DELL Technologies

Zero-day: rafforzamento della sicurezza informatica e della resilienza con Dell Technologies

La crescente minaccia degli attacchi zero-day

Gli attacchi zero-day si sono rapidamente trasformati in una delle sfide più impegnative nel panorama odierno della sicurezza informatica. Questi attacchi sfruttano vulnerabilità sconosciute ai fornitori di software e agli esperti di sicurezza, lasciando le aziende impreparate ed esposte. Le organizzazioni di tutti i settori, dal settore sanitario a quello finanziario, sono vulnerabili a tali violazioni, che spesso comportano gravi conseguenze finanziarie e operative.

Il ritmo della trasformazione digitale sta accelerando e gli attacchi zero-day sono diventati più frequenti e sofisticati. Non c'è mai stata così tanta necessità di protezioni solide. Dell Technologies comprende la natura critica di questa minaccia e fornisce alle aziende difese innovative e scalabili per combattere e ripristinare efficacemente gli attacchi zero-day.

Che cosa sono gli attacchi zero-day?

Un attacco zero-day comporta sfrutta una vulnerabilità di sicurezza non rivelata nel software o nell'hardware prima che sia disponibile una patch o una correzione. Gli autori di attacchi sfruttano la finestra di opportunità, causando spesso interruzioni diffuse prima che la vulnerabilità venga individuata e risolta.

Come funzionano gli attacchi zero-day

1. **Individuazione di vulnerabilità:** gli hacker identificano difetti di codifica o backdoor nascosti all'interno di applicazioni software o sistemi.
2. **Sviluppo di exploit:** il malware viene creato per sfruttare la vulnerabilità. Gli autori di attacchi potrebbero utilizzare campagne di phishing mirate o siti web carichi di malware per fornire l'exploit.
3. **Esecuzione di un attacco:** l'exploit viene implementato, compromettendo il sistema e potenzialmente consentendo il furto di dati o interferenze operative.

Tecniche comuni

- I drive-by-download inducono gli utenti a installare inconsapevolmente malware.
- Le e-mail di phishing distribuiscono link o payload dannosi per sfruttare le vulnerabilità.
- Gli attacchi fileless eludono il rilevamento eseguendo operazioni interamente nella memoria di un sistema.

Questi vettori di attacco altamente avanzati rendono gli attacchi zero-day particolarmente pericolosi, in quanto i tradizionali strumenti di rilevamento basati su firma spesso non li riconoscono.

Impatto sulle aziende

Gli attacchi zero-day comportano rischi significativi a causa della loro imprevedibilità e del ritardo nel rilevamento. Le conseguenze possono essere catastrofiche su diversi fronti.

Perdite finanziarie

Un attacco zero-day riuscito può comportare costi elevati, dalle sanzioni normative alla perdita di entrate durante il downtime. Ad esempio, una vulnerabilità non identificata sfruttata in una piattaforma di e-commerce potrebbe disabilitare il processo di pagamento, con un impatto diretto sulle vendite.

Conseguenze sulla reputazione

La percezione pubblica di un'azienda può essere irreparabilmente danneggiata. I clienti perdono fiducia quando vengono esposte informazioni sensibili o i servizi non funzionano.

Interruzione operativa

Le vulnerabilità non risolte spesso paralizzano i sistemi, con conseguente riduzione della produttività, ritardi nei progetti e opportunità di business perse.

Esempio del mondo reale

Un importante fornitore di servizi sanitari è stato vittima di un attacco zero-day che ha preso di mira software per dispositivi medici senza patch. L'attacco ha interrotto le operazioni chiave, ha esposto i dati dei pazienti ed è costato all'organizzazione **milionI** in spese di ripristino, erodendo al contempo la fiducia dei pazienti.

Statistiche allarmanti

Secondo uno studio di Ponemon del 2023, la percentuale di violazioni zero-day è di circa l'80%

Gli attacchi zero-day rappresentano costantemente oltre il **70%** delle vulnerabilità sfruttate

Fonte: 2024: IMandiant "M-Trends"

Combattere gli attacchi zero-day con Dell Technologies

Dell Technologies offre soluzioni leader del settore per aiutare le aziende a proteggersi attivamente dagli attacchi zero-day, promuovendo al contempo un ripristino rapido dopo tali violazioni.

Soluzioni di sicurezza per server e storage

Le soluzioni Dell per la sicurezza di server e storage offrono livelli aggiuntivi di protezione:

- I server protetti monitorano e bloccano i tentativi di accesso non autorizzati.
- I sistemi di backup e ripristino dei dati garantiscono che, anche nello scenario peggiore, le informazioni critiche rimangano accessibili e intatte.

Endpoint rafforzati con Dell Trusted Device

Gli endpoint sono un punto di ingresso chiave per gli autori di attacchi. I Dell Trusted Device integrano misure di sicurezza avanzate, garantendo la protezione degli endpoint contro le minacce non rilevate.

- **SafeBIOS** protegge il firmware dalla manipolazione, garantendo l'integrità del sistema da zero.
- **SafeID** protegge le credenziali utente proteggendo i processi di autenticazione.
- **SafeData** crittografa i dati sensibili inattivi e in transito, rendendoli inutili in caso di intercettazione o sfruttamento.

Rilevamento proattivo delle minacce con CrowdStrike

CrowdStrike sfrutta l'analisi avanzata e l'AI per monitorare l'attività degli endpoint, rilevando comportamenti insoliti che potrebbero indicare exploit zero-day. Il rilevamento proattivo delle minacce garantisce una risposta rapida prima che le vulnerabilità possano causare danni diffusi.

Ad esempio, un provider di telecomunicazioni che utilizza CrowdStrike è stato in grado di rilevare tempestivamente anomalie nel traffico di rete, mitigando un potenziale exploit zero-day sui server dei clienti.

Soluzioni Dell PowerProtect

Dell PowerProtect offre backup affidabili e immutabili e opzioni di ripristino isolate. Le aziende possono ripristinare le operazioni in modo rapido ed efficiente dopo un attacco zero-day, mantenendo la continuità aziendale e proteggendo i dati vitali dei clienti.

Ad esempio, una grande catena di vendita al dettaglio ha utilizzato PowerProtect per ripristinare i file crittografati compromessi da un attacco ransomware derivante da una vulnerabilità zero-day, evitando downtime prolungati.

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

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

L'importanza di un approccio alla sicurezza multilivello

La vera sicurezza richiede più di una soluzione. Una strategia multilivello combina tecnologia, processi e persone per formare un framework di protezione completo.

Azioni chiave per rafforzare la difesa

- **Adozione dei principi Zero Trust:** verifica ogni singolo utente e dispositivo che tenta di accedere alla rete.
- **Implementazione della crittografia avanzata:** utilizza i protocolli di crittografia per proteggere sia i dati in movimento che quelli inattivi.
- **Formazione dei dipendenti:** offri sessioni di formazione dettagliate per insegnare ai dipendenti come riconoscere i tentativi di phishing e le tattiche di social engineering.
- **Test periodici dei sistemi:** esegui test di penetrazione coerenti e scansioni delle vulnerabilità per garantire che le difese si adattino alle nuove minacce.

Dell Technologies abbina queste pratiche alle sue soluzioni di sicurezza avanzate, garantendo che le organizzazioni siano pronte a combattere efficacemente le vulnerabilità zero-day.

Partnership che rafforzano la sicurezza informatica

La collaborazione di Dell con i leader del settore **Microsoft**, **CrowdStrike** e **Secureworks** offre ai clienti l'accesso a strumenti e intelligence di sicurezza all'avanguardia.

- **Microsoft** si integra perfettamente con le soluzioni Dell per garantire la compatibilità a livello di sistema e meccanismi di protezione proattiva.
- **CrowdStrike** offre Threat Intelligence avanzata per gli endpoint per rilevare potenziali exploit zero-day.
- **SecureWorks** offre monitoraggio continuo e correzione da parte di esperti per risposte agli attacchi in tempo reale.

Utilizzo di Dell Professional Services

I Dell Professional Services offrono una gamma completa di consulenza, implementazione e assistenza per il ripristino, per aiutare le aziende ad affrontare e ridurre i rischi associati alle minacce zero-day. Dalla risposta agli incidenti alla pianificazione della roadmap per la sicurezza informatica, Dell aiuta le organizzazioni a raggiungere la resilienza a lungo termine.

Creazione di un futuro resiliente

Investire in Dell Technologies significa avere un partner che offra non solo una tecnologia superiore, ma anche la massima tranquillità. Grazie a soluzioni all'avanguardia, partnership strategiche e competenze ineguagliabili, Dell consente alle organizzazioni di prevedere, rilevare e ripristinare anche dagli attacchi zero-day più avanzati.

Contatta Dell Technologies oggi stesso per proteggere il tuo business e la tua reputazione e prosperare in un panorama digitale imprevedibile. Affidati a Dell per rafforzare il tuo futuro contro le minacce di domani.

Dell Technologies ispira fiducia, consentendo alle aziende di rimanere un passo avanti rispetto alle sfide degli attacchi zero-day in continua evoluzione attraverso soluzioni e servizi di sicurezza progettati per proteggere ciò che conta di più.

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