DELL Technologies

EBOOK INTERATTIVO SUGLI SCENARI DI SICUREZZA INFORMATICA

Scenari reali. Decisioni più intelligenti. Difese più solide.

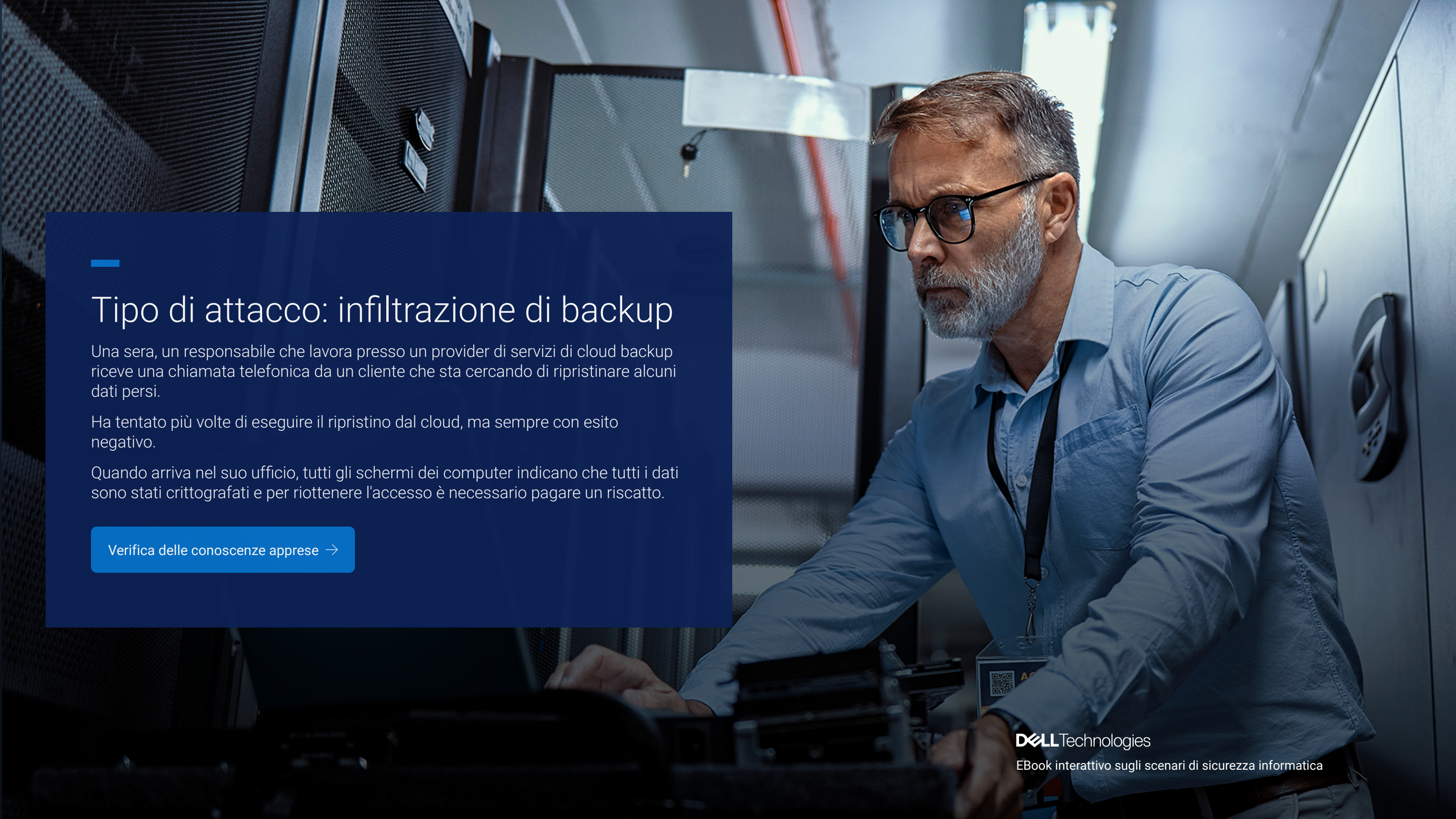
Il nostro impegno per la sicurezza è al centro di tutto quello che facciamo. Questo eBook condivide informazioni, best practice e tecnologie innovative, allo scopo di fornire le informazioni e gli strumenti necessari per tenere il passo con i rischi informatici emergenti.

Scelta dello scenario di attacco

Le minacce alla sicurezza informatica sono in continua evoluzione e, per proteggere i propri dati, le imprese devono rispondere in modo efficace. Per preparare al meglio l'azienda forniamo esercitazioni che simulano gli scenari reali, permettendo di esplorare le strategie di sicurezza informatica da adottare per contrastare gli attacchi.

Vengono illustrate varie tipologie di attacco e problematiche specifiche di settori come la pubblica amministrazione nazionale, regionale e locale, i servizi finanziari e l'assistenza sanitaria. Lungo il percorso, questo eBook illustra le soluzioni di sicurezza integrate nei notebook, nei desktop e nei sistemi aziendali Dell, espressamente progettate per fornire protezione da queste minacce.

- Infiltrazione di backup →
- Ransomware →
- DDoS (Distributed Denial of Service) →
- Componenti hardware della supply chain →
- Minaccia interna malevola →
- Componenti software della supply chain →
- MITM (Man-in-the-Middle) →
- Attacchi zero-day →
- Prompt/SQL Injection →



Tipo di attacco: infiltrazione di backup

Una sera, un responsabile che lavora presso un provider di servizi di cloud backup riceve una chiamata telefonica da un cliente che sta cercando di ripristinare alcuni dati persi.

Ha tentato più volte di eseguire il ripristino dal cloud, ma sempre con esito negativo.

Quando arriva nel suo ufficio, tutti gli schermi dei computer indicano che tutti i dati sono stati crittografati e per riottenere l'accesso è necessario pagare un riscatto.

Verifica delle conoscenze apprese →

Tipo di attacco: infiltrazione di backup

1. Riduzione della superficie di attacco
2
3
4

Poiché non è possibile identificare con certezza i sistemi di backup o i clienti colpiti, quale dovrebbe essere il primo passo?

- [ ] Informare le autorità
- [ ] Arrestare tutti i sistemi
- [ ] Cercare di contenere e isolare la minaccia
- [ ] Verificare la disponibilità di un backup pulito da cui eseguire il ripristino

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1. Riduzione della superficie di attacco
2
3
4

Poiché non è possibile identificare con certezza i sistemi di backup o i clienti colpiti, quale dovrebbe essere il primo passo?

- ✗ Informare le autorità
- ✗ Arrestare tutti i sistemi
- ✓ Cercare di contenere e isolare la minaccia
- ✗ Verificare la disponibilità di un backup pulito da cui eseguire il ripristino

Per impedire l'ulteriore diffusione, limitare i danni e consentire la valutazione della portata dell'incidente è necessario contenere e isolare immediatamente la minaccia. Questo offre la possibilità di ridurre l'impatto di qualsiasi tipo di attacco informatico, inclusi quelli che sfruttano l'AI.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

La priorità è ripristinare tempestivamente l'accesso ai dati del cliente. Cosa bisogna fare per raggiungere questo obiettivo?

- [ ] Pagare il riscatto
- [ ] Identificare la tipologia di ransomware
- [ ] Informare le autorità
- [ ] Identificare i dati compromessi

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

La priorità è ripristinare tempestivamente l'accesso ai dati del cliente. Cosa bisogna fare per raggiungere questo obiettivo?

- ✗ Pagare il riscatto
- ✗ Identificare la tipologia di ransomware
- ✗ Informare le autorità
- ✓ Identificare i dati compromessi

L'identificazione dei dati compromessi consente di concentrare le attività sul ripristino delle informazioni più critiche del cliente. Questo aumenta la disponibilità dei dati ed evita di eseguire attività inutili sui sistemi non interessati.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1 — 2 — 3. Ripristino da un attacco informatico — 4

Viene identificato un backup utilizzabile per il ripristino. Quale dovrebbe essere il primo passo da eseguire?

- [ ] Ripristinare innanzitutto i sistemi critici
- [ ] Eseguire un'analisi forense per verificare che l'attacco sia completamente contenuto
- [ ] Modificare tutte le password e revocare le credenziali compromesse
- [ ] Implementare i principi Zero Trust

Selezionare la risposta corretta →

Tipo di attacco: infiltrazione di backup

1 — 2 — 3. Ripristino da un attacco informatico — 4

Viene identificato un backup utilizzabile per il ripristino. Quale dovrebbe essere il primo passo da eseguire?

- ✗ Ripristinare innanzitutto i sistemi critici
- ✓ Eseguire un'analisi forense per verificare che l'attacco sia completamente contenuto
- ✗ Modificare tutte le password e revocare le credenziali compromesse
- ✗ Implementare i principi Zero Trust

Prima di ripristinare i sistemi, è necessario assicurarsi che l'attacco sia completamente contenuto, in modo da prevenire la reinfezione accidentale ed evitare ulteriori danni. Questo impedisce alle minacce di attecchire e diffondersi nell'ambiente.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1 2 3 4. Best practice generali

Cosa si può fare per ridurre la probabilità di subire un attacco simile in futuro?

- [ ] Usa i principi Zero Trust
- [ ] Abilitare le funzionalità EDR (Endpoint Detection and Response)
- [ ] Implementare backup immutabili, isolati tramite air-gap
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: infiltrazione di backup

1 2 3 4. Best practice generali

Cosa si può fare per ridurre la probabilità di subire un attacco simile in futuro?

- [x] Usa i principi Zero Trust
- [x] Abilitare le funzionalità EDR (Endpoint Detection and Response)
- [x] Implementare backup immutabili, isolati tramite air-gap
- [x] Tutte le opzioni precedenti

Poiché non esiste una misura singola sufficiente, occorre adottare una strategia di difesa multi-livello per mitigare i rischi, ridurre al minimo i danni e migliorare la resilienza dell'azienda.

Scopri le soluzioni →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

TIPO DI ATTACCO: INFILTRAZIONE DI BACKUP

Conclusioni

L'infiltrazione dei backup si verifica quando i criminali informatici sfruttano le vulnerabilità nei sistemi di backup per compromettere, distruggere o crittografare i dati di ripristino critici. Per acuire le ripercussioni operative e finanziarie, questi attacchi sofisticati possono essere sferrati in concomitanza o dopo altri incidenti, come il deployment di ransomware o malware.

Noi di Dell facciamo tutto il possibile per aiutare le aziende ad aumentare la resilienza di fronte a minacce informatiche in continua evoluzione. Con le nostre soluzioni all'avanguardia, i nostri servizi specialistici e le nostre partnership di fiducia, siamo sempre a disposizione per aiutarle a proteggere le risorse più importanti per loro.

Per ulteriori informazioni sulle nostre soluzioni e su come affrontiamo i problemi informatici più difficili, fare clic sul pulsante sotto.

Informazioni sintetiche sull'infiltrazione di backup →

Torna agli scenari

Portafoglio PowerProtect ›

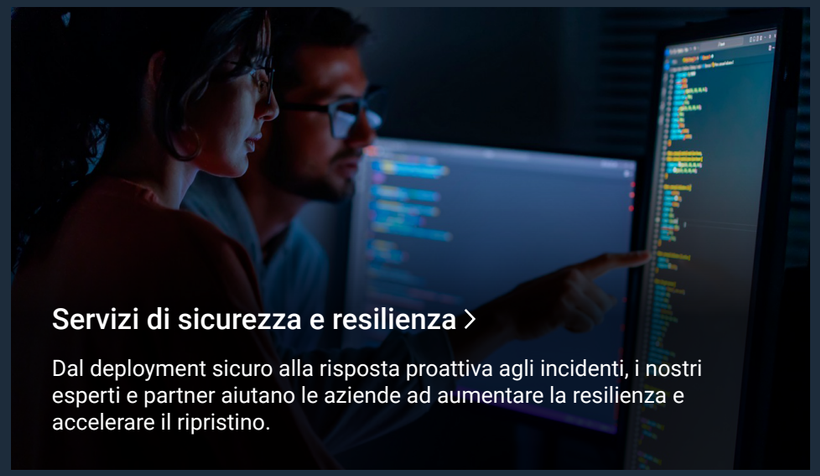
I nostri vault di backup immutabili, crittografati e isolati tramite air-gap sfruttano l'analisi CyberSense basata sull'AI per accelerare il rilevamento e il ripristino, in modo da mantenere la resilienza.

Server PowerEdge ›

Dell fornisce un'infrastruttura affidabile per la protezione dei backup, con funzioni come avvio sicuro, Root of Trust hardware e blocco dei sistemi.

Ambiente di lavoro affidabile ›

Al fine di ridurre i rischi, le funzioni di protezione SafeBIOS e SafeData garantiscono sistemi di backup inviolabili e sempre pronti in caso di necessità.



Servizi di sicurezza e resilienza ›

Dal deployment sicuro alla risposta proattiva agli incidenti, i nostri esperti e partner aiutano le aziende ad aumentare la resilienza e accelerare il ripristino.

Soluzioni di networking ›

Con la segmentazione della rete, l'autenticazione a più fattori (MFA) e le configurazioni con privilegi minimi, le soluzioni Dell consentono di bloccare l'accesso e proteggere i dati critici.

Tipo di attacco: DDoS (Distributed Denial of Service)

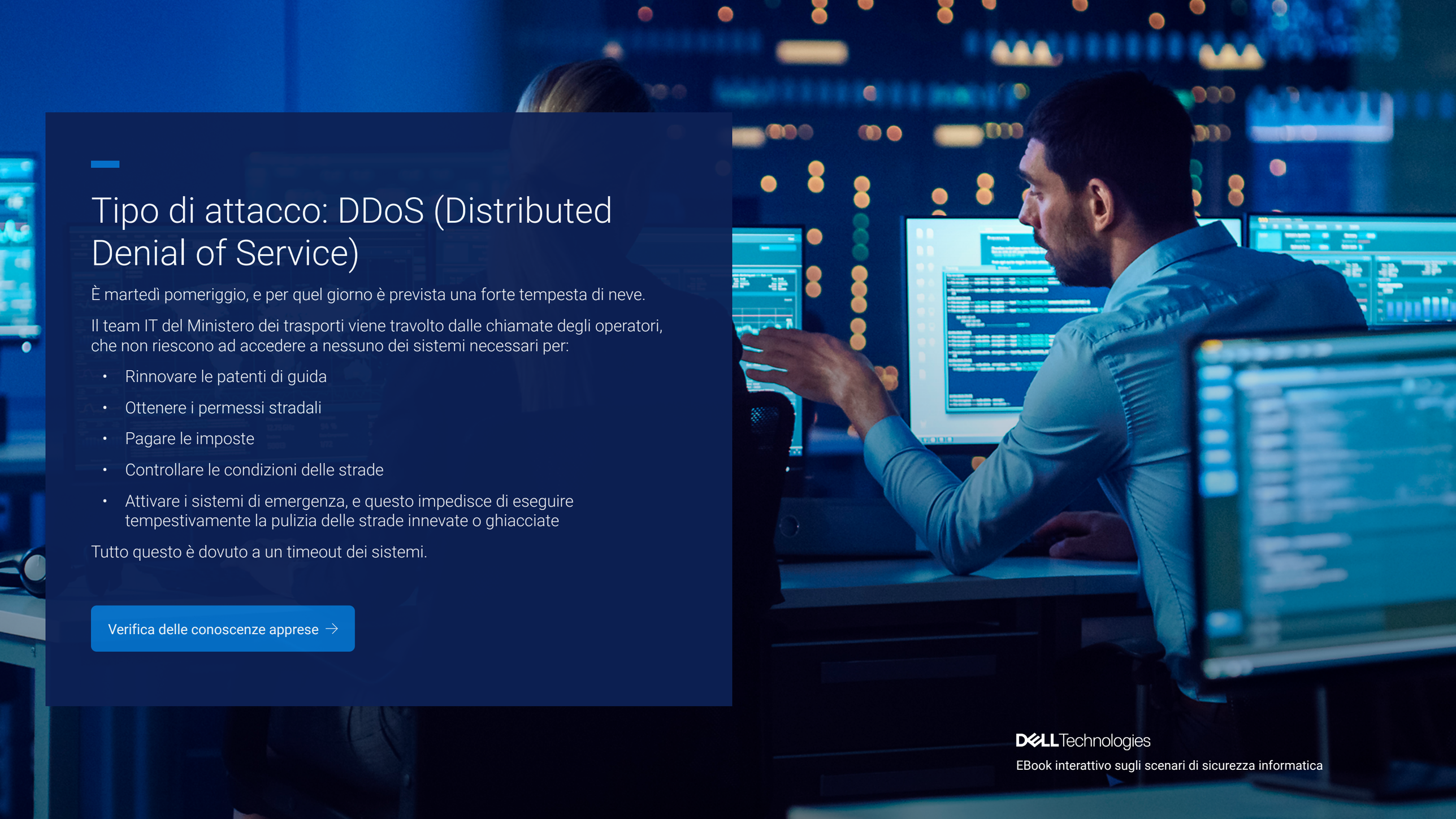
È martedì pomeriggio, e per quel giorno è prevista una forte tempesta di neve.

Il team IT del Ministero dei trasporti viene travolto dalle chiamate degli operatori, che non riescono ad accedere a nessuno dei sistemi necessari per:

- Rinnovare le patenti di guida
- Ottenere i permessi stradali
- Pagare le imposte
- Controllare le condizioni delle strade
- Attivare i sistemi di emergenza, e questo impedisce di eseguire tempestivamente la pulizia delle strade innevate o ghiacciate

Tutto questo è dovuto a un timeout dei sistemi.

Verifica delle conoscenze apprese →



Tipo di attacco: DDoS (Distributed Denial of Service)

1. Riduzione della superficie di attacco
2
3
4

Qual è la prima cosa da fare per cercare l'origine del problema?

- [ ] Controllare i dispositivi di rete per verificare la presenza di aumenti improvvisi e inspiegabili del traffico in entrata
- [ ] Cercare nei dispositivi di rete eventuale traffico insolito proveniente da un piccolo gruppo di indirizzi IP o da un indirizzo singolo
- [ ] Controllare i log degli strumenti di visibilità della rete o del firewall, per stabilire se si è verificati un numero eccessivo di errori di connessione o eventi di blocco del traffico
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1. Riduzione della superficie di attacco
2
3
4

Qual è la prima cosa da fare per cercare l'origine del problema?

- [x] Controllare i dispositivi di rete per verificare la presenza di aumenti improvvisi e inspiegabili del traffico in entrata
- [x] Cercare nei dispositivi di rete eventuale traffico insolito proveniente da un piccolo gruppo di indirizzi IP o da un indirizzo singolo
- [x] Controllare i log degli strumenti di visibilità della rete o del firewall, per stabilire se si è verificati un numero eccessivo di errori di connessione o eventi di blocco del traffico
- [x] Tutte le opzioni precedenti

Per diagnosticare correttamente le interruzioni dei servizi su vasta scala, è necessario esaminare sia le attività dei dispositivi di rete, sia i log degli strumenti di visibilità o dei firewall, allo scopo di individuare tempestivamente eventi di blocco o pattern insoliti. In questo modo è possibile distinguere gli incidenti informatici dai problemi dell'infrastruttura, per garantire una risposta più rapida e precisa agli incidenti.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Si sospetta che si tratti di un attacco DDoS. Qual è il passo successivo?

- [ ] Reindirizzare tutto il traffico di rete tramite un servizio di mitigazione degli attacchi DDoS
- [ ] Attivare le regole del WAF (Web Application Firewall) per filtrare i pattern nocivi
- [ ] Verificare se il picco di traffico proviene da fonti legittime
- [ ] Segnalare la situazione, sia internamente che esternamente

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Si sospetta che si tratti di un attacco DDoS. Qual è il passo successivo?

- ✗ Reindirizzare tutto il traffico di rete tramite un servizio di mitigazione degli attacchi DDoS
- ✗ Attivare le regole del WAF (Web Application Firewall) per filtrare i pattern nocivi
- ✓ Verificare se il picco di traffico proviene da fonti legittime
- ✗ Segnalare la situazione, sia internamente che esternamente

Prima di attivare le contromisure DDoS, è essenziale verificare se si tratta di un picco di traffico legittimo. In questo modo si evita di bloccare accidentalmente gli utenti autorizzati e di interrompere i servizi destinati alle figure critiche. È inoltre possibile garantire l'adozione di misure di protezione aggiuntive appropriate e attentamente mirate, per ridurre al minimo gli effetti negativi sugli interventi della pubblica amministrazione e sulla continuità operativa in generale.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 2 3. Ripristino da un attacco informatico 4

Quali misure si possono adottare per evitare gli attacchi DDoS in futuro?

- [ ] Bloccare gli indirizzi IP da cui proviene l'attacco
- [ ] Eseguire test di penetrazione regolari, con simulazioni di attacchi DDoS
- [ ] Spostare tutte le applicazioni nel cloud, perché di solito i provider di servizi cloud non subiscono attacchi DDoS
- [ ] Implementare i principi Zero Trust

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 — 2 — 3. Ripristino da un attacco informatico — 4

Quali misure si possono adottare per evitare gli attacchi DDoS in futuro?

- ✗ Bloccare gli indirizzi IP da cui proviene l'attacco
- ✓ Eseguire test di penetrazione regolari, con simulazioni di attacchi DDoS
- ✗ Spostare tutte le applicazioni nel cloud, perché di solito i provider di servizi cloud non subiscono attacchi DDoS
- ✓ Implementare i principi Zero Trust

I test proattivi di penetrazione con simulazione di attacchi DDoS permettono di identificare e colmare le lacune nelle difese, mentre i principi Zero Trust hanno lo scopo di contenere i rischi attraverso l'applicazione regolare del principio del privilegio minimo. Questo contribuisce a ridurre il rischio di interruzione dei servizi essenziali, come il coordinamento della risposta alle emergenze o il controllo in tempo reale dei segnali stradali, che devono rimanere in funzione anche in caso di attacco.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 2 3 4. Best practice generali

Nell'ambito del piano generale di risposta e ripristino in seguito a un incidente (IRR, Incident Response And Recovery), chi è necessario informare?

- [ ] Il team legale
- [ ] La compagnia che fornisce l'assicurazione informatica
- [ ] La CISA (Cybersecurity and Infrastructure Security Agency), l'FBI e l'MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: DDoS (Distributed Denial of Service)

1 2 3 4. Best practice generali

Nell'ambito del piano generale di risposta e ripristino in seguito a un incidente (IRR, Incident Response And Recovery), chi è necessario informare?

- [x] Il team legale
- [x] La compagnia che fornisce l'assicurazione informatica
- [x] La CISA (Cybersecurity and Infrastructure Security Agency), l'FBI e l'MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Tutte le opzioni precedenti

Durante un incidente informatico su vasta scala, è consigliabile coordinarsi con il team legale, la compagnia assicurativa e la pubblica amministrazione, per garantire la conformità, ottenere un indennizzo e richiedere l'intervento delle forze dell'ordine. Quando ha la certezza che tutti i requisiti normativi sono soddisfatti, l'azienda può contenere l'incidente, risolvere il problema ed eseguire un ripristino efficace.

Scopri le soluzioni →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

TIPO DI ATTACCO: DDOS (DISTRIBUTED DENIAL OF SERVICE)

Conclusioni

Un attacco DDoS cerca di interrompere il normale funzionamento di una rete, di un servizio o di un server sovraccaricandolo di un enorme volume di traffico da più origini. Questi attacchi vengono eseguiti sfruttando le botnet, ovvero reti di dispositivi infetti controllati da remoto dai malintenzionati.

Noi di Dell facciamo tutto il possibile per aiutare le aziende ad aumentare la resilienza di fronte agli attacchi DDoS, combinando tecnologie di rilevamento e mitigazione avanzate con servizi specialistici e un approccio Zero Trust, allo scopo di garantire una risposta rapida, ridurre al minimo le interruzioni e rafforzare le difese.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi DDoS, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi DDoS →

Torna agli scenari

Soluzioni di networking ›

Applicano la segmentazione della rete, la micro-segmentazione e il principio del privilegio minimo per isolare gli asset critici, limitare la diffusione degli attacchi e accelerare il contenimento degli attacchi DDoS.

Server PowerEdge ›

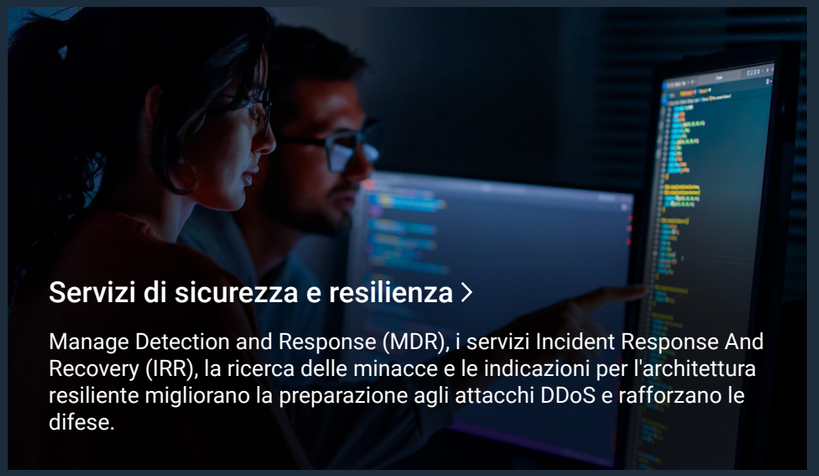
Con Root of Trust hardware, avvio sicuro, blocco dei sistemi e raccolta delle prove di manomissione in tempo reale, Dell offre una protezione resiliente e ad alte prestazioni dagli attacchi DDoS, che consente di accelerare il ripristino.

Dispositivi affidabili ›

Le funzioni integrate SafeBIOS e SecureData, insieme al rilevamento e alla risposta automatizzati, riducono fino al 70% la superficie di attacco degli endpoint, per impedire che le distrazioni dovute agli incidenti DDoS si trasformino in vettori di attacco.

Portafoglio PowerProtect ›

I nostri ambienti di backup crittografati, immutabili e isolati tramite air-gap, che sfruttano l'analisi delle minacce basata sull'AI, garantiscono un ripristino rapido e convalidato, per garantire la continuità operativa durante gli attacchi DDoS.



Servizi di sicurezza e resilienza ›

Manage Detection and Response (MDR), i servizi Incident Response And Recovery (IRR), la ricerca delle minacce e le indicazioni per l'architettura resiliente migliorano la preparazione agli attacchi DDoS e rafforzano le difese.

Tipo di attacco: utente malintenzionato interno

Sono le 8 di un martedì mattina. Per i dipendenti di un'azienda sanitaria statunitense, la giornata di lavoro è appena iniziata.

Dopo aver lavorato in ufficio fino a tarda notte, una dipendente di alto livello che utilizza i dati altamente sensibili dei pazienti effettua l'accesso

e nota che una cartella su cui aveva lavorato la notte precedente è stata modificata. Dopo aver informato il suo team, presenta una richiesta di assistenza al reparto IT.

Le indagini rivelano che un dipendente junior del reparto IT legato a un'organizzazione criminale ha indotto con l'inganno un dipendente di alto livello a inserire nel suo dispositivo un Rubber Ducky USB che esegue il downgrade del BIOS (Basic input/Output System) a una versione vulnerabile, allo scopo di compromettere il sistema.

Verifica delle conoscenze apprese →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: utente malintenzionato interno

1. Riduzione della superficie di attacco
2
3
4
5

L'utente malintenzionato interno ha effettuato questo attacco utilizzando due metodi che vengono monitorati dal framework MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Quali sono queste nuove tecnologie?

- [ ] Rapporto di fiducia + replica tramite supporto rimovibile
- [ ] Social engineering + replica tramite supporto rimovibile
- [ ] Social engineering + servizi remoti esterni
- [ ] Rapporto di fiducia + componenti hardware aggiuntivi

Selezionare la risposta corretta →

Tipo di attacco: utente malintenzionato interno

1. Riduzione della superficie di attacco
2
3
4
5

L'utente malintenzionato interno ha effettuato questo attacco utilizzando due metodi che vengono monitorati dal framework MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Quali sono queste nuove tecnologie?

- ✗ Rapporto di fiducia + replica tramite supporto rimovibile
- ✓ Social engineering + replica tramite supporto rimovibile
- ✗ Social engineering + servizi remoti esterni
- ✗ Rapporto di fiducia + componenti hardware aggiuntivi

Allineandosi alle tecniche MITRE ATT&CK per la manipolazione umana e la replica tramite dispositivi di storage portatili, l'autore dell'attacco ha sfruttato il social engineering per indurre con l'inganno un dipendente di alto livello a inserire un Rubber Ducky USB per caricare dati compromessi tramite un supporto rimovibile.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: utente malintenzionato interno

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4 — 5

Perché l'utente malintenzionato ha dovuto utilizzare entrambi i metodi?

- [ ] Per effettuare il downgrade del BIOS (Basic input/Output System) occorre accedere alla rete come amministratore globale
- [ ] Per consentire il downgrade del BIOS è necessario ingannare l'amministratore
- [ ] Per ottenere le credenziali di accesso una tantum alla rete occorre modificare il provider DNS (Domain Name System) del dispositivo
- [ ] Per ottenere le credenziali di accesso continuo alla rete occorre installare malware su un dispositivo

Selezionare la risposta corretta →

Tipo di attacco: utente malintenzionato interno

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4 — 5

Perché l'utente malintenzionato ha dovuto utilizzare entrambi i metodi?

- ✗ Per effettuare il downgrade del BIOS (Basic input/Output System) occorre accedere alla rete come amministratore globale
- ✗ Per consentire il downgrade del BIOS è necessario ingannare l'amministratore
- ✗ Per ottenere le credenziali di accesso una tantum alla rete occorre modificare il provider DNS (Domain Name System) del dispositivo
- ✓ Per ottenere le credenziali di accesso continuo alla rete occorre installare malware su un dispositivo

L'utente malintenzionato doveva utilizzare entrambi i metodi, ovvero installare il malware tramite un Rubber Ducky USB per compromettere il dispositivo e ottenere le credenziali di accesso continuo alla rete, in modo da stabilire un controllo persistente e non autorizzato sull'ambiente di destinazione.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: utente malintenzionato interno

1 — 2 — 3. Rilevamento e risposta alle minacce informatiche — 4 — 5

Quale fra i seguenti è un metodo di rilevamento delle attività di rete irregolari?

- [ ] Application Control
- [ ] Rilevamento e risposta estesi (XDR)
- [ ] Antivirus di nuova generazione (NGAV)
- [ ] Geofencing degli endpoint

Selezionare la risposta corretta →

Tipo di attacco: utente malintenzionato interno

1 2 3. Rilevamento e risposta alle minacce informatiche 4 5

Quale fra i seguenti è un metodo di rilevamento delle attività di rete irregolari?

- ✗ Application Control
- ✓ Rilevamento e risposta estesi (XDR)
- ✗ Antivirus di nuova generazione (NGAV)
- ✗ Geofencing degli endpoint

XDR è l'ideale per rilevare le attività di rete sospette, perché monitora e analizza continuativamente le attività di endpoint, reti e ambienti cloud allo scopo di fornire una visibilità ampia e correlata che accelera il rilevamento delle minacce.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: utente malintenzionato interno

1 2 3 4. Ripristino da un attacco informatico 5

Quale misura di sicurezza integrata nei PC potrebbe rilevare le attività sospette nelle prime fasi della kill chain?

- [ ] Security Information and Event Management (SIEM)
- [ ] Rilevamento e risposta estesi (XDR)
- [ ] Indicatori di attacco (IoA)
- [ ] Controllo degli accessi basato su ruoli (RBAC)

Selezionare la risposta corretta →

Tipo di attacco: utente malintenzionato interno

1 2 3 4. Ripristino da un attacco informatico 5

Quale misura di sicurezza integrata nei PC potrebbe rilevare le attività sospette nelle prime fasi della kill chain?

- ✗ Security Information and Event Management (SIEM)
- ✗ Rilevamento e risposta estesi (XDR)
- ✓ Indicatori di attacco (IoA)
- ✗ Controllo degli accessi basato su ruoli (RBAC)

Gli indicatori di attacco si concentrano sul rilevamento dei comportamenti dei malintenzionati e dei pattern di attività sospette a mano a mano che si presentano, per consentire ai team di sicurezza di identificare le minacce più tempestivamente, rispetto ai metodi basati sulla firma, e di intervenire prima che possano causare danni gravi.

Domanda successiva →

Tipo di attacco: utente malintenzionato interno

1 2 3 4 5. Best practice generali

Dopo aver individuato il metodo di accesso iniziale, quale misura è possibile adottare per eseguire il ripristino e prevenire violazioni future dello stesso tipo?

- [ ] Aggiornare il BIOS alla versione più recente
- [ ] Disabilitare l'opzione di downgrade del BIOS
- [ ] Disabilitare le porte USB
- [ ] Implementare il controllo granulare per consentire l'utilizzo sicuro dei dispositivi USB e prevenire la diffusione del malware
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: utente malintenzionato interno

1 2 3 4 5. Best practice generali

Dopo aver individuato il metodo di accesso iniziale, quale misura è possibile adottare per eseguire il ripristino e prevenire violazioni future dello stesso tipo?

- [x] Aggiornare il BIOS alla versione più recente
- [x] Disabilitare l'opzione di downgrade del BIOS
- [x] Disabilitare le porte USB
- [x] Implementare il controllo granulare per consentire l'utilizzo sicuro dei dispositivi USB e prevenire la diffusione del malware
- [x] Tutte le opzioni precedenti

La gestione di vettori di attacco distinti, per garantire la protezione dell'hardware e il blocco dei downgrade, permette di contenere le minacce che sfruttano i dispositivi USB e interrompere la diffusione del malware in più punti, in modo da creare una difesa multilivello completa che ripristina i sistemi interessati e li protegge dalle violazioni future.

Scopri le soluzioni →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

TIPO DI ATTACCO: UTENTE MALINTENZIONATO INTERNO

Conclusioni

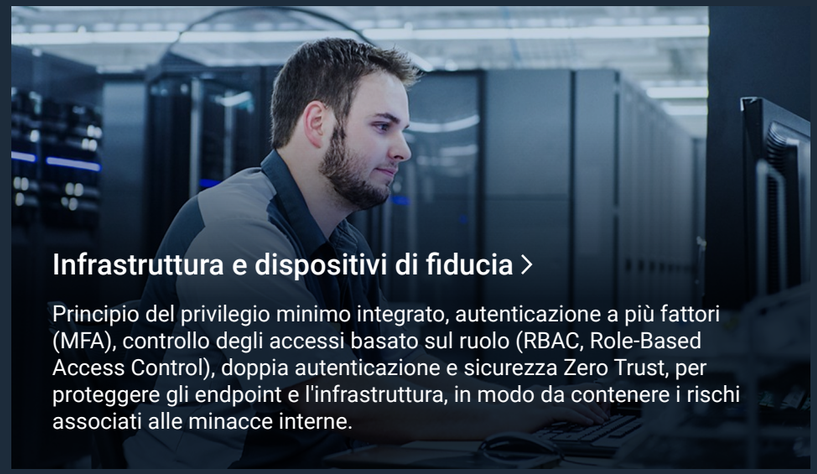
L'espressione "attacco di un utente interno malintenzionato" si riferisce a una persona che opera all'interno di un'organizzazione e sfrutta indebitamente il suo accesso allo scopo di compromettere dati, interrompere operazioni o estrarre informazioni sensibili per finalità personali, finanziarie o di concorrenza. Questa persona può essere un dipendente, un appaltatore, un partner o chiunque abbia accesso legittimo ai sistemi e alle reti dell'azienda.

Per difendere i sistemi dagli attacchi degli utenti malintenzionati interni, Dell fornisce una combinazione di tecnologie avanzate e protocolli di sicurezza rigorosi.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi degli utenti malintenzionati interni, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi degli utenti malintenzionati interni →

Torna agli scenari



Infrastruttura e dispositivi di fiducia >

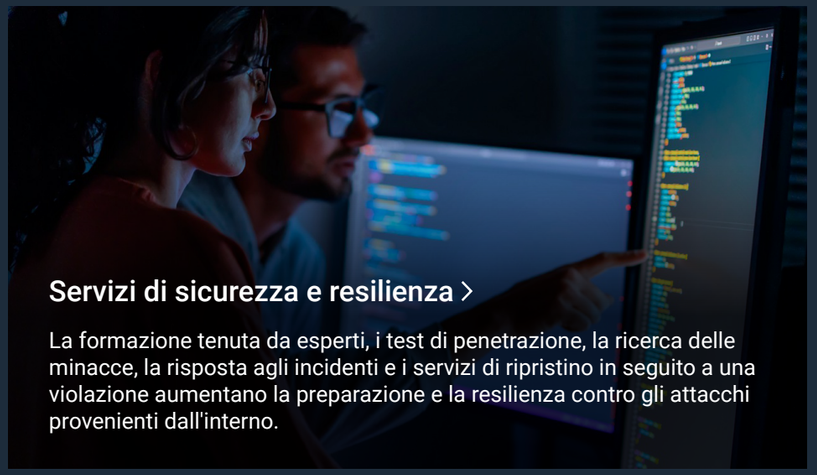
Principio del privilegio minimo integrato, autenticazione a più fattori (MFA), controllo degli accessi basato sul ruolo (RBAC, Role-Based Access Control), doppia autenticazione e sicurezza Zero Trust, per proteggere gli endpoint e l'infrastruttura, in modo da contenere i rischi associati alle minacce interne.

Server PowerEdge >

Root of Trust hardware, avvio sicuro, gestione dinamica delle porte USB e blocco dei sistemi proteggono dalle manomissioni e bloccano gli attacchi interni, sia fisici che basati sul firmware.

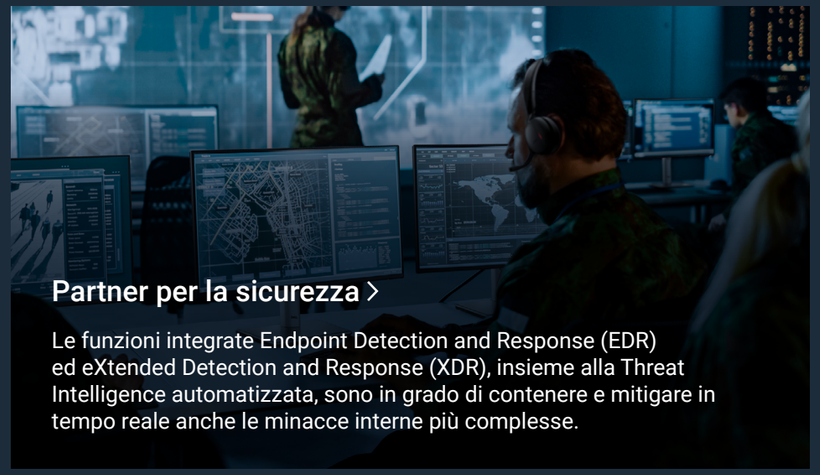
Portafoglio PowerProtect >

I backup isolati e immutabili garantiscono l'integrità dei dati, il ripristino rapido e il rilevamento tempestivo dei tentativi di manipolazione, consentendo di recuperare i dati anche in caso di attacco interno.



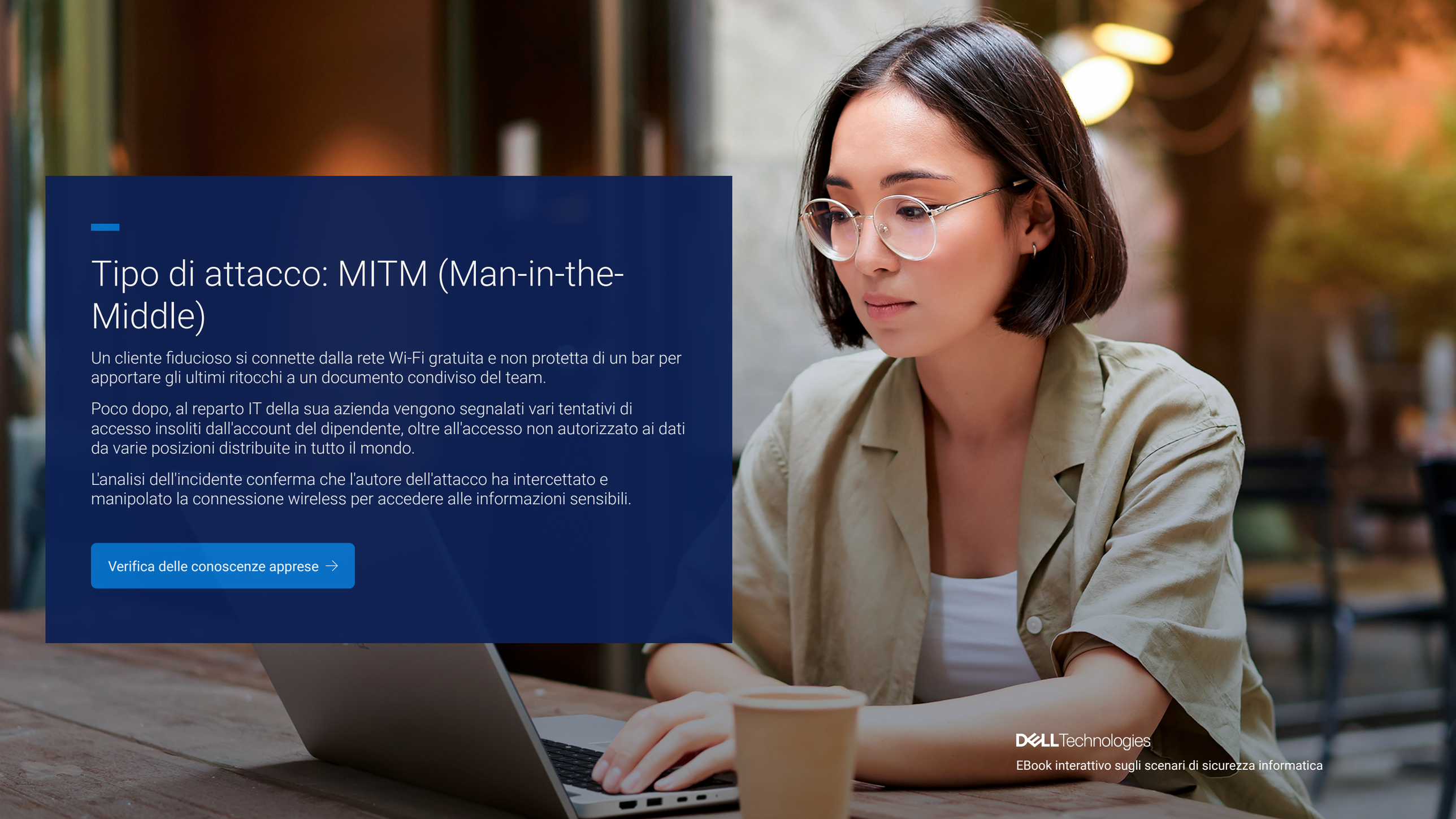
Servizi di sicurezza e resilienza >

La formazione tenuta da esperti, i test di penetrazione, la ricerca delle minacce, la risposta agli incidenti e i servizi di ripristino in seguito a una violazione aumentano la preparazione e la resilienza contro gli attacchi provenienti dall'interno.



Partner per la sicurezza >

Le funzioni integrate Endpoint Detection and Response (EDR) ed eXtended Detection and Response (XDR), insieme alla Threat Intelligence automatizzata, sono in grado di contenere e mitigare in tempo reale anche le minacce interne più complesse.



Tipo di attacco: MITM (Man-in-the-Middle)

Un cliente fiducioso si connette dalla rete Wi-Fi gratuita e non protetta di un bar per apportare gli ultimi ritocchi a un documento condiviso del team.

Poco dopo, al reparto IT della sua azienda vengono segnalati vari tentativi di accesso insoliti dall'account del dipendente, oltre all'accesso non autorizzato ai dati da varie posizioni distribuite in tutto il mondo.

L'analisi dell'incidente conferma che l'autore dell'attacco ha intercettato e manipolato la connessione wireless per accedere alle informazioni sensibili.

Verifica delle conoscenze apprese →

Tipo di attacco: MITM (Man-in-the-Middle)

1. Riduzione della superficie di attacco
2
3
4

Qual è il primo aspetto che il team IT deve verificare dopo aver rilevato i tentativi di accesso insoliti?

- [ ] Firewall, log dei sistemi IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e XDR (eXtended Detection Response)
- [ ] Notebook del dipendente interessato
- [ ] Traffico sulla rete Wi-Fi non protetta del bar
- [ ] Log di autenticazione dei sistemi aziendali

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: MITM (Man-in-the-Middle)

1. Riduzione della superficie di attacco
2
3
4

Qual è il primo aspetto che il team IT deve verificare dopo aver rilevato i tentativi di accesso insoliti?

- [x] Firewall, log dei sistemi IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e XDR (eXtended Detection Response)
- [ ] Notebook del dipendente interessato
- [ ] Traffico sulla rete Wi-Fi non protetta del bar
- [x] Log di autenticazione dei sistemi aziendali

Il personale IT può analizzare i log di firewall, IDS/IPS e autenticazione per tracciare i tentativi di accesso non autorizzati, valutare gli account compromessi e comprendere meglio la portata dell'incidente.

Domanda successiva →

Tipo di attacco: MITM (Man-in-the-Middle)

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Dopo aver confermato l'attacco MITM, quale azione immediata deve intraprendere il personale IT?

- [ ] Disconnettere immediatamente dalla rete il dispositivo compromesso del dipendente e isolarlo per eseguirne l'analisi
- [ ] Aggiornare le regole del firewall e le configurazioni di rete per impedire ulteriori accessi non autorizzati
- [ ] Reimpostare le password degli account di tutti i dipendenti
- [ ] Disabilitare i sistemi colpiti per evitare l'esfiltrazione dei dati

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: MITM (Man-in-the-Middle)

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Dopo aver confermato l'attacco MITM, quale azione immediata deve intraprendere il personale IT?

- [x] Disconnettere immediatamente dalla rete il dispositivo compromesso del dipendente e isolarlo per eseguirne l'analisi
- [x] Aggiornare le regole del firewall e le configurazioni di rete per impedire ulteriori accessi non autorizzati
- [ ] Reimpostare le password degli account di tutti i dipendenti
- [ ] Disabilitare i sistemi colpiti per evitare l'esfiltrazione dei dati

La disconnessione e l'isolamento immediati del dispositivo compromesso impediscono l'accesso ai malintenzionati e conservano le prove forensi, mentre l'aggiornamento delle regole del firewall e della rete blocca le ulteriori connessioni nocive e protegge tutta la rete dal tentativo di compromissione in corso.

Domanda successiva →

Tipo di attacco: MITM (Man-in-the-Middle)

1 — 2 — 3. Ripristino da un attacco informatico — 4

Quali misure preventive si potrebbero adottare per ridurre la vulnerabilità agli attacchi MITM?

- [ ] Imposizione dell'utilizzo di una VPN a tutti i dipendenti
- [ ] Implementazione dei principi di sicurezza Zero Trust, come l'autenticazione a più fattori (MFA)
- [ ] Divieto di utilizzo delle reti Wi-Fi pubbliche
- [ ] Crittografia dei file di dati sensibili condivisi tramite e-mail

Selezionare la risposta corretta →

Tipo di attacco: MITM (Man-in-the-Middle)

1 — 2 — 3. Ripristino da un attacco informatico — 4

Quali misure preventive si potrebbero adottare per ridurre la vulnerabilità agli attacchi MITM?

- ✓ Imposizione dell'utilizzo di una VPN a tutti i dipendenti
- ✓ Implementazione dei principi di sicurezza Zero Trust, come l'autenticazione a più fattori (MFA)
- ✗ Divieto di utilizzo delle reti Wi-Fi pubbliche
- ✗ Crittografia dei file di dati sensibili condivisi tramite e-mail

Quando gli utenti si connettono tramite una rete non protetta, l'utilizzo di una VPN garantisce la crittografia del traffico trasmesso su Internet dai dipendenti, per evitare che venga intercettato, mentre l'implementazione della sicurezza Zero Trust e dell'autenticazione a più fattori garantisce la verifica di ogni singola richiesta di accesso.

Domanda successiva →

Tipo di attacco: MITM (Man-in-the-Middle)

1 2 3 4. Best practice generali

Dopo aver risolto la violazione, quali strategie a lungo termine deve implementare l'azienda?

- [ ] Regolari attività di verifica e applicazione di patch ai sistemi
- [ ] Ulteriore segmentazione della rete per isolare i dati e i sistemi sensibili
- [ ] Implementazione di soluzioni EDR (Endpoint Detection and Response) ed MDR (Managed Detection and Response)
- [ ] Fornitura di una formazione completa e regolare ai dipendenti
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

Tipo di attacco: MITM (Man-in-the-Middle)

1 2 3 4. Best practice generali

Dopo aver risolto la violazione, quali strategie a lungo termine deve implementare l'azienda?

- [x] Regolari attività di verifica e applicazione di patch ai sistemi
- [x] Ulteriore segmentazione della rete per isolare i dati e i sistemi sensibili
- [x] Implementazione di soluzioni EDR (Endpoint Detection and Response) ed MDR (Managed Detection and Response)
- [x] Fornitura di una formazione completa e regolare ai dipendenti
- [x] Tutte le opzioni precedenti

Per proteggersi da minacce diverse, è necessario combinare queste strategie a lungo termine in modo da ottenere un profilo di sicurezza esaustivo e resiliente, che impedisce agli hacker di sfruttare le lacune e garantisce una risposta rapida ed efficace alle violazioni.

Scopri le soluzioni →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

TIPO DI ATTACCO: MITM (MAN-IN-THE-MIDDLE)

Conclusioni

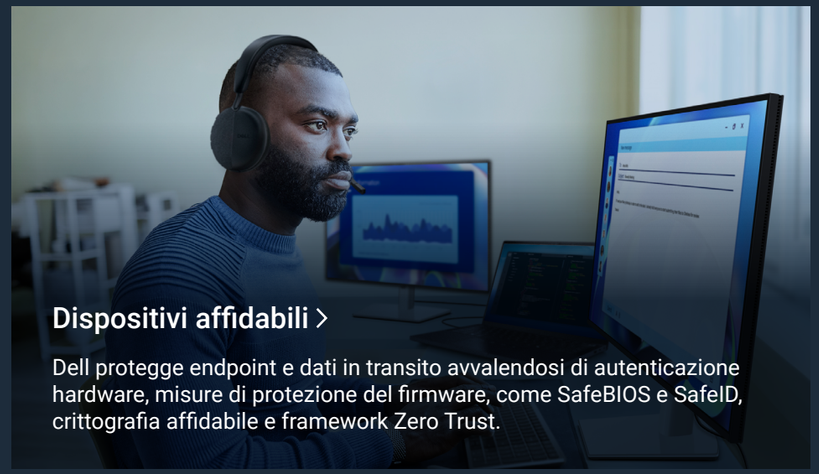
Si verifica un attacco MITM quando un criminale informatico intercetta segretamente le comunicazioni tra due parti, ad esempio tra un dipendente e un server aziendale o tra un cliente e un sito web aziendale. Gli obiettivi dei malintenzionati possono variare, ma il risultato è sempre una violazione della sicurezza, con una conseguente perdita di fiducia.

Dell offre soluzioni di sicurezza scalabili e innovative, che permettono alle aziende di neutralizzare le minacce MITM, proteggere gli asset e mantenere l'integrità del business, offrendo tutti gli strumenti e le competenze necessari per eseguire in tutta sicurezza le attività di rilevamento, risposta e ripristino.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi MITM, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi MITM →

Torna agli scenari



Dispositivi affidabili ›

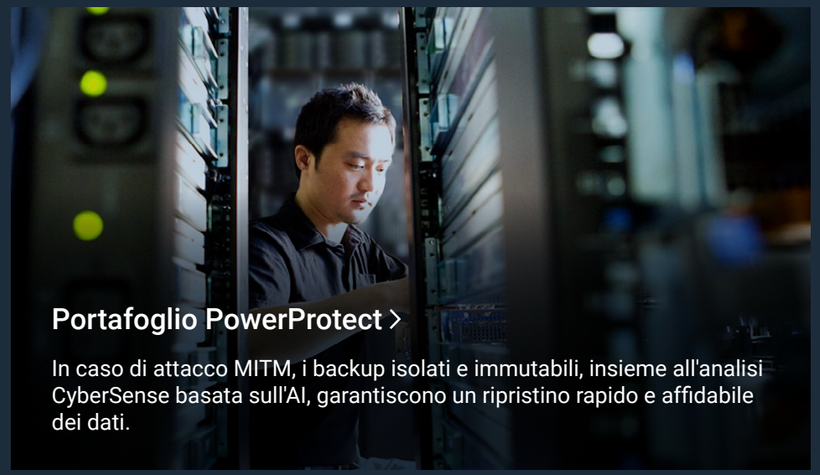
Dell protegge endpoint e dati in transito avvalendosi di autenticazione hardware, misure di protezione del firmware, come SafeBIOS e SafeID, crittografia affidabile e framework Zero Trust.

Server PowerEdge ›

Avvio sicuro, Silicon Root of Trust, gestione dinamica delle porte USB e blocco dei sistemi assicurano l'integrità dell'hardware e proteggono i carichi di lavoro critici dalle minacce provenienti dalla rete.

Soluzioni di storage ›

La crittografia dei dati inattivi e in transito, combinata con gli snapshot isolati e le funzionalità di ripristino rapido, garantisce la sicurezza dei file e consente di ripristinarli velocemente in caso di attacco MITM.

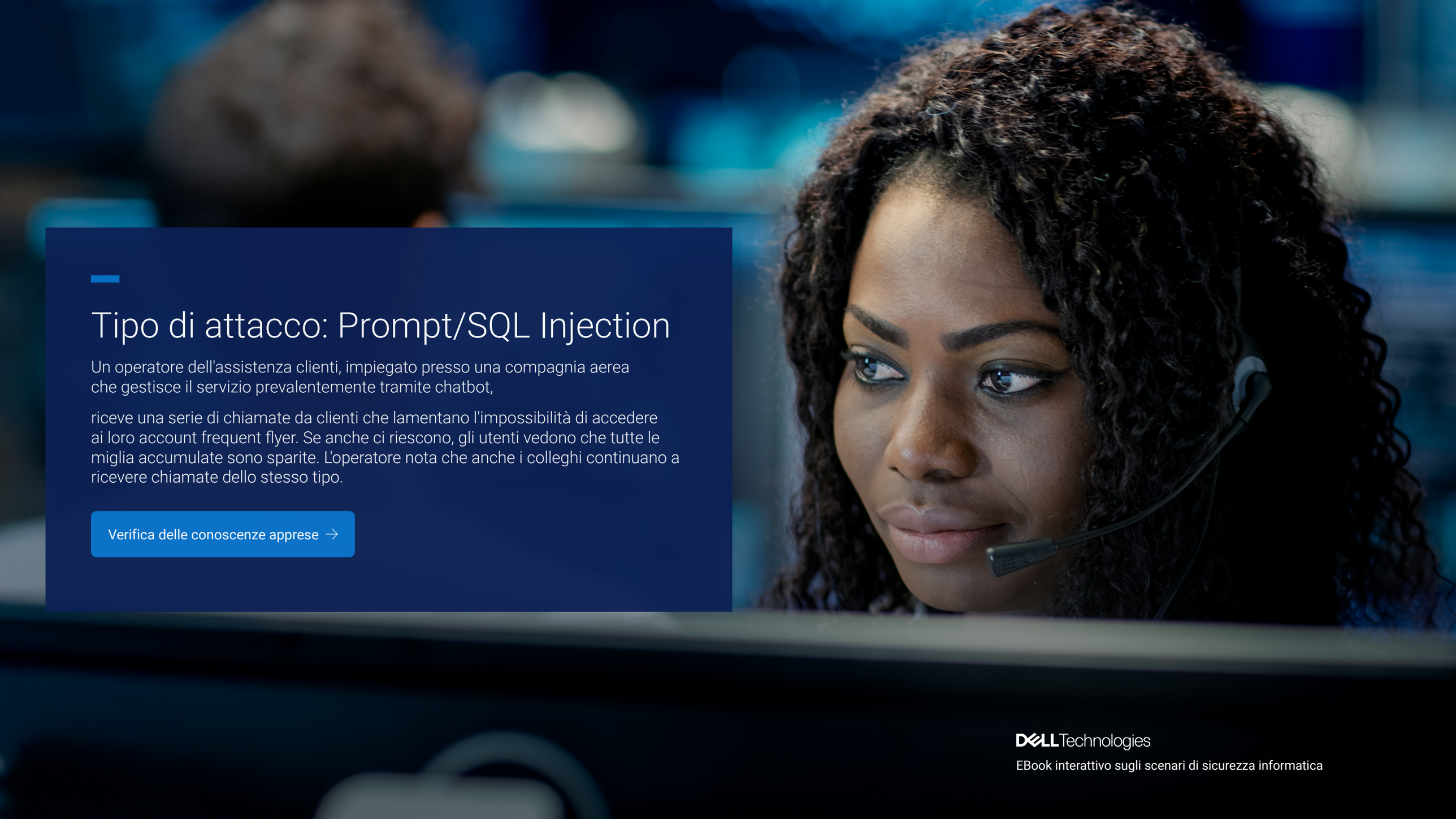


Portafoglio PowerProtect ›

In caso di attacco MITM, i backup isolati e immutabili, insieme all'analisi CyberSense basata sull'AI, garantiscono un ripristino rapido e affidabile dei dati.

Servizi di sicurezza e resilienza ›

Dalla valutazione delle vulnerabilità alla formazione degli utenti, fino ai test di penetrazione e alla risposta agli incidenti, gli esperti e i partner Dell forniscono un supporto completo per rafforzare le difese.



Tipo di attacco: Prompt/SQL Injection

Un operatore dell'assistenza clienti, impiegato presso una compagnia aerea che gestisce il servizio prevalentemente tramite chatbot,

riceve una serie di chiamate da clienti che lamentano l'impossibilità di accedere ai loro account frequent flyer. Se anche ci riescono, gli utenti vedono che tutte le miglia accumulate sono sparite. L'operatore nota che anche i colleghi continuano a ricevere chiamate dello stesso tipo.

Verifica delle conoscenze apprese →

Tipo di attacco: Prompt/SQL Injection

1. Riduzione della superficie di attacco
2
3
4

Durante l'indagine nota che i log contengono errori come *Syntax error in Structured Query Language (SQL) statement o Invalid column name 'admin'*. Di quale tipo di incidente informatico si tratta?

- [ ] Furto di credenziali
- [ ] Attacco di Prompt/SQL Injection
- [ ] Attacco Man-in-the-Middle
- [ ] Phishing

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1. Riduzione della superficie di attacco
2
3
4

Durante l'indagine nota che i log contengono errori come *Syntax error in Structured Query Language (SQL) statement* o *Invalid column name 'admin'*. Di quale tipo di incidente informatico si tratta?

- ✗ Furto di credenziali
- ✓ Attacco di Prompt/SQL Injection
- ✗ Attacco Man-in-the-Middle
- ✗ Phishing

Si tratta di un attacco di "Prompt/SQL Injection", perché la registrazione di errori come "Syntax error in SQL statement" o "Invalid column name 'admin'" nei log indica che l'autore dell'attacco sfrutta i campi di input del chatbot per inserire codice SQL nocivo al fine di accedere ai dati degli account dei clienti, o di alterarli. Questi indicatori tecnici sono un chiaro sintomo di un attacco di SQL Injection, che corrisponde all'attività sospetta descritta.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

L'operatore capisce di aver subito un attacco di Prompt/SQL Injection tramite il chatbot dell'assistenza clienti. Che cosa devi fare?

- [ ] Disconnettere il chatbot
- [ ] Analizzare i log di database per individuare l'accesso non autorizzato e i dati rubati, modificati o eliminati
- [ ] Adempiere a tutti gli obblighi previsti dalle leggi sulla divulgazione dei dati in seguito a una violazione
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

L'operatore capisce di aver subito un attacco di Prompt/SQL Injection tramite il chatbot dell'assistenza clienti. Che cosa devi fare?

- [x] Disconnettere il chatbot
- [x] Analizzare i log di database per individuare l'accesso non autorizzato e i dati rubati, modificati o eliminati
- [x] Adempiere a tutti gli obblighi previsti dalle leggi sulla divulgazione dei dati in seguito a una violazione
- [x] Tutte le opzioni precedenti

Per rispondere a un attacco di Prompt/SQL Injection è necessario disconnettere il chatbot, esaminare i log di database per individuare l'accesso non autorizzato e garantire la conformità alle leggi sulla divulgazione dei dati. Queste operazioni sono essenziali per impedire l'exploit, valutare i danni e adempiere agli obblighi etici e normativi.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 — 2 — 3. Ripristino da un attacco informatico — 4

Quali misure è necessario adottare per bloccare l'attacco di Prompt/SQL Injection?

- [ ] Chiedere ai team di sviluppo di utilizzare istruzioni preparate e query parametrizzate nelle loro pratiche di programmazione
- [ ] Utilizzare strumenti Manage Detection and Response (MDR)
- [ ] Applicare il principio del privilegio minimo agli accessi, utilizzando ad esempio l'autenticazione a più fattori (MFA), il controllo degli accessi basato sul ruolo (RBAC), Web Application Firewall (WAF) e così via
- [ ] Segmentare i database back-end e la Knowledge Base

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 — 2 — 3. Ripristino da un attacco informatico — 4

Quali misure è necessario adottare per bloccare l'attacco di Prompt/SQL Injection?

- ✓ Chiedere ai team di sviluppo di utilizzare istruzioni preparate e query parametrizzate nelle loro pratiche di programmazione
- ✗ Utilizzare strumenti Manage Detection and Response (MDR)
- ✓ Applicare il principio del privilegio minimo agli accessi, utilizzando ad esempio l'autenticazione a più fattori (MFA), il controllo degli accessi basato sul ruolo (RBAC), Web Application Firewall (WAF) e così via
- ✗ Segmentare i database back-end e la Knowledge Base

La richiesta di utilizzare istruzioni preparate e query parametrizzate durante le attività di programmazione dei team di sviluppo consente di bloccare gli attacchi SQL Injection all'origine. Se si applica anche il principio del privilegio minimo agli accessi, ad esempio tramite autenticazione a più fattori (MFA), RBAC e WAF, è possibile limitare l'impatto di qualsiasi tentativo di Injection, impedendo ai malintenzionati di aumentare i privilegi acquisiti o di spostarsi lateralmente.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 2 3 4. Best practice generali

Cosa bisogna fare per recuperare i dati dei clienti della compagnia aerea?

- [ ] Rintracciare i dati rubati
- [ ] Chiedere ai clienti di ricostruire i loro profili
- [ ] Riacquistali dagli autori dell'attacco informatico
- [ ] Ripristinare l'ultimo backup non compromesso per recuperare i dati relativi alle miglia accumulate, quindi chiedere ai clienti di modificare le password e controllare le carte di credito

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: Prompt/SQL Injection

1 2 3 4. Best practice generali

Cosa bisogna fare per recuperare i dati dei clienti della compagnia aerea?

- ✗ Rintracciare i dati rubati
- ✗ Chiedere ai clienti di ricostruire i loro profili
- ✗ Riacquistali dagli autori dell'attacco informatico
- ✓ Ripristinare l'ultimo backup non compromesso per recuperare i dati relativi alle miglia accumulate, quindi chiedere ai clienti di modificare le password e controllare le carte di credito

Il ripristino dei dati persi dall'ultimo backup non compromesso contribuisce a mantenere l'integrità dei dati e ridurre i tempi di fermo. Per garantire ulteriormente la conformità alle normative in seguito a un attacco distruttivo, occorre anche chiedere tempestivamente ai clienti di reimpostare le password e monitorare l'attività sulle carte di credito.

Scopri le soluzioni →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

TIPO DI ATTACCO: PROMPT/SQL INJECTION

Conclusioni

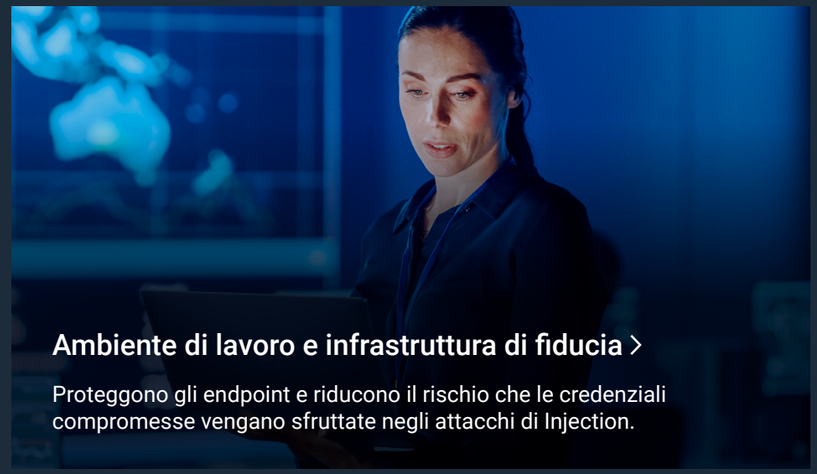
Gli attacchi di Prompt/SQL Injection hanno ripetutamente dimostrato di essere fra i metodi più dannosi e pervasivi utilizzati dai criminali informatici. Sfruttano le vulnerabilità presenti nei sistemi di database o query degli utenti, consentendo ai malintenzionati di manipolare server, rubare dati o interrompere i flussi di lavoro.

Nell'ambito del suo costante impegno per la sicurezza informatica, Dell protegge le aziende da minacce e attacchi di Prompt/SQL Injection in continua evoluzione e fornisce tutti gli strumenti e le competenze necessari per il rilevamento, la risposta e il ripristino.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi di Prompt/SQL Injection, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi di Prompt/SQL Injection →

Torna agli scenari

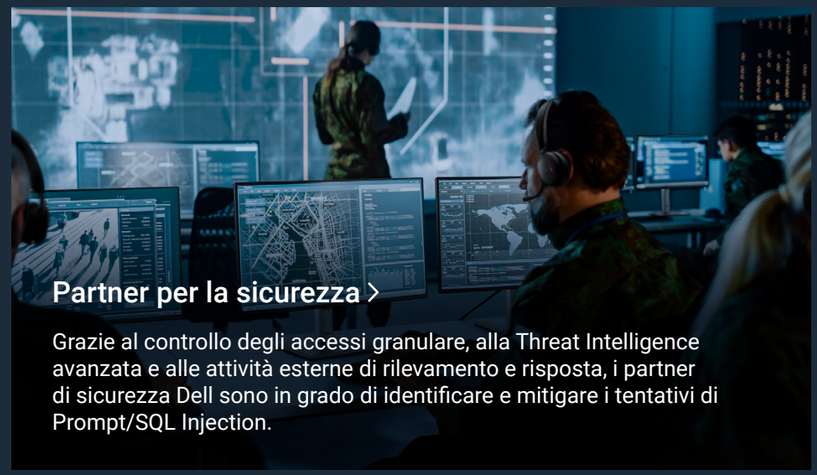


Ambiente di lavoro e infrastruttura di fiducia ›

Proteggono gli endpoint e riducono il rischio che le credenziali compromesse vengano sfruttate negli attacchi di Injection.

Server PowerEdge ›

Dotati di Root of Trust hardware, avvio sicuro, sicurezza a livello di circuito e convalida della configurazione in tempo reale, i server Dell PowerEdge garantiscono un'infrastruttura resistente alle manomissioni, che esegue solo codice affidabile.



Partner per la sicurezza ›

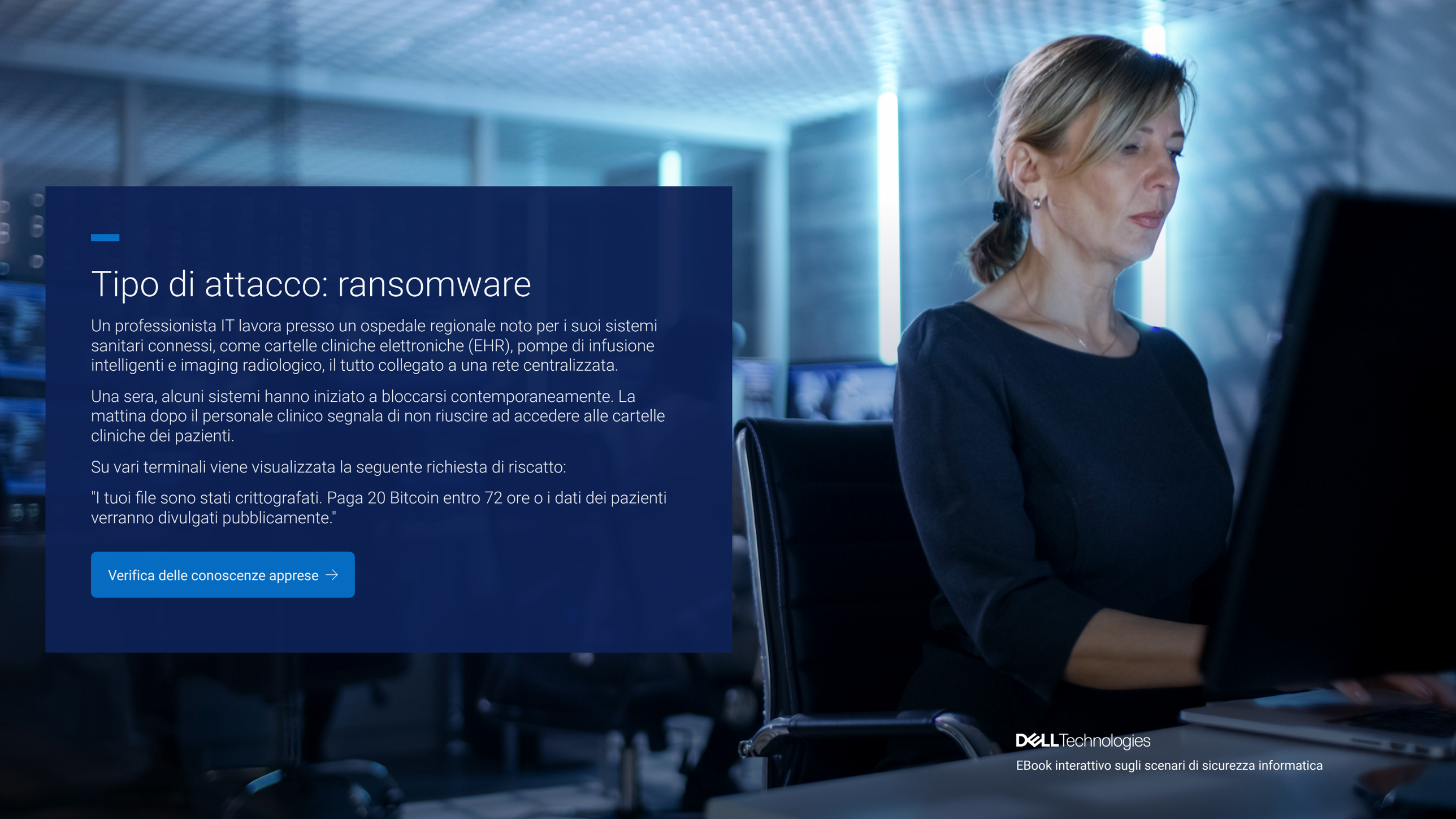
Grazie al controllo degli accessi granulare, alla Threat Intelligence avanzata e alle attività esterne di rilevamento e risposta, i partner di sicurezza Dell sono in grado di identificare e mitigare i tentativi di Prompt/SQL Injection.

Portafoglio PowerProtect ›

I backup immutabili e isolati tramite air-gap di Dell, insieme all'analisi avanzata del Cyber Recovery dopo un attacco informatico, garantiscono punti di ripristino affidabili per l'esecuzione di un ripristino rapido in caso di danneggiamento o esfiltrazione dei dati.

Servizi di sicurezza e resilienza ›

Dalla formazione allo sviluppo e dai test di penetrazione sicuri alla ricerca delle minacce, fino alla risposta agli incidenti, gli esperti e i partner Dell aiutano le aziende a convalidare le misure di protezione e garantiscono una risposta rapida agli attacchi di Injection.



Tipo di attacco: ransomware

Un professionista IT lavora presso un ospedale regionale noto per i suoi sistemi sanitari connessi, come cartelle cliniche elettroniche (EHR), pompe di infusione intelligenti e imaging radiologico, il tutto collegato a una rete centralizzata.

Una sera, alcuni sistemi hanno iniziato a bloccarsi contemporaneamente. La mattina dopo il personale clinico segnala di non riuscire ad accedere alle cartelle cliniche dei pazienti.

Su vari terminali viene visualizzata la seguente richiesta di riscatto:

"I tuoi file sono stati crittografati. Paga 20 Bitcoin entro 72 ore o i dati dei pazienti verranno divulgati pubblicamente."

Verifica delle conoscenze apprese →

Tipo di attacco: ransomware

1. Riduzione della superficie di attacco
2
3
4

L'help desk riceve oltre 100 segnalazioni di errore delle applicazioni e della crittografia dei file. I log di sicurezza mostrano un'attività di ridenominazione dei file insolita da un account del dominio interno. Qual è il passo successivo?

- [ ] Pagare immediatamente il riscatto per ripristinare i servizi critici
- [ ] Informare le forze dell'ordine e il consulente legale
- [ ] Iniziare a riapplicare l'immagine a tutti gli endpoint interessati
- [ ] Disconnettere i sistemi infetti dalla rete

Selezionare la risposta corretta →

Tipo di attacco: ransomware

1. Riduzione della superficie di attacco
2
3
4

L'help desk riceve oltre 100 segnalazioni di errore delle applicazioni e della crittografia dei file. I log di sicurezza mostrano un'attività di ridenominazione dei file insolita da un account del dominio interno. Qual è il passo successivo?

- ✗ Pagare immediatamente il riscatto per ripristinare i servizi critici
- ✗ Informare le forze dell'ordine e il consulente legale
- ✗ Iniziare a riapplicare l'immagine a tutti gli endpoint interessati
- ✓ Disconnettere i sistemi infetti dalla rete

Disconnettere e isolare immediatamente i sistemi ospedalieri infetti impedisce la diffusione del ransomware, protegge i dispositivi sanitari critici e i dati sensibili dei pazienti, conserva le prove per l'indagine e permette di recuperare il tempo necessario per coordinare la risposta e il ripristino.

Domanda successiva →

Tipo di attacco: ransomware

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il team di risposta agli incidenti scopre che, probabilmente, l'attacco è partito da un account compromesso utilizzato per accedere a un server senza eseguire l'autenticazione a più fattori (MFA). Quale di questi elementi ha contribuito più direttamente all'attacco?

- [ ] Definizioni antivirus obsolete
- [ ] Database EHR (Electronic Health Record) esposto
- [ ] Mancanza di MFA per l'accesso remoto
- [ ] Filtraggio e-mail inefficace

Selezionare la risposta corretta →

Tipo di attacco: ransomware

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il team di risposta agli incidenti scopre che, probabilmente, l'attacco è partito da un account compromesso utilizzato per accedere a un server senza eseguire l'autenticazione a più fattori (MFA). Quale di questi elementi ha contribuito più direttamente all'attacco?

- ✗ Definizioni antivirus obsolete
- ✗ Database EHR (Electronic Health Record) esposto
- ✓ Mancanza di MFA per l'accesso remoto
- ✗ Filtraggio e-mail inefficace

La mancanza di MFA per l'accesso remoto ha consentito la violazione del server, permettendo ai malintenzionati di effettuare l'accesso tramite credenziali rubate o indovinate, senza eseguire ulteriori passaggi di verifica. Con l'MFA, anche gli account compromessi richiedono un secondo fattore, e questo riduce drasticamente il rischio di accesso non autorizzato.

Domanda successiva →

Tipo di attacco: ransomware

1 — 2 — 3. Ripristino da un attacco informatico — 4

Il personale medico deve ricorrere a flussi di lavoro cartacei. I pazienti pianificati per un intervento chirurgico in giornata non possono essere verificati nel sistema. Qual è la migliore misura a breve termine da adottare per supportare le attività ospedaliere?

- [ ] Riavviare il server del database essenziale per tentare la reinizializzazione
- [ ] Abilitare tutti i backup precedenti, anche se risalgono a sei mesi prima
- [ ] Attivare le procedure manuali di downtime dell'ospedale ed eseguire l'escalation al team di emergenza
- [ ] Consentire al personale decida come procedere caso per caso

Selezionare la risposta corretta →

Tipo di attacco: ransomware

1 2 3. Ripristino da un attacco informatico 4

Il personale medico deve ricorrere a flussi di lavoro cartacei. I pazienti pianificati per un intervento chirurgico in giornata non possono essere verificati nel sistema. Qual è la migliore misura a breve termine da adottare per supportare le attività ospedaliere?

- ✗ Riavviare il server del database essenziale per tentare la reinizializzazione
- ✗ Abilitare tutti i backup precedenti, anche se risalgono a sei mesi prima
- ✓ Attivare le procedure manuali di downtime dell'ospedale ed eseguire l'escalation al team di emergenza
- ✗ Consentire al personale decida come procedere caso per caso

L'attivazione delle procedure manuali di downtime e l'escalation al team di emergenza garantiscono la ripresa immediata dei flussi di lavoro clinici essenziali, tutelano la sicurezza dei pazienti e introducono un processo standard per la verifica e la documentazione delle cure. Questo approccio riduce al minimo gli errori, garantisce una gestione efficiente di rischi e risorse, mentre aiuta gli esperti a ripristinare i sistemi digitali in tutta sicurezza.

Domanda successiva →

Tipo di attacco: ransomware

1 2 3 4. Best practice generali

I media locali sono venuti a conoscenza dell'incidente. La leadership vuole sapere se è necessario rilasciare una dichiarazione pubblica e l'ufficio legale chiede informazioni in merito agli obblighi HIPAA (Health Insurance Portability and Accountability Act). Qual è il passaggio successivo più appropriato?

- [ ] Negare pubblicamente l'incidente fino a quando non saranno disponibili ulteriori informazioni
- [ ] Rilasciare un comunicato stampa che attribuisce la colpa al fornitore IT di terze parti
- [ ] Avvisare le autorità e avviare le procedure interne di segnalazione delle violazioni
- [ ] Pagare immediatamente il riscatto ed evitate la divulgazione pubblica

Selezionare la risposta corretta →

Tipo di attacco: ransomware

1 2 3 4. Best practice generali

I media locali sono venuti a conoscenza dell'incidente. La leadership vuole sapere se è necessario rilasciare una dichiarazione pubblica e l'ufficio legale chiede informazioni in merito agli obblighi HIPAA (Health Insurance Portability and Accountability Act). Qual è il passaggio successivo più appropriato?

- ✗ Negare pubblicamente l'incidente fino a quando non saranno disponibili ulteriori informazioni
- ✗ Rilasciare un comunicato stampa che attribuisce la colpa al fornitore IT di terze parti
- ✓ Avvisare le autorità e avviare le procedure interne di segnalazione delle violazioni
- ✗ Pagare immediatamente il riscatto ed evitate la divulgazione pubblica

Per garantire la conformità alle normative, la protezione legale e la trasparenza delle best practice allo scopo di prevenire conseguenze legali e reputazionali, rispettando gli obblighi di divulgazione e assicurando una comunicazione adeguata con pazienti, personale e stakeholder, occorre segnalare tempestivamente la violazione dei dati sanitari protetti alle autorità e alle persone interessate, come richiesto dall'HIPAA e dalle leggi statali.

Scopri le soluzioni →

TIPO DI ATTACCO: RANSOMWARE

Conclusioni

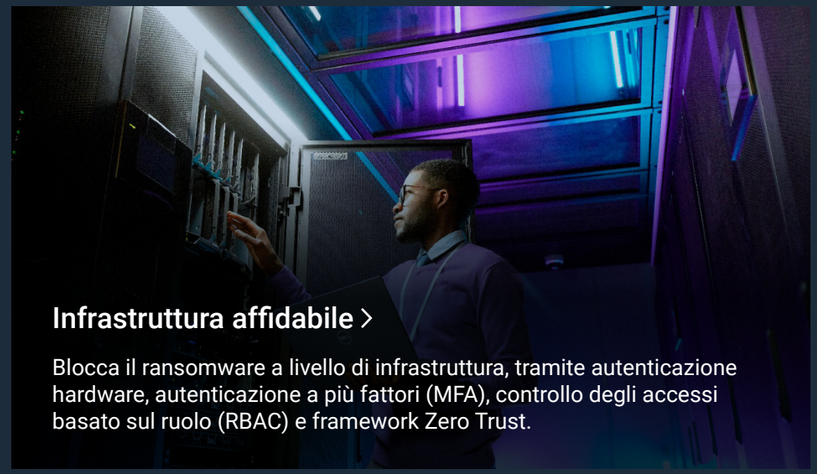
Il ransomware è un tipo di malware che blocca l'accesso a un sistema informatico o ai dati fino a quando non viene pagato un riscatto. È uno degli attacchi informatici in grado di causare più danni potenziali. L'anno scorso, il 50% delle organizzazioni a livello globale è stato colpito da ransomware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

Dell presta la massima attenzione alla tutela delle aziende, tramite framework Zero Trust, protezione degli endpoint e segmentazione della rete, per bloccare l'accesso al ransomware e limitarne la diffusione. I nostri esperti pianificano la risposta agli incidenti per aiutarle a rimanere resilienti e a ripristinare rapidamente l'operatività in seguito a un attacco.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi ransomware, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi ransomware →

Torna agli scenari



Infrastruttura affidabile ›

Blocca il ransomware a livello di infrastruttura, tramite autenticazione hardware, autenticazione a più fattori (MFA), controllo degli accessi basato sul ruolo (RBAC) e framework Zero Trust.

Server di rete e PowerEdge ›

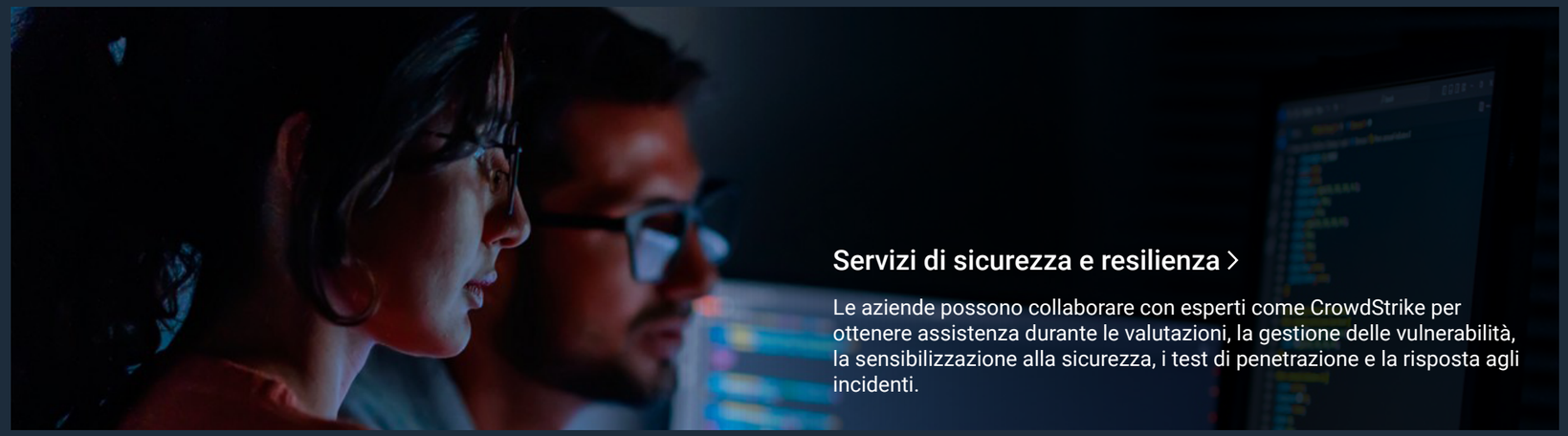
Limitano gli spostamenti del ransomware tramite segmentazione della rete, avvio sicuro, Silicon Root of Trust, gestione dinamica delle porte USB e blocco dei sistemi.

Ambiente di lavoro affidabile ›

Integra SafeBIOS, SafeID, SafeData e strumenti EDR (Endpoint Detection and Response) per fornire Threat Intelligence proattiva, rilevamento in tempo reale e contenimento automatizzato del malware a livello di dispositivo.

Portafoglio PowerProtect ›

Protegge i dati critici con backup immutabili e isolati tramite air-gap, analisi intelligente del Cyber Recovery dopo un attacco informatico e funzionalità di ripristino rapido, allo scopo di prevenire l'estorsione e garantire la resilienza.



Servizi di sicurezza e resilienza ›

Le aziende possono collaborare con esperti come CrowdStrike per ottenere assistenza durante le valutazioni, la gestione delle vulnerabilità, la sensibilizzazione alla sicurezza, i test di penetrazione e la risposta agli incidenti.

Tipo di attacco: componenti hardware della supply chain

Un'azienda distribuisce 500 nuovi notebook nei suoi uffici di tutto il mondo. Per velocizzare le operazioni, esternalizza la preparazione dell'imaging e dell'hardware a una ditta esterna che fornisce servizi logistici per l'IT. Il fornitore spedisce i sistemi preconfigurati direttamente ai dipendenti.

Dopo alcuni giorni l'azienda riceve diverse chiamate dal personale sul campo, che indicano quanto segue:

- Le richieste di autenticazione a più fattori (MFA) vengono ignorate o non funzionano correttamente.
- Il team di sicurezza rileva un numero degli accessi amministrativi non autorizzati in orari insoliti.
- Inoltre, viene rilevato traffico VPN di utenti che dovrebbero essere offline.

Verifica delle conoscenze apprese →

Tipo di attacco: componenti hardware della supply chain

1. Riduzione della superficie di attacco
2
3
4

Un dipendente segnala di ricevere notifiche push di autenticazione a più fattori (MFA) quando non tenta di accedere. Il dashboard di sicurezza dell'azienda mostra che l'accesso è stato effettuato da un dispositivo con un codice asset fornito dall'azienda. Qual è il primo passo più logico per il team Security Operations Center (SOC)?

- [ ] Disabilitare l'account dell'utente e cancellare il notebook da remoto
- [ ] Confrontare l'indirizzo IP di accesso e l'impronta digitale del dispositivo in questione con quelli di altri utenti compromessi noti
- [ ] Eseguire l'escalation alle risorse umane, presupponendo un errore dell'utente
- [ ] Emanare un avviso a livello aziendale, per richiedere la modifica immediata delle password

Selezionare la risposta corretta →

Tipo di attacco: componenti hardware della supply chain

1. Riduzione della superficie di attacco
2
3
4

Un dipendente segnala di ricevere notifiche push di autenticazione a più fattori (MFA) quando non tenta di accedere. Il dashboard di sicurezza dell'azienda mostra che l'accesso è stato effettuato da un dispositivo con un codice asset fornito dall'azienda. Qual è il primo passo più logico per il team Security Operations Center (SOC)?

- ✗ Disabilitare l'account dell'utente e cancellare il notebook da remoto
- ✓ Confrontare l'indirizzo IP di accesso e l'impronta digitale del dispositivo in questione con quelli di altri utenti compromessi noti
- ✗ Eseguire l'escalation alle risorse umane, presupponendo un errore dell'utente
- ✗ Emanare un avviso a livello aziendale, per richiedere la modifica immediata delle password

Quando il team SOC cerca di determinare se un'attività sospetta è un incidente isolato o rientra in un attacco su vasta scala, per consentire il riconoscimento rapido dei pattern, il primo passo logico dopo l'identificazione di un attacco dovuto all'hardware della supply chain è costituito dalla risposta mirata all'incidente seguita dal contenimento dei rischi associati.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: componenti hardware della supply chain

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il team di risposta agli incidenti rileva che alcuni dei notebook interessati eseguono versioni del firmware SSD non corrispondenti alle note di rilascio ufficiali del fornitore. La funzione EDR non mostra processi dannosi. Cosa indica tutto questo, più probabilmente?

- [ ] Errore di configurazione del vendor IT
- [ ] Un nuovo tipo di ransomware che si elimina da solo
- [ ] Una compromissione della supply chain a livello di firmware
- [ ] Un comportamento normale durante l'imaging

Selezionare la risposta corretta →

Tipo di attacco: componenti hardware della supply chain

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il team di risposta agli incidenti rileva che alcuni dei notebook interessati eseguono versioni del firmware SSD non corrispondenti alle note di rilascio ufficiali del fornitore. La funzione EDR non mostra processi dannosi. Cosa indica tutto questo, più probabilmente?

- ✗ Errore di configurazione del vendor IT
- ✗ Un nuovo tipo di ransomware che si elimina da solo
- ✓ Una compromissione della supply chain a livello di firmware
- ✗ Un comportamento normale durante l'imaging

Il firmware SSD non autorizzato su più notebook, non rilevato dall'EDR e non corrispondente alle versioni ufficiali, indica una manomissione intenzionale dell'hardware o del firmware, tipico della compromissione della supply chain a livello di firmware.

Domanda successiva →

Tipo di attacco: componenti hardware della supply chain

1 — 2 — 3. Ripristino da un attacco informatico — 4

Sono stati isolati 100 dispositivi sospetti con firmware SSD non autorizzato. È necessario decidere come procedere senza informare l'autore dell'attacco, che potrebbe avere accesso remoto. Qual è la mossa successiva ottimale?

- [ ] Spegnere tutti i dispositivi e sottoporli all'analisi forense
- [ ] Eseguire dump della memoria in tempo reale e analizzare i sistemi mentre sono in esecuzione
- [ ] Segnalare la violazione al fornitore esterno
- [ ] Cancellare tutti i dispositivi e ridistribuire nuovi notebook a tutti gli utenti, a livello globale

Selezionare la risposta corretta →

Tipo di attacco: componenti hardware della supply chain

1 — 2 — 3. Ripristino da un attacco informatico — 4

Sono stati isolati 100 dispositivi sospetti con firmware SSD non autorizzato. È necessario decidere come procedere senza informare l'autore dell'attacco, che potrebbe avere accesso remoto. Qual è la mossa successiva ottimale?

- ✗ Spegnere tutti i dispositivi e sottoporli all'analisi forense
- ✓ Eseguire dump della memoria in tempo reale e analizzare i sistemi mentre sono in esecuzione
- ✗ Segnalare la violazione al fornitore esterno
- ✗ Cancellare tutti i dispositivi e ridistribuire nuovi notebook a tutti gli utenti, a livello globale

I dump di memoria in tempo reale sono fondamentali per preservare le prove volatili, come il malware e i rootkit attivi, consentendo una risposta mirata agli incidenti attraverso la scoperta di minacce nascoste e punti di accesso prima che vengano persi o che l'autore dell'attacco venga informato.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: componenti hardware della supply chain

1 2 3 4. Best practice generali

Il Chief Information Security Officer richiede una sintesi sulla modalità di penetrazione dell'attacco nell'ambiente. È necessario presentare una spiegazione concisa al team esecutivo. Come si può spiegare questo attacco?

- [ ] È stato accidentalmente scaricato un virus da un collegamento di phishing
- [ ] È stata riscontrato un errore di configurazione della rete che ha consentito l'accesso dall'esterno
- [ ] Il firmware dannoso è stato introdotto da un fornitore hardware, che è stato compromesso durante il provisioning del notebook
- [ ] Uno dei nostri sviluppatori ha introdotto codice non sicuro nell'ambiente di produzione

Selezionare la risposta corretta →

Tipo di attacco: componenti hardware della supply chain

1 2 3 4. Best practice generali

Il Chief Information Security Officer richiede una sintesi sulla modalità di penetrazione dell'attacco nell'ambiente. È necessario presentare una spiegazione concisa al team esecutivo. Come si può spiegare questo attacco?

- ✗ È stato accidentalmente scaricato un virus da un collegamento di phishing
- ✗ È stata riscontrato un errore di configurazione della rete che ha consentito l'accesso dall'esterno
- ✓ Il firmware dannoso è stato introdotto da un fornitore hardware, che è stato compromesso durante il provisioning del notebook
- ✗ Uno dei nostri sviluppatori ha introdotto codice non sicuro nell'ambiente di produzione

Le versioni del firmware non corrispondenti e l'assenza di malware attivi confermano che si tratta di un attacco a livello di firmware originato dal fornitore, non di un errore dell'utente o di una configurazione errata.

Scopri le soluzioni →

TIPO DI ATTACCO: COMPONENTI HARDWARE DELLA SUPPLY CHAIN

Conclusioni

Gli attacchi alla supply chain sono cresciuti notevolmente negli ultimi anni. Attraverso la manomissione dei dispositivi fisici durante la produzione, la spedizione o il deployment oppure l'individuazione dei punti deboli dei fornitori di software, gli autori degli attacchi riescono a introdurre componenti o codici dannosi, danneggiare i sistemi o esfiltrare i dati sensibili. Le vittime, che spaziano dalle piccole imprese alle multinazionali, si trovano quindi a dover affrontare gravi perdite finanziarie, perdita di fiducia da parte dei clienti e ripercussioni legali.

Dell mitiga gli attacchi hardware della supply chain integrando rigorosi assessment dei rischi associati ai fornitori e integrando i principi Zero Trust, insieme alla convalida continua dei dispositivi e ai controlli di integrità indipendenti. Rafforziamo l'integrità durante l'intero ciclo di vita dell'hardware.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi che sfruttano l'hardware della supply chain, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi che sfruttano l'hardware della supply chain →

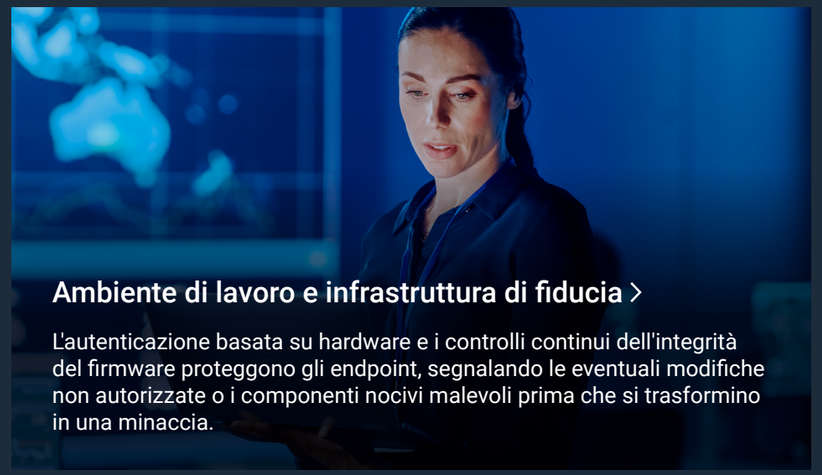
Torna agli scenari

Garanzia della supply chain ›

Grazie ai controlli avanzati della provenienza, alla logistica a prova di manomissione e all'approvvigionamento trasparente, la supply chain di Dell garantisce una verifica rigorosa di hardware, firmware e fornitori prima dell'invio dei sistemi all'azienda.

Secure Component Verification (SCV) ›

La verifica crittografica dei componenti dei PC in fabbrica e durante l'installazione garantisce l'autenticità, rileva le alterazioni nascoste e riduce i rischi di manomissione della supply chain.



Ambiente di lavoro e infrastruttura di fiducia ›

L'autenticazione basata su hardware e i controlli continui dell'integrità del firmware proteggono gli endpoint, segnalando le eventuali modifiche non autorizzate o i componenti nocivi malevoli prima che si trasformino in una minaccia.

Monitoraggio degli asset e ProSupport Suite con SupportAssist ›

Il monitoraggio completo degli asset, il monitoraggio in tempo reale della provenienza dei dispositivi e la verifica proattiva dell'integrità garantiscono il rilevamento rapido delle anomalie e la sicurezza dell'intera flotta.

Partner per la sicurezza: rilevamento e risposta basati sull'AI ›

Gli strumenti di sicurezza basati sull'AI garantiscono il monitoraggio continuo, le indagini forensi e il contenimento automatizzato di manomissioni o comportamenti anomali dei dispositivi, assicurando interventi rapidi contro le minacce provenienti dalla supply chain.

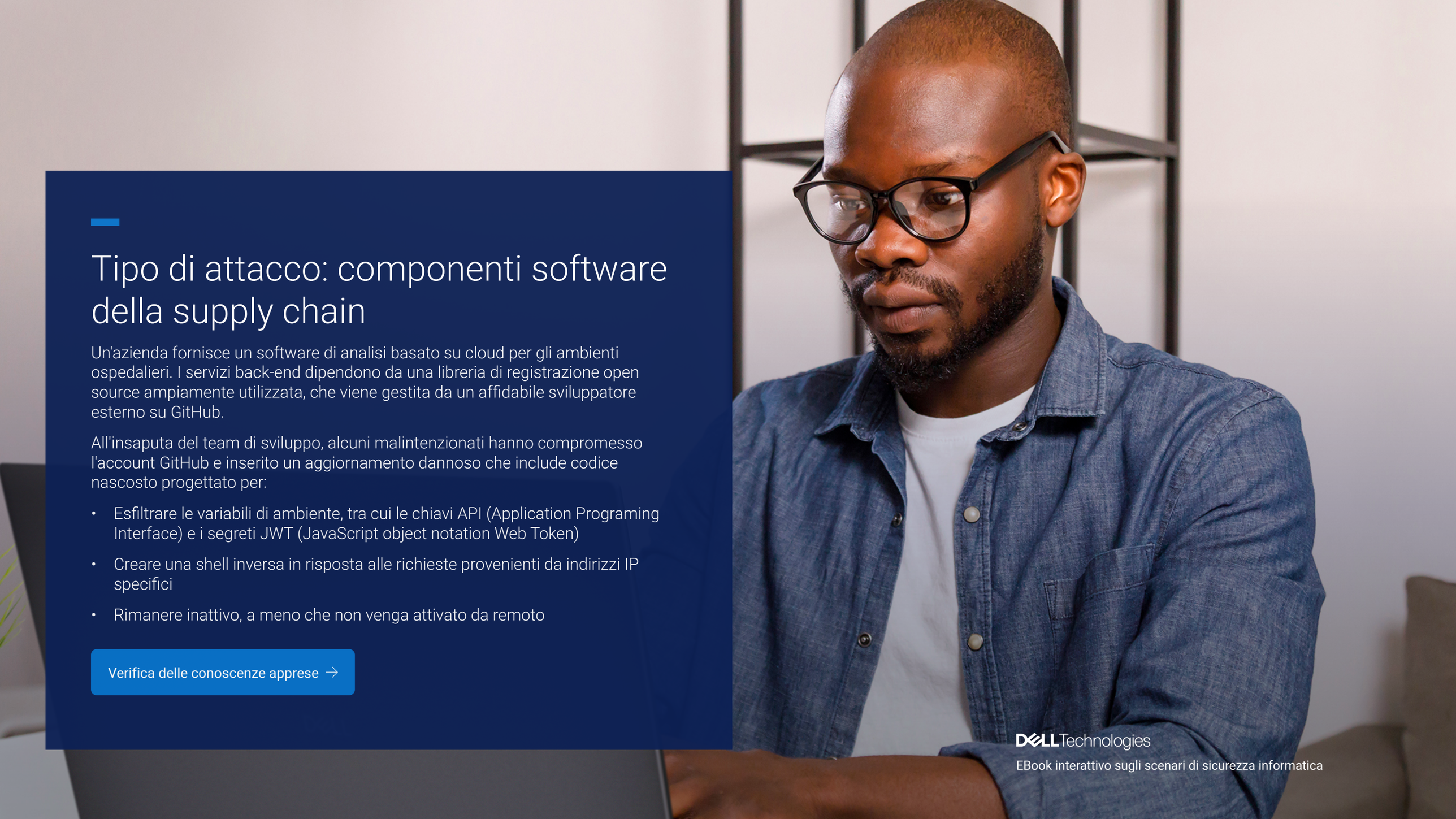
Tipo di attacco: componenti software della supply chain

Un'azienda fornisce un software di analisi basato su cloud per gli ambienti ospedalieri. I servizi back-end dipendono da una libreria di registrazione open source ampiamente utilizzata, che viene gestita da un affidabile sviluppatore esterno su GitHub.

All'insaputa del team di sviluppo, alcuni malintenzionati hanno compromesso l'account GitHub e inserito un aggiornamento dannoso che include codice nascosto progettato per:

- Esfiltrare le variabili di ambiente, tra cui le chiavi API (Application Programing Interface) e i segreti JWT (JavaScript object notation Web Token)
- Creare una shell inversa in risposta alle richieste provenienti da indirizzi IP specifici
- Rimanere inattivo, a meno che non venga attivato da remoto

Verifica delle conoscenze apprese →



Tipo di attacco: componenti software della supply chain

1. Riduzione della superficie di attacco
2
3
4

L'API inizia improvvisamente a restituire 500 errori ai client chiave. Il monitoraggio cloud rileva connessioni in uscita dai servizi containerizzati a un dominio mai visto prima. Qual è la prima misura da adottare come risposta?

- [ ] Disabilitare tutto il traffico di rete in uscita dai container
- [ ] Riavviare i servizi interessati per cancellare gli eventuali problemi di memoria
- [ ] Verificare la presenza di commit di codice recenti nel repository GitHub
- [ ] Contattare il provider di hosting del dominio

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: componenti software della supply chain

1. Riduzione della superficie di attacco
2
3
4

L'API inizia improvvisamente a restituire 500 errori ai client chiave. Il monitoraggio cloud rileva connessioni in uscita dai servizi containerizzati a un dominio mai visto prima. Qual è la prima misura da adottare come risposta?

- ✓ Disabilitare tutto il traffico di rete in uscita dai container
- ✗ Riavviare i servizi interessati per cancellare gli eventuali problemi di memoria
- ✗ Verificare la presenza di commit di codice recenti nel repository GitHub
- ✗ Contattare il provider di hosting del dominio

La disabilitazione di tutto il traffico di rete in uscita dai container blocca immediatamente i tentativi degli hacker di esfiltrare i dati sensibili o di accedere da remoto tramite la libreria di registrazione compromessa, isolando l'ambiente in tempo reale e recuperando tempo essenziale per analizzare, proteggere le chiavi o i segreti API e impedire l'attivazione di meccanismi di attacco dormienti.

Domanda successiva →

Tipo di attacco: componenti software della supply chain

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il responsabile tecnico conferma che il codice dell'applicazione è stato estratto automaticamente da GitHub tre giorni prima dell'inizio dei problemi. Tale versione non è ancora stata contrassegnata come dannosa in alcun database pubblico. Qual è l'azione immediata più responsabile?

- [ ] Contattare il gestore della libreria direttamente tramite GitHub
- [ ] Eliminare tutte le dipendenze dal progetto locale e ricostruirlo
- [ ] Attendere la pubblicazione delle CVE (Common Vulnerabilities and Exposure) prima di intraprendere ulteriori azioni
- [ ] Eseguire il rollback all'ultima versione del codice nota come sicura

Selezionare la risposta corretta →

Tipo di attacco: componenti software della supply chain

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Il responsabile tecnico conferma che il codice dell'applicazione è stato estratto automaticamente da GitHub tre giorni prima dell'inizio dei problemi. Tale versione non è ancora stata contrassegnata come dannosa in alcun database pubblico. Qual è l'azione immediata più responsabile?

- ✗ Contattare il gestore della libreria direttamente tramite GitHub
- ✗ Eliminare tutte le dipendenze dal progetto locale e ricostruirlo
- ✗ Attendere la pubblicazione delle CVE (Common Vulnerabilities and Exposure) prima di intraprendere ulteriori azioni
- ✓ Eseguire il rollback all'ultima versione del codice nota come sicura

Il rollback all'ultima versione del codice nota come sicura rimuove immediatamente l'aggiornamento compromesso, elimina il punto di appoggio dell'autore dell'attacco e ripristina l'integrità operativa, per contenere i rischi e proteggere i dati sensibili in modo proattivo.

Domanda successiva →

Tipo di attacco: componenti software della supply chain

1 — 2 — 3. Ripristino da un attacco informatico — 4

L'analisi conferma che la libreria esfiltrava le chiavi API e le credenziali cloud. Sono stati identificati vari container creati con la versione compromessa. Qual è il passaggio più critico nella strategia di contenimento?

- [ ] Revocare e ruotare tutte le credenziali negli ambienti interessati
- [ ] Riapplicare ai container un'immagine aggiornata del sistema operativo
- [ ] Cancellare i notebook del team di sviluppo
- [ ] Inviare un avviso di disattivazione per il repository GitHub

Selezionare la risposta corretta →

Tipo di attacco: componenti software della supply chain

1 — 2 — 3. Ripristino da un attacco informatico — 4

L'analisi conferma che la libreria esfiltrava le chiavi API e le credenziali cloud. Sono stati identificati vari container creati con la versione compromessa. Qual è il passaggio più critico nella strategia di contenimento?

- ✓ Revocare e ruotare tutte le credenziali negli ambienti interessati
- ✗ Riapplicare ai container un'immagine aggiornata del sistema operativo
- ✗ Cancellare i notebook del team di sviluppo
- ✗ Inviare un avviso di disattivazione per il repository GitHub

Dopo una compromissione del cloud, il primo passo critico è costituito dalla revoca e dalla rotazione delle credenziali, per impedire agli hacker di accedere ai servizi, impedire il furto dei dati e proteggere i sistemi indipendentemente dalla portata della violazione.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: componenti software della supply chain

1 2 3 4. Best practice generali

È necessario spiegare l'accaduto al Chief Technology Officer, all'Ufficio legale e al team per la conformità. Qual è la spiegazione più chiara e precisa? Come si può riassumere l'incidente?

- [ ] Gli strumenti CI/CD (Continuous Deployment/Delivery) interni sono risultati inefficaci e hanno permesso il deployment di codice non valido
- [ ] Una dipendenza software esterna è stata compromessa e i nostri servizi di automazione l'hanno inserita nell'ambiente di produzione
- [ ] Uno sviluppatore ha incluso codice non testato in una versione urgente
- [ ] Un malintenzionato ha forzato il repository GitHub

Selezionare la risposta corretta →

Tipo di attacco: componenti software della supply chain

1 2 3 4. Best practice generali

È necessario spiegare l'accaduto al Chief Technology Officer, all'Ufficio legale e al team per la conformità. Qual è la spiegazione più chiara e precisa? Come si può riassumere l'incidente?

- ✗ Gli strumenti CI/CD (Continuous Deployment/Delivery) interni sono risultati inefficaci e hanno permesso il deployment di codice non valido
- ✓ Una dipendenza software esterna è stata compromessa e i nostri servizi di automazione l'hanno inserita nell'ambiente di produzione
- ✗ Uno sviluppatore ha incluso codice non testato in una versione urgente
- ✗ Un malintenzionato ha forzato il repository GitHub

La causa alla radice è costituita da un attacco alla supply chain. Gli autori hanno compromesso una dipendenza software esterna e il processo di creazione automatizzato ha applicato l'aggiornamento dannoso direttamente all'ambiente di produzione, compromettendo l'integrità delle applicazioni e gli ambienti sensibili, facendo emergere il rischio di aggiornamento dannoso delle dipendenze esterne ritenute affidabili.

Scopri le soluzioni →

TIPO DI ATTACCO: COMPONENTI SOFTWARE DELLA SUPPLY CHAIN

Conclusioni

Gli attacchi informatici al software proveniente dalla supply chain sfruttano le vulnerabilità negli aggiornamenti software, nelle integrazioni di terze parti e negli ambienti di sviluppo per incorporare codice dannoso da diffondere in rete. Questi attacchi possono causare violazioni dei dati su vasta scala, interrompere le operazioni e compromettere interi ecosistemi, danneggiando aziende di tutte le dimensioni.

Dell si impegna a garantire cyber-resilienza attraverso la trasparenza, lo sviluppo sicuro e il monitoraggio continuo, mantenendo al contempo un solido piano di risposta agli incidenti per garantire il ripristino rapido e la comunicazione con gli stakeholder.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi che sfruttano il software della supply chain, fare clic sul pulsante sotto.

Informazioni sintetiche sugli attacchi che sfruttano il software della supply chain →

Torna agli scenari

Garanzia della supply chain >

Grazie ai controlli avanzati della provenienza, alla logistica a prova di manomissione e all'approvvigionamento trasparente, la supply chain di Dell garantisce una verifica rigorosa di hardware, firmware e fornitori prima dell'invio dei sistemi all'azienda.

Secure Development Lifecycle (SDL) >

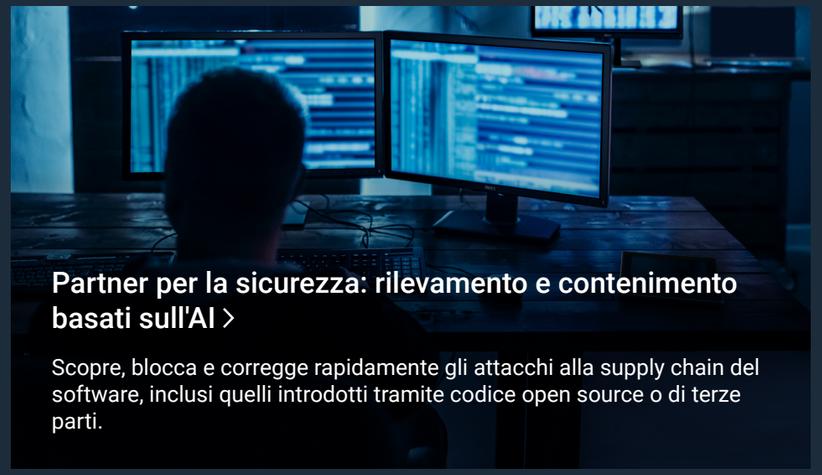
Implementa pratiche di sviluppo sicure, leader del settore, allo scopo di ridurre i rischi derivanti dalle dipendenze esterne e prevenire gli attacchi basati su software nelle soluzioni fornite.

Ambiente di lavoro e infrastruttura di fiducia >

L'autenticazione hardware tramite SafeBIOS, SafeID e SafeDataDelivers garantisce che gli endpoint eseguano solo codice attendibile e rilevino tempestivamente le modifiche non autorizzate o nocive al software.

Monitoraggio degli asset e ProSupport Suite con SupportAssist >

Il monitoraggio in tempo reale di software e dispositivi consente di rilevare tempestivamente le anomalie introdotte nella supply chain e rispondere velocemente.



Partner per la sicurezza: rilevamento e contenimento basati sull'AI >

Scopre, blocca e corregge rapidamente gli attacchi alla supply chain del software, inclusi quelli introdotti tramite codice open source o di terze parti.

Tipo di attacco: zero-day

Un analista della sicurezza monitora i log di autenticazione di un'azienda. Di recente, gli utenti hanno segnalato l'accesso non autorizzato ai propri account, anche se non hanno condiviso le loro credenziali.

Dall'analisi dei log emergono la attività seguenti:

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

In parallelo, un ricercatore che si occupa di sicurezza identifica una vulnerabilità nell'API (Application Programming Interface):

- I token JWT non scadono mai.
- I token vengono memorizzati nello storage locale, anziché nei cookie solo HTTP.
- Non viene applicata alcuna autenticazione a più fattori (MFA).

Verifica delle conoscenze apprese →

Tipo di attacco: zero-day

1. Riduzione della superficie di attacco
2
3
4

Poiché non sono state attivate notifiche di allarme, il team di sicurezza sospetta che si tratti di un attacco zero-day. Cosa bisogna fare per verificarlo?

- [ ] Disconnettere tutti gli utenti dai relativi sistemi
- [ ] Identificare i principali comportamenti di autenticazione anomali nei log
- [ ] Chiamare colleghi che lavorano in altre aziende per verificare se hanno lo stesso problema
- [ ] Provare a stabilire una correlazione con altre attività di sicurezza anomale

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1. Riduzione della superficie di attacco
2
3
4

Poiché non sono state attivate notifiche di allarme, il team di sicurezza sospetta che si tratti di un attacco zero-day. Cosa bisogna fare per verificarlo?

- ✗ Disconnettere tutti gli utenti dai relativi sistemi
- ✓ Identificare i principali comportamenti di autenticazione anomali nei log
- ✗ Chiamare colleghi che lavorano in altre aziende per verificare se hanno lo stesso problema
- ✓ Provare a stabilire una correlazione con altre attività di sicurezza anomale

L'individuazione di comportamenti di autenticazione anomali, come orari di accesso insoliti, riutilizzo delle credenziali o accesso da dispositivi atipici, e la correlazione con altre attività di sicurezza anomale, quali anomalie di accesso ai dati o escalation dei privilegi, confermano un attacco zero-day coordinato.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Poiché la vulnerabilità è sconosciuta, i team di sicurezza devono limitare i danni durante le indagini. Cosa devono fare?

- [ ] Invalidare tutte le sessioni di autenticazione a livello di sistema
- [ ] Concentrare tutte le risorse sul punto di ingresso dell'attacco
- [ ] Consentire solo gli accessi che utilizzano l'autenticazione a più fattori (MFA)
- [ ] Affidarsi alle regole statiche attuali del firewall e del Web Application Firewall (WAF)

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 — 2. Rilevamento e risposta alle minacce informatiche — 3 — 4

Poiché la vulnerabilità è sconosciuta, i team di sicurezza devono limitare i danni durante le indagini. Cosa devono fare?

- ✓ Invalidare tutte le sessioni di autenticazione a livello di sistema
- ✗ Concentrare tutte le risorse sul punto di ingresso dell'attacco
- ✓ Consentire solo gli accessi che utilizzano l'autenticazione a più fattori (MFA)
- ✗ Affidarsi alle regole statiche attuali del firewall e del Web Application Firewall (WAF)

Insieme, queste misure rafforzano la sicurezza e riducono al minimo i rischi, oltre a impedire l'accesso ai malintenzionati, per lasciare ai team di sicurezza il tempo di analizzare ed eliminare la vulnerabilità sottostante.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 2 3. Ripristino da un attacco informatico 4

I PC Dell integrano tecnologie come avvio sicuro, TPM (Trusted Platform Module), protezione della password del BIOS e SafeBIOS. In che modo possono aiutare a contrastare un attacco zero-day?

- [ ] Proteggono dagli attacchi di dump delle credenziali che rubano token API (Application Programming Interface)
- [ ] Impediscono ai malintenzionati con accesso fisico di eludere la sicurezza del sistema operativo per installare malware che ruba token di autenticazione
- [ ] Impediscono ai malintenzionati di manipolare le impostazioni del BIOS per indebolire la sicurezza del sistema operativo nell'intento di dirottare le sessioni API
- [ ] Tutte le opzioni precedenti

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 2 3. Ripristino da un attacco informatico 4

I PC Dell integrano tecnologie come avvio sicuro, TPM (Trusted Platform Module), protezione della password del BIOS e SafeBIOS. In che modo possono aiutare a contrastare un attacco zero-day?

- [x] Proteggono dagli attacchi di dump delle credenziali che rubano token API (Application Programming Interface)
- [x] Impediscono ai malintenzionati con accesso fisico di eludere la sicurezza del sistema operativo per installare malware che ruba token di autenticazione
- [x] Impediscono ai malintenzionati di manipolare le impostazioni del BIOS per indebolire la sicurezza del sistema operativo nell'intento di dirottare le sessioni API
- [x] Tutte le opzioni precedenti

Questo approccio multilivello fornisce una protezione completa dagli attacchi zero-day contro BIOS, firmware, credenziali e configurazioni di sistema. Queste tecnologie impediscono la manipolazione, l'accesso non autorizzato o il furto di credenziali, e rimangono efficaci anche quando i malintenzionati scoprono nuove vulnerabilità.

Domanda successiva →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 2 3 4. Best practice generali

Qual è il modo migliore per evitare gli attacchi zero-day?

- [ ] Evitare l'utilizzo di software open source
- [ ] Adottare i principi Zero Trust
- [ ] Applicare regolarmente tutte le patch, incluse quelle per sistemi operativi, firmware, API, librerie e container
- [ ] Installare un cancello elettrificato attorno all'azienda per impedire l'accesso ai malintenzionati

Selezionare la risposta corretta →

DELL Technologies

EBook interattivo sugli scenari di sicurezza informatica

Tipo di attacco: zero-day

1 2 3 4. Best practice generali

Qual è il modo migliore per evitare gli attacchi zero-day?

- ✗ Evitare l'utilizzo di software open source
- ✓ Adottare i principi Zero Trust
- ✗ Applicare regolarmente tutte le patch, incluse quelle per sistemi operativi, firmware, API, librerie e container
- ✗ Installare un cancello elettrificato attorno all'azienda per impedire l'accesso ai malintenzionati

Se esistono vulnerabilità sconosciute o sistemi privi di patch, i principi Zero Trust impediscono di considerare implicitamente attendibili gli utenti e i dispositivi, applicano l'autenticazione continua, limitano l'accesso alle sole informazioni necessarie e frenano gli spostamenti dei malintenzionati, per ridurre drasticamente il rischio associato alle minacce non rilevate e prevenire gli attacchi zero-day.

Scopri le soluzioni →

TIPO DI ATTACCO: ZERO-DAY

Conclusioni

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

Dell affronta gli attacchi zero-day tramite controlli Zero Trust, segmentazione della rete, contenimento rapido e formazione degli utenti, rafforzando ulteriormente le difese contro le minacce emergenti.

Per ottenere ulteriori informazioni sulle strategie avanzate di cyber-resilienza e scoprire cosa può fare Dell per proteggere le aziende dagli attacchi zero-day, fare clic sul pulsante sotto

Informazioni sintetiche sugli attacchi zero-day →

Torna agli scenari

Ambiente di lavoro e infrastruttura di fiducia ›

Difendono gli endpoint e l'infrastruttura. Tramite le funzioni di protezione SafeBIOS, SafeID e SafeData, a cui si aggiunge il framework Zero Trust che prevede l'autenticazione a più fattori (MFA) e il controllo degli accessi basato sui ruolo (RBAC), Dell offre difese multilivello per limitare i percorsi di exploit e garantire l'autenticazione hardware.

Server PowerEdge ›

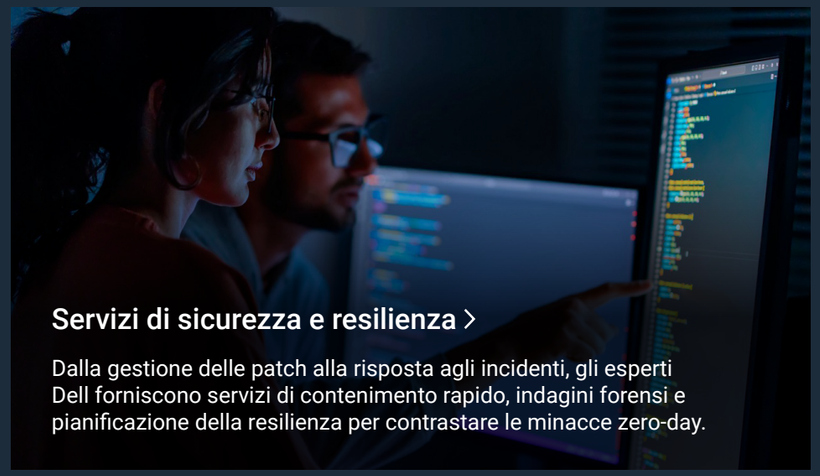
Secure Boot, Silicon Root of Trust e la segmentazione della rete tramite SmartFabric limitano i movimenti laterali, garantendo che sull'infrastruttura venga eseguito solo codice attendibile.

Partner per la sicurezza ›

Threat Intelligence avanzata, Managed Detection and Response (MDR), eXtended Detection and Response (XDR) e controllo granulare degli accessi consentono di rilevare, ricercare e contenere gli attacchi zero-day prima che si diffondano.

Portafoglio PowerProtect ›

I backup immutabili, i vault isolati per il Cyber Recovery dopo un attacco informatico e l'analisi CyberSense basata sull'AI accelerano il ripristino e aumentano la resilienza dopo le violazioni zero-day.



Servizi di sicurezza e resilienza ›

Dalla gestione delle patch alla risposta agli incidenti, gli esperti Dell forniscono servizi di contenimento rapido, indagini forensi e pianificazione della resilienza per contrastare le minacce zero-day.


DELL Technologies