DELL Technologies

Ransomware: rafforzare la sicurezza informatica e la resilienza con Dell Technologies

Che cos'è il ransomware?

Il ransomware è un tipo di software malevolo (malware) che blocca l'accesso a un sistema informatico o ai dati fino a quando non viene pagato un riscatto. È uno degli attacchi informatici in grado di causare più danni potenziali. L'anno scorso, il 50% delle organizzazioni a livello globale è stato colpito da ransomware almeno una volta. Il downtime medio dopo un attacco ransomware è di tre settimane, il che determina una significativa interruzione delle operazioni

Ransomware, una minaccia crescente

Il ransomware è un tipo di software malevolo (malware) che blocca l'accesso a un sistema informatico o ai dati fino a quando non viene pagato un riscatto. È uno degli attacchi informatici in grado di causare più danni potenziali. L'anno scorso, il 50% delle organizzazioni a livello globale è stato colpito da ransomware almeno una volta. Il downtime medio dopo un attacco ransomware è di tre settimane, il che determina una significativa interruzione delle operazioni.

Come funziona un attacco ransomware

Il ransomware di solito infetta le organizzazioni quando qualcuno fa clic su un link malevolo, apre un allegato infetto o visita un sito web compromesso. Il malware penetra così nei sistemi e crittografa i file rendendoli illeggibili. A questo punto, di solito, il programma ransomware visualizza un messaggio che richiede un pagamento (quasi sempre in criptovaluta) in cambio di una chiave di decrittografia. Se il riscatto non viene pagato, l'autore dell'attacco minaccia di eliminare o divulgare i dati. Un esempio spesso citato di attacco ransomware è quello di WannaCry, lanciato nel 2017 e diffusosi rapidamente in tutto il mondo. Ne sono stati vittima ospedali, aziende e agenzie governative, che hanno subito enormi perdite finanziarie. L'impatto economico globale del virus WannaCry è stato valutato da Cyber Risk Management (CyRiM) e Lloyd's of London tra i quattro e gli otto miliardi di dollari, con oltre 200.000 sistemi interessati in 150 Paesi nell'arco di pochi giorni.

Due delle principali società a livello globale ad essere colpite sono state FedEx, che ha riportato una perdita di $ 300 milioni dovuta a interruzioni del servizio e pulizia dei sistemi, e Renault-Nissan, che ha dovuto interrompere temporaneamente la produzione in diversi stabilimenti. I costi nascosti di un attacco ransomware possono essere numerosi e comprendono:

- Downtime e perdita di produttività dell'azienda
- Danni alla reputazione
- Costo del ripristino e della correzione di sicurezza dei sistemi
- Sanzioni legali e normative

Di fronte a un attacco ransomware, è necessario che le aziende agiscano nel modo seguente;

- Non pagare, a meno che non sia assolutamente necessario. Non ci sono infatti garanzie che gli autori dell'attacco ripristinino l'accesso ai dati.
- Ripristinare i dati da un backup, se disponibile.
- Segnalare l'attacco alle autorità competenti.
- Rafforzare le difese per prevenire future infezioni (ad esempio, mantenere aggiornato il software, istruire il personale, utilizzare protezioni per gli endpoint).

Contrasto agli attacchi ransomware con Dell Technologies

Dell Technologies fornisce alle organizzazioni strumenti completi e all'avanguardia, progettati per contrastare i rischi degli attacchi ransomware prima che causino danni.

Maggiore sicurezza degli endpoint con Dell Trusted Device

Gli endpoint sono spesso i principali punti di ingresso per gli attacchi ransomware e pertanto la sicurezza degli endpoint è un'area di interesse cruciale. I dispositivi Dell Trusted Devices integrano funzionalità di protezione abilitate per l'hardware e proteggono i sistemi senza comprometterne le prestazioni. Soluzioni come Dell SafeBIOS e SafeID rafforzano i dispositivi endpoint contro l'accesso non autorizzato, mentre Dell SafeData crittografa i dati per proteggere le informazioni sensibili anche all'esterno del firewall aziendale. Attraverso l'integrazione della sicurezza direttamente nei dispositivi, le aziende implementano una protezione a livello di hardware, che riduce le opportunità per i cybercriminali di stabilire un punto di appoggio da cui lanciare l'attacco.

Rilevamento proattivo con CrowdStrike

Evitare gli attacchi ransomware è possibile se le organizzazioni utilizzano gli strumenti giusti per rilevare e rispondere alle minacce in tempo reale. CrowdStrike, una delle soluzioni del portafoglio Dell, fornisce una piattaforma di protezione degli endpoint di nuova generazione basata sull'AI e sull'analisi comportamentale. Questa tecnologia identifica e neutralizza le attività sospette prima che si trasformino in un attacco vero e proprio. Grazie all'integrazione ottimale di CrowdStrike nell'infrastruttura Dell, i team IT mantengono la visibilità sull'intero ambiente e forniscono una risposta immediata ed efficace alle minacce.

Protezione dei dati completa con Dell PowerProtect

Le soluzioni Dell PowerProtect sono la colonna portante della resilienza ai ransomware. Questi strumenti avanzati sono progettati per proteggere i dati aziendali da minacce interne ed esterne. Funzionalità come i backup immutabili garantiscono che i dati non possano essere modificati, eliminati o crittografati dai ransomware e creano una rete di sicurezza affidabile anche in caso di attacchi sofisticati. Dell PowerProtect Cyber Recovery Vault, ad esempio, isola i dati critici dalla rete attraverso la tecnologia air-gap, che li mantiene al sicuro anche durante le violazioni più avanzate. Rilevamento automatizzato delle anomalie e flussi di lavoro intelligenti sono strumenti a disposizione delle organizzazioni per individuare tempestivamente le attività malevole e rispondere prima che il ransomware si diffonda.

Sicurezza di rete avanzata e microsegmentazione con Dell PowerSwitch Networking e SmartFabric OS

Rafforza le difese dagli attacchi zero-day attraverso una segmentazione avanzata della rete, rigorosi controlli degli accessi e analisi del traffico in tempo reale nell'intera infrastruttura.

Ripristino efficiente con Dell Data Protection Services

Dell è consapevole che, sebbene la prevenzione sia essenziale, il ripristino è un aspetto altrettanto importante della risposta a un attacco ransomware. Oltre a soluzioni automatizzate di backup e ripristino, Dell Data Protection Services offre anche la consulenza di esperti per garantire alle aziende di eseguire rapidamente il ripristino e ridurre al minimo il downtime. Servizi come Remote Data Recovery e Incident Response garantiscono alle organizzazioni il supporto di cui hanno bisogno durante i momenti di maggior crisi. Questo approccio completo garantisce l'integrità dei dati e la riduzione dei tempi di ripristino e previene le interruzioni operative.

Questi sono solo alcuni esempi di soluzioni del portafoglio Dell che aiutano a contrastare minacce alla sicurezza interne.

Forza che nasce dalla collaborazione

L'approccio collaborativo estende la protezione delle soluzioni Dell oltre la tecnologia proprietaria di Dell. Attraverso partnership con le principali aziende di sicurezza informatica come CrowdStrike e Secureworks, Dell offre un ecosistema di soluzioni integrate in grado di contrastare ogni possibile vettore di attacco. Insieme, queste soluzioni forniscono sicurezza end-to-end poiché le aziende creano difese multilivello, su misura per il proprio specifico profilo di rischio.

Perché scegliere Dell?

Dell Technologies è molto più di un fornitore di tecnologia: è un partner di fiducia nella lotta al ransomware. Attraverso la combinazione di innovazione, competenze e impegno per rafforzare le difese delle aziende, Dell fornisce alle organizzazioni gli strumenti e la fiducia necessari per rispondere a minacce sempre più evolute. Che si tratti di proteggere endpoint e dati critici o abilitare il ripristino rapido di dati e sistemi, i prodotti e i servizi Dell garantiscono continuità operativa e tranquillità.

Creare un futuro resiliente

Gli attacchi ransomware continuano a evolversi, ma con Dell Technologies le aziende restano sempre un passo avanti. Con l'utilizzo di hardware, software e servizi avanzati, le organizzazioni creano un framework di sicurezza informatica resiliente, adattabile e affidabile. Le aziende proteggono i dati e le operazioni e rendono il business di oggi a prova di futuro scegliendo le soluzioni complete Dell contro il ransomware.

Per garantire la resilienza delle operazioni, è fondamentale comprendere l'attuale panorama delle minacce e rimanere informati sulle minacce emergenti. Gli esperti di sicurezza informatica di Dell Technologies monitorano costantemente la presenza di nuovi vettori di attacco (come lo chiamiamo?) e lavorano per contrastare in modo proattivo potenziali vulnerabilità nei nostri prodotti e servizi. In questo modo la protezione che offriamo è sempre aggiornata contro le minacce ransomware in continua evoluzione.

Oltre a rimanere informati, è essenziale anche che le aziende seguano un approccio multi-livello alla sicurezza, che significa implementare una serie di misure di sicurezza come firewall, software antimalware, sistemi di rilevamento delle intrusioni e backup dei dati. Attraverso la diversificazione delle strategie di difesa, l'impatto di qualsiasi attacco viene ridotto al minimo e l'azienda resta operativa anche in seguito a un tentativo di ransomware riuscito.

È inoltre importante testare e aggiornare regolarmente le misure di sicurezza (applicare patch ai sistemi e aggiornare le policy). Gli hacker trovano modi sempre nuovi di aggirare le misure di sicurezza tradizionali ed è perciò essenziale che le aziende restino vigili testando regolarmente le proprie difese e aggiornandole se necessario. Ad esempio, è importante eseguire periodicamente valutazioni delle vulnerabilità, test di penetrazione e gestione delle patch.

Un altro aspetto chiave per proteggere l'azienda dal ransomware è istruire i dipendenti sulle best practice di sicurezza informatica. Molti attacchi ransomware vengono avviati mediante l'uso di tattiche di social engineering come e-mail di phishing o link malevoli. È perciò importante istruire i dipendenti su come individuare ed evitare queste minacce per ridurre notevolmente la probabilità che un attacco venga portato a termine.

Anche la disponibilità di un piano di ripristino di emergenza riduce notevolmente le conseguenze di un attacco ransomware. Un piano efficace include backup regolari dei dati e dei sistemi più importanti, nonché una procedura chiaramente definita di risposta a un attacco e di esecuzione di un ripristino.

Oltre a queste misure proattive, è importante anche disporre di un solido piano di risposta agli incidenti. A tale scopo, è importante definire chiaramente ruoli e responsabilità per la gestione di un attacco ransomware, così come predisporre protocolli di comunicazione per avvisare le entità interessate e mitigare i danni.

Infine, rimanere informati sulle tendenze e sugli sviluppi più recenti degli attacchi ransomware aiuta a conservare una posizione di vantaggio rispetto alle potenziali minacce. È buona abitudine consultare regolarmente i report di settore e gli aggiornamenti degli esperti di sicurezza e implementare in modo proattivo nuove misure di sicurezza per proteggere la propria azienda.

Anche se nessuna azienda può dirsi immune agli attacchi ransomware, con le strategie e gli strumenti idonei, il rischio e l'impatto di tali attacchi si riduce drasticamente. Adottare un approccio proattivo alla sicurezza informatica significa non solo proteggere la propria azienda ma anche guadagnare la fiducia dei clienti e delle altre entità interessate.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi alla pagina **Dell.com/SecuritySolutions**

Scopri di più sulle soluzioni Dell

Contatta un esperto Dell Technologies

Visualizza più risorse

Partecipa alla conversazione con #HashTag

DELL Technologies