e soluzioni aggiuntive che rispondono rapidamente alle tue domande sulla sicurezza aziendale e consumer.

Dall'edge al core fino al cloud, con i nostri esperti del settore ricevi assistenza strategica e funzionalità pratiche comprovate per proteggere l'azienda e preservare la reputazione da minacce informatiche: affidati a Dell Technologies.

In che modo Dell contribuisce a migliorare le tue capacità di rilevamento:

- Sicurezza degli endpoint e dispositivi: il numero di utenti finali che lavorano in remoto e in viaggio è aumentato in misura esponenziale. Con le attuali violazioni che vanno ben oltre il sistema operativo, occorrono soluzioni intelligenti che impediscono, rilevano e rispondono alle minacce ovunque si presentino.
- VMware Carbon Black™ Cloud: i criminali informatici aggiornano costantemente le tattiche e oscurano le proprie azioni all'interno di strumenti e processi comuni. È necessaria una piattaforma di endpoint tramite cui individuare le fluttuazioni minori dietro alle quali si celano attacchi malevoli e adattare la prevenzione di conseguenza.
- Resilienza proattiva di PowerEdge: integra la fiducia nella Digital Transformation con l'infrastruttura progettata per interazioni sicure e la capacità di prevedere potenziali minacce.

In che modo Dell contribuisce a migliorare le tue capacità di risposta:

- Managed Detection and Response: Managed Detection and Response, con tecnologia SecureWorks® Taegis™ XDR, sfrutta analisi e competenze avanzate per analizzare potenziali compromissioni e garantire correzioni qualora vengano individuate delle minacce.
- Servizi di resilienza aziendale: con Dell Technologies Services le organizzazioni diventano altamente resilienti, mentre il business si basa maggiormente su servizi IT basati sul cloud e aumentano le pressioni da parte delle entità interessate e delle autorità di regolamentazione.
- Servizi di Cyber Recovery: grazie a Dell Technologies Services, le organizzazioni incrementano la propria cyber-resilienza attraverso il programma olistico di ripristino informatico che riunisce tecnologia, processi e persone per formare l'ultima linea di difesa per l'organizzazione.

In che modo Dell contribuisce a migliorare il ripristino in seguito ad attacchi:

- PowerProtect Cyber Recovery: PowerProtect Cyber Recovery protegge e isola i dati critici da ransomware e altre minacce sofisticate, in modo da recuperare i dati integri noti e riprendere con sicurezza le normali operazioni aziendali.
- Servizi di resilienza aziendale: con Dell Technologies Services le organizzazioni diventano altamente resilienti, mentre il business si basa maggiormente su servizi IT basati sul cloud e aumentano le pressioni da parte delle entità interessate e delle autorità di regolamentazione.
- PowerScale con Superna Eyeglass Ransomware Defender: Superna Eyeglass® Ransomware Defender è la soluzione di elaborazione degli eventi in tempo reale altamente scalabile che utilizza l'analisi del comportamento utente per rilevare e arrestare gli attacchi ransomware.