DELL Technologies

Migliorare la sicurezza informatica e la maturità Zero Trust

Non lasciare che i rischi per la sicurezza ostacolino l'innovazione

Scopri lo stato attuale della tua sicurezza informatica

Scopri il suo stato ottimale

Nel panorama delle minacce odierno, complesso e in rapida evoluzione, le organizzazioni spesso si trovano ad affrontare risorse e conoscenze limitate per quanto riguarda l'attuazione di procedure efficaci per la sicurezza informatica. L'aumento della sicurezza informatica e la maturità Zero Trust sono essenziali per combattere le minacce informatiche in continua evoluzione e garantire la sicurezza dell'ambiente senza compromettere l'innovazione.

Utilizza questi elenchi per valutare il tuo livello di maturità nel campo della sicurezza informatica. Conoscere i punti di forza e le vulnerabilità della tua organizzazione ti consentirà di adottare le misure più adeguate per rafforzare la tua maturità nel campo della sicurezza informatica.

Sommario

Checklist: Riduzione della superficie di attacco 3

Checklist: Rilevamento e risposta alle minacce 4

Checklist: Ripristino da un attacco informatico 5

Scopri di più

Ulteriori informazioni su come migliorare la sicurezza informatica e la maturità Zero Trust

Checklist:

Riduzione della superficie di attacco

Con "superficie di attacco" ci si riferisce a tutti i punti o a tutte le aree possibili in un ambiente che possono essere attaccati o sfruttati da un attacco informatico. Questi punti possono includere vulnerabilità del software, configurazioni errate, meccanismi di autenticazione deboli, sistemi senza patch, privilegi utente eccessivi, porte di rete aperte, scarsa sicurezza fisica e altro ancora. Queste domande possono aiutare a determinare in che modo è possibile ridurre al minimo le vulnerabilità e i punti di ingresso che un malintenzionato può compromettere.

Sì	No	
☐	☐	La tua organizzazione esegue regolarmente valutazioni, test di penetrazione o simulazioni di attacchi di violazione per identificare vulnerabilità e punti deboli nei sistemi e nelle reti, consentendo interventi e miglioramenti tempestivi?
☐	☐	La tua organizzazione esegue regolarmente corsi di formazione sulla sicurezza per i vostri dipendenti?
☐	☐	La tua organizzazione utilizza l'autenticazione a più fattori (MFA) e il controllo di accesso basato sui ruoli (RBAC)?
☐	☐	La tua organizzazione ha implementato la segmentazione della rete per isolare le risorse critiche e limitare l'accesso tra diverse parti della rete?
☐	☐	La tua organizzazione implementa pratiche di programmazione sicure, conduce regolarmente test di sicurezza, esamina periodicamente il codice e utilizza firewall per le applicazioni web allo scopo di facilitare la protezione dagli attacchi comuni a livello di applicazione e ridurre la superficie di attacco delle applicazioni web?
☐	☐	La tua organizzazione sceglie fornitori IT in grado di certificare l'uso dei processi e delle procedure per proteggere la propria supply chain?
☐	☐	La tua organizzazione sta implementando principi Zero Trust per sostituire la sicurezza tradizionale basata sul perimetro?
☐	☐	La tua organizzazione utilizza il principio dei privilegi minimi per limitare gli utenti e gli account di sistema ad avere solo i diritti di accesso minimi necessari per eseguire le proprie attività?
☐	☐	La tua organizzazione applica regolarmente patch a sistemi e software?
☐	☐	I sistemi di sicurezza della tua azienda utilizzano funzioni AI/ML per individuare in modo proattivo eventuali vulnerabilità?

Checklist:

Rilevamento e risposta alle minacce

Il rilevamento e la risposta alle minacce informatiche sono elementi essenziali di ogni strategia di sicurezza. Implicano il monitoraggio e l'analisi del traffico di rete, dei log di sistema e di altre aree, nonché dei dati di sicurezza per identificare i segni di accesso non autorizzato, intrusioni, infezioni da malware, violazioni di dati o altre minacce informatiche. Queste domande possono aiutare a determinare in che modo la tua organizzazione identifica e gestisce attivamente potenziali incidenti di sicurezza e attività dannose all'interno di una rete di computer, un sistema o un'organizzazione.

Sì	No	
☐	☐	La tua organizzazione monitora costantemente le attività di rete e di sistema utilizzando strumenti e tecnologie di sicurezza XDR (Extended Detection and Response), IDS (Intrusion Detection System), IPS (Intrusion Prevention System), SIEM e analisi dei log?
☐	☐	La tua organizzazione analizza i dati raccolti per identificare schemi, anomalie e indicatori di compromissione (IOC) e/o indicatori di attacco (IOA) che potrebbero indicare una potenziale minaccia informatica?
☐	☐	La tua organizzazione ha implementato i più recenti strumenti di visibilità e monitoraggio per rilevare e segnalare rapidamente potenziali problemi?
☐	☐	La tua organizzazione monitora il traffico di rete per individuare modelli insoliti o attività sospette che potrebbero indicare un attacco informatico in corso?
☐	☐	La tua organizzazione ha implementato strumenti AI/ML per aiutare a rilevare minacce informatiche attraverso l'analisi in tempo reale di modelli di dati insoliti o comportamenti anomali?
☐	☐	La tua organizzazione ha preso in considerazione l'implementazione di una soluzione SIEM di nuova generazione per gestire meglio gli avvisi di sicurezza e avviare la correlazione dei dati degli eventi di sicurezza in tutto l'ecosistema IT?
☐	☐	La tua organizzazione esegue test e gestione delle vulnerabilità per stabilire le priorità e affrontare le vulnerabilità esistenti e rispondere in modo efficiente alle nuove vulnerabilità?
☐	☐	La tua organizzazione dispone di un piano di risposta agli incidenti per indagare e mitigare gli incidenti di sicurezza confermati?
☐	☐	La tua organizzazione incorpora strumenti SOAR (Security Orchestration, Automation and Response) per velocizzare le azioni di risposta agli incidenti che possono contribuire a ridurre la diffusione di un attacco informatico?
☐	☐	Il piano di risposta agli incidenti della tua organizzazione tiene conto delle policy di contenimento, dei piani di comunicazione, dei requisiti di conformità, dell'analisi forense e del processo di ripristino?

Checklist:

Ripristino da un attacco informatico

Il ripristino da un attacco informatico è il processo di ripristino a uno stato operativo sicuro dei sistemi, delle reti e dei dati compromessi dopo un incidente di sicurezza. Implica l'adozione di misure per mitigare i danni causati dall'attacco, la ricostruzione di servizi e dispositivi compromessi o interrotti, l'analisi dell'incidente per prevenire futuri attacchi e il ritorno alle normali attività dell'organizzazione. Queste domande possono aiutare a stabilire se la tua organizzazione esegue in modo efficace il ripristino dagli attacchi informatici.

Sì	No	
☐	☐	La tua organizzazione ha implementato misure di contenimento degli incidenti per isolare e contenere un attacco informatico?
☐	☐	La tua organizzazione dispone di processi per il ripristino del sistema e/o del dispositivo dopo il contenimento di un incidente?
☐	☐	La tua organizzazione utilizza l'isolamento dei dati, l'immutabilità o un cyber vault per proteggere i dati?
☐	☐	La tua organizzazione ha stabilito delle procedure per recuperare in modo pulito i dati in caso di dati compromessi, crittografati o eliminati?
☐	☐	La tua organizzazione utilizza tecnologie AI/ML per automatizzare o accelerare il ripristino dopo un attacco informatico?
☐	☐	La tua organizzazione valuta continuamente l'incidente e identifica le aree di miglioramento dopo un attacco e un ripristino?
☐	☐	La tua organizzazione ha condotto un'analisi forense per comprendere la metodologia di attacco, determinare l'entità della violazione, identificare i sistemi e i dati interessati e raccogliere prove per aumentare la sicurezza e intraprendere azioni legali o disciplinari?
☐	☐	La tua organizzazione sa come informare le parti interessate, come clienti, partner e fornitori, di un attacco informatico e di eventuali impatti sui loro dati o sulle loro operazioni?
☐	☐	La tua organizzazione mette in pratica le strategie di ripristino più volte all'anno per acquisire sicurezza nelle operazioni di ripristino delle attività e rispettare gli SLA?
☐	☐	La tua organizzazione collabora con fornitori di servizi che forniscono assistenza nelle attività di ripristino dell'organizzazione?

Miglioramento della sicurezza informatica e della maturità Zero Trust

Quando si parla di sicurezza informatica, è fondamentale che le organizzazioni IT pianifichino lo scenario peggiore e che dispongano di più livelli di difesa. Nel panorama in continua evoluzione delle minacce alla sicurezza informatica, è fondamentale migliorare costantemente le pratiche di sicurezza e adottare i principi Zero Trust. Ciò comprende:

Riduzione della superficie di attacco

Ridurre al minimo le vulnerabilità e i punti di ingresso che possono essere sfruttati per compromettere l'ambiente.

Rilevamento e risposta alle minacce informatiche

Identificare e affrontare attivamente potenziali incidenti di sicurezza e attività malevole.

Ripristino dagli attacchi informatici

Eseguire il ripristino dell'organizzazione a uno stato operativo precedente e sicuro dopo un incidente di sicurezza.

Sfruttando l'esperienza dei servizi professionali e collaborando con partner aziendali di fiducia, Dell può aiutare le organizzazioni a stabilire un profilo di sicurezza completo che protegga dalle minacce informatiche in continua evoluzione. La tecnologia continua ad avanzare ed è fondamentale tenere sempre aggiornato l'approccio alla sicurezza informatica al fine di proteggere la nostra infrastruttura digitale e preservare la fiducia nel mondo digitale.

DELL Technologies

Informazioni su Dell Technologies

Dell Technologies aiuta organizzazioni e privati a costruire il proprio futuro digitale e trasformare il modo in cui lavorano, vivono e giocano. L'azienda fornisce ai clienti il portafoglio di tecnologie e servizi più ampio e innovativo del settore per l'era dei dati.

Maggiori informazioni sul sito
www.dell.com/securitysolutions