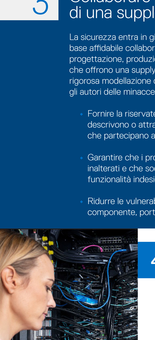
10 consigli per la sicurezza informatica

La tecnologia avanza a un ritmo rapidissimo e, mentre abbracciamo nuovi strumenti e sistemi che migliorano le nostre capacità, creiamo simultaneamente nuove opportunità per minacce informatiche che cercano di sfruttare le vulnerabilità. In questo contesto, è fondamentale implementare misure di sicurezza informatica efficaci che aiutino a proteggersi da queste minacce emergenti, garantendo che l'innovazione possa prosperare in un ambiente sicuro. Man mano che le organizzazioni si adattano ai nuovi rischi, gli esperti di sicurezza informatica di Dell Technologies consigliano 10 azioni fondamentali per il progresso della maturità della sicurezza informatica.

1 Comprendere il panorama dei rischi di minacce.

I partner esperti in materia di sicurezza informatica possono fornire preziose competenze e risorse che aiutano a orientarsi nel panorama delle minacce in rapida evoluzione.

- Condurre valutazioni approfondite delle vulnerabilità e test di penetrazione per identificare i potenziali punti deboli da affrontare e identificare eventuali lacune nella strategia.
- Sfruttare le competenze e conoscenze specializzate che potrebbero non essere disponibili internamente, come informazioni su rischi emergenti, tecniche di attacco avanzate e le più recenti strategie e best practice in materia di sicurezza.
- Definire i privilegi di accesso e le motivazioni, consentendo di stabilire il framework di sicurezza appropriato per l'implementazione dei controlli e della governance aziendale.



2 Creare una strategia completa per la sicurezza informatica.

Garantire la resilienza informatica richiede sforzi coordinati che coinvolgono team IT, professionisti della sicurezza informatica, responsabili della gestione e, in alcuni casi, esperti esterni.

- Promuovere il coinvolgimento dell'intera azienda: la sicurezza è responsabilità di tutti.
- Sfruttare l'automazione ove possibile.
- Assicurarsi di disporre di un piano IRR ben aggiornato che consenta a tutte le persone appropriate di sapere quando si verifica un attacco informatico.

3 Collaborare con i fornitori che dispongono di una supply chain protetta.

La sicurezza entra in gioco prima di quanto si possa immaginare. Garantire una base affidabile collaborando con i fornitori che danno priorità alla sicurezza nella progettazione, produzione e distribuzione di dispositivi e infrastrutture. I fornitori che offrono una supply chain protetta, un Secure Development Lifecycle e una rigorosa modellazione delle minacce possono contribuire a restare al passo con gli autori delle minacce.

- Fornire la riservatezza, l'integrità e la disponibilità delle informazioni che descrivono o attraversano la supply chain IT, nonché informazioni sulle parti che partecipano alla supply chain IT.
- Garantire che i prodotti o i servizi IT nella supply chain siano originali, inalterati e che soddisfino le specifiche dell'acquirente senza ulteriori funzionalità indesiderate.
- Ridurre le vulnerabilità che potrebbero limitare la funzione di un componente, portare a guasti o fornire opportunità di exploitation.

4 Adottare i principi Zero Trust.

Zero Trust è un concetto di sicurezza incentrato sulla convinzione che le organizzazioni non dovrebbero affidarsi automaticamente a nulla all'interno o all'esterno dei propri perimetri e devono invece verificare tutto ciò che cerca di connettersi ai propri sistemi prima di concedere l'accesso.

- Allontanarsi da un modello di sicurezza basato sul perimetro e adottare i principi di Zero Trust.
- Applicare il principio dei privilegi minimi, che prevede che gli account utente e di sistema abbiano solo i diritti di accesso minimi necessari per lo svolgimento delle rispettive attività. Questo approccio riduce la superficie di attacco e il potenziale impatto degli accessi non autorizzati da parte degli autori di attacchi.
- Integrare soluzioni come la micro-segmentazione, la gestione dell'identità e degli accessi (IAM), l'autenticazione a più fattori (MFA) e le analisi della sicurezza, per citarne alcune.

5 Ridurre la superficie di attacco.

La superficie di attacco è rappresentata da potenziali vulnerabilità e punti di ingresso che possono essere sfruttati da utenti malintenzionati. Per migliorare il profilo di sicurezza, le organizzazioni devono ridurre al minimo la superficie di attacco, mitigare i rischi e migliorare le difese informatiche complessive contro minacce nuove ed emergenti.

- Prevedere attività di formazione per dipendenti e utenti affinché riconoscano e segnalino potenziali minacce alla sicurezza, tentativi di phishing e tattiche di social engineering allo scopo di ridurre al minimo il rischio di successo degli attacchi che sfruttano le vulnerabilità degli utenti.
- Implementare misure preventive, come la segmentazione completa della rete, l'isolamento dei dati critici, l'applicazione di rigorosi controlli degli accessi e l'aggiornamento e l'applicazione di patch regolari su sistemi e applicazioni.
- Assicurarsi che i sistemi, le reti e i dispositivi siano correttamente configurati con best practice in termini di sicurezza, come la disabilitazione dei servizi non necessari, l'utilizzo di password sicure e l'applicazione di controlli di accesso.

6 Rilevare e rispondere alle minacce informatiche.

Davanti a minacce sofisticate, le tradizionali misure di sicurezza non sono più sufficienti. Le organizzazioni devono utilizzare tecnologie e metodologie avanzate di rilevamento delle minacce per identificare e rispondere in modo efficace a minacce note e sconosciute.

- Monitorare e analizzare il traffico di rete, i log di sistema e altre aree, nonché i dati sulla sicurezza per identificare in modo proattivo i segni di accesso non autorizzato, intrusioni, infezioni da malware, violazioni di dati o altre minacce informatiche.
- Implementare un piano di risposta per analizzare e mitigare in maniera tempestiva gli incidenti di sicurezza confermati. Il piano prevede il contenimento dell'impatto, l'identificazione della root cause e l'implementazione delle azioni necessarie per ripristinare i sistemi ed evitare ulteriori danni.
- Sfruttare AI/ML per individuare tempestivamente le minacce informatiche, analizzando in tempo reale i comportamenti o i modelli di dati anomali. Queste tecnologie facilitano inoltre la ricezione di una risposta rapida attraverso la valutazione della gravità delle minacce, la previsione degli impatti, l'automazione di alcune azioni difensive e la scalabilità delle pratiche di sicurezza, riducendo al minimo i potenziali danni.

7 Effettuare un ripristino da un attacco informatico.

Anche con misure proattive critiche in atto, le organizzazioni devono sempre presumere di essere state violate e devono disporre di capacità resilienti che vengano testate frequentemente per garantire un recupero efficace dopo aver subito un attacco informatico andato a buon fine.

- Adottare immediatamente misure di contenimento per ridurre al minimo i danni provocati da un attacco informatico, isolando e contenendone l'impatto.
- Disconnettere dalla rete i sistemi colpiti, disabilitare gli account compromessi e implementare misure per evitare ulteriori danni o l'espansione dell'attacco.
- L'utilizzo di AI/ML accelera il ripristino individuando rapidamente i sistemi e i dati colpiti dall'attacco e automatizza il processo di ripristino dai backup.

8 Richiedere il supporto di partner esperti.

Nessun singolo fornitore dispone di tutte le funzionalità necessarie per garantire la sicurezza end-to-end, di persone, processi o tecnologie: serve la collaborazione di tutti. Pertanto, è essenziale collaborare con una rete di partner esperti.

- Interagire con partner esperti in sicurezza informatica che vantano competenze e risorse preziose che aiutano a orientarsi nel panorama delle minacce in rapida evoluzione.
- Sfruttare le competenze e le conoscenze specializzate che potrebbero non essere disponibili internamente, incluse le informazioni su rischi emergenti, le tecniche di attacco avanzate e le più recenti strategie e best practice in materia di sicurezza.
- Sfruttare l'esperienza di servizi professionali esperti e stabilire rapporti di collaborazione con partner aziendali affidabili per definire un profilo di sicurezza completo che protegga efficacemente dalle minacce informatiche in costante evoluzione.

9 Estendere la sicurezza informatica agli ambienti edge e cloud.

Con la diffusione delle reti dal core all'edge fino al cloud, tali ambienti sono diventati un punto cruciale delle vulnerabilità. Indipendentemente dal modo in cui le applicazioni vengono distribuite, esse richiedono lo stesso livello di sicurezza e allineamento con le politiche aziendali per garantire la coerenza sia per gli utenti sia per la gestione delle applicazioni.

- Assicurarsi che i principi Zero Trust siano estesi per coprire gli ambienti edge e cloud, fornendo solidi controlli degli accessi, autenticazione continua e visibilità e controllo completi sul traffico di rete.
- Implementare misure di sicurezza, come la segmentazione della rete, la crittografia e il monitoraggio continuo, in ambienti di rete core e cloud per proteggersi da potenziali minacce.
- Collaborare con servizi professionali specializzati nella sicurezza dell'edge, del core e del cloud per sfruttare la loro esperienza nell'implementazione di misure efficaci che proteggano l'organizzazione sotto ogni aspetto.

10 Gestire in modo proattivo e aumentare la resilienza end-to-end.

La gestione di Threat Intelligence, incidenti, risposte e operazioni di sicurezza può migliorare le capacità di un'organizzazione nel rilevamento e nella risposta alle minacce informatiche.

- Stabilire protocolli proattivi di risposta agli incidenti e di ripristino che delineino chiaramente ruoli e responsabilità, garantendo una comunicazione e un coordinamento ottimali tra i membri del team.
- Migliorare la visibilità dell'ambiente per consentire alle organizzazioni di monitorare e rispondere in modo proattivo alle minacce all'interno delle proprie reti, fornendo al contempo avvisi per il ripristino quando necessario.
- Rafforzare la capacità di rilevare e rispondere in modo proattivo alle minacce informatiche sfruttando Advanced Threat Intelligence, Security Information and Event Management (SIEM), soluzioni di protezione degli endpoint e analisi comportamentali.

Non lasciare che la sicurezza ostacoli l'innovazione.
Scopri come migliorare la sicurezza informatica e la maturità Zero Trust all'indirizzo dell.com/SecuritySolutions

DELL Technologies