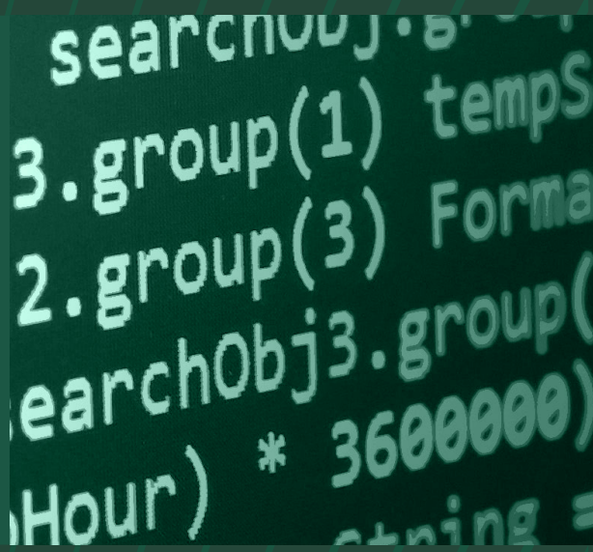
DELL Technologies

5 Raccomandazioni per superare con successo un attacco ransomware



1 Mantieni un piano di risposta completo agli incidenti

Concentrati nel ridurre al minimo l'impatto di un attacco

Esercitati, effettua dei test e tieniti aggiornato costantemente

Preparati per tempo a disporre di un team di risposta agli incidenti, già pronto e attivo prima che si verifichi l'incidente

Considera l'assicurazione informatica come parte integrante della strategia complessiva di resilienza

Includi piani di collaborazione con le forze dell'ordine

2 Adotta una strategia di comunicazione chiara

Crea modelli di comunicazione in anticipo

Garantisci comunicazioni chiare e tempestive all'interno dell'organizzazione

Preparati a comunicare all'esterno, se applicabile

Rispetta le normative di notifica applicabili

3 Garantisci una protezione dei dati solida

Proteggi i dati critici in un data vault isolato, immutabile e autosufficiente

Dai priorità al recupero in base al servizio/all'infrastruttura

Esercitati nella recuperabilità

Associa funzionalità come camere bianche al Recovery Time Objective

Garantisci 'integrità dei dati recuperabili

4 Non dare per scontato un ritorno immediato alla normalità

Il pagamento di un riscatto dovrebbe essere l'ultima spiaggia

Prima di procedere con il pagamento, assicurati che i requisiti richiesti dalle normative vigenti siano rispettati.

Non c'è garanzia che l'hacker ti restituirà i tuoi dati anche dopo il pagamento del riscatto

5 Enfatizza la formazione e l'istruzione

Esegui simulazioni degli attacchi

Monitora e testa le pratiche di sicurezza dei dipendenti

Utilizza strumenti come test di phishing e formazione sulla sicurezza della posta elettronica

Non è più una questione di "se" ma di "quando".

Le aziende devono pianificare come se un attacco fosse inevitabile, nonostante le loro migliori difese. Per discutere cosa fare in caso di emergenza, Jim Shook, Global Director of Cybersecurity and Compliance Practice e Steven Granat, Principal Consultant, soluzioni per la sicurezza informatica e partnership strategiche, ha incontrato Brian White, Senior Consultant, Product Marketing, per Dell Data Protection.

> È fondamentale selezionare le persone giuste e condurre azioni di esercitazione e simulazione. In questo modo, quando si verifica un attacco, tutte le persone coinvolte sapranno immediatamente cosa fare.
>
> ***Steven Granat**, Principal Consultant,*
> *soluzioni per la sicurezza informatica e partnership strategiche, Dell Technologies*

Mantieni un piano di risposta completo agli incidenti

Quando si verifica un attacco, tutte le principali entità interessate, praticamente ogni persona all'interno dell'organizzazione e anche terze parti come i fornitori, devono sapere cosa fare. Il piano di risposta agli incidenti dovrebbe essere redatto per iscritto e contenere una chiara sequenza di azioni da intraprendere in caso di incidente, consiglia Shook. Un piano completo prenderà in considerazione tutte le fasi tecnologiche, di processo e di comunicazione, dall'azione immediata fino alla fase di recupero. Assicurati di conservare anche un documento cartaceo, poiché le modalità di comunicazione digitali potrebbero non essere operative. "C'è bisogno di un piano che possa letteralmente essere tirato giù dallo scaffale", afferma Granat.

Adotta una strategia di comunicazione chiara

La maggior parte delle organizzazioni dovrà comunicare con le principali entità interessate e, in molti casi, dovrà rispettare i requisiti richiesti dalle normative vigenti. Crea diversi modelli per le comunicazioni interne ed esterne con istruzioni sistematiche su chi notificare, in quale sequenza e quando. Preparati all'eventualità che i sistemi telefonici e quelli di posta elettronica possano non funzionare per un certo periodo di tempo.

Implementa una solida strategia di protezione dei dati

Uno degli obiettivi chiave nel superare un attacco ransomware consiste nel ripristinare i dati e recuperarli nel modo più indolore possibile, evitando al contempo di pagare il riscatto. Una solida strategia di protezione dei dati è una parte fondamentale del raggiungimento di tali obiettivi, ma dovrà comprendere sia la tecnologia sia i processi. "Bisogna utilizzare dati immutabili e cyber vault per archiviare una quantità sufficiente di dati, che siano affidabili, almeno come punti di convalida, che consentano di recuperare i sistemi", consiglia Swook. Assicurarsi che i dati siano protetti è il primo passo; per recuperarli è necessario disporre anche di persone e processi. Gli esperti di terze parti possono offrire supporto, ma è necessario coinvolgerli nella fase di pianificazione.

Non dare per scontato ritorno immediato alla normalità, anche nel caso in cui si decida di pagare il riscatto

Il pagamento di un riscatto, che deve essere considerato solo come ultima spiaggia, non garantisce che tutto tornerà alla normalità immediatamente. Ricorda che stai negoziando con un criminale e, anche se dovessi ottenere i codici di decodifica, avrai bisogno di una strategia per i dati appena recuperati. Per prima cosa, è necessario testare i dati decrittografati e ricostruire tutti i sistemi in modo metodico. Prestare meticolosamente attenzione agli eventi "what-if" prima ancora che un attacco sarà di grandissimo aiuto per raggiungere la resilienza. "Capire le diverse applicazioni e dipendenze dell'infrastruttura tecnologica è cruciale per un ritorno efficace allo stato di stabilità. Ho una fonte di recupero valida e un target recuperabile? Ho dei dati privi di compromessi? Queste sono considerazioni importanti su cui riflettere", afferma Granat.

Nella fase di recupero, bisogna inoltre assicurarsi che il nemico sia realmente uscito dai sistemi. "È necessario assicurarsi l'incendio sia stato domato e scoprire cosa ha iniziato a prendere fuoco in primo luogo, perché senza queste due informazioni critiche, si resta vulnerabili ai futuri attacchi", afferma Swook.

La formazione e la pratica sono fondamentali

Una parte importante della cyber-resilienza è la formazione completa, che va dal garantire che i dipendenti seguano una solida pratica di sicurezza informatica fino all'esecuzione regolare del piano di recupero. "È fondamentale selezionare le persone giuste e condurre azioni di esercitazione e simulazione. In questo modo, quando si verifica un attacco, tutte le persone coinvolte sapranno immediatamente cosa fare", afferma Swook.

Il ransomware può essere inevitabile nel panorama delle minacce attuali, ma attraverso la pianificazione e l'esecuzione è possibile ridurre al minimo l'impatto operativo, finanziario e di reputazione. Lo scopo è quello di ritornare alla normalità nel minor tempo possibile e nel modo più indolore possibile.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**

DELL Technologies