DELL Technologies

INTERAKTIVES E-BOOK ZU CYBERSICHERHEITSSZENARIEN

Reale Szenarien. Intelligentere Entscheidungen. Stärkere Abwehrmaßnahmen.

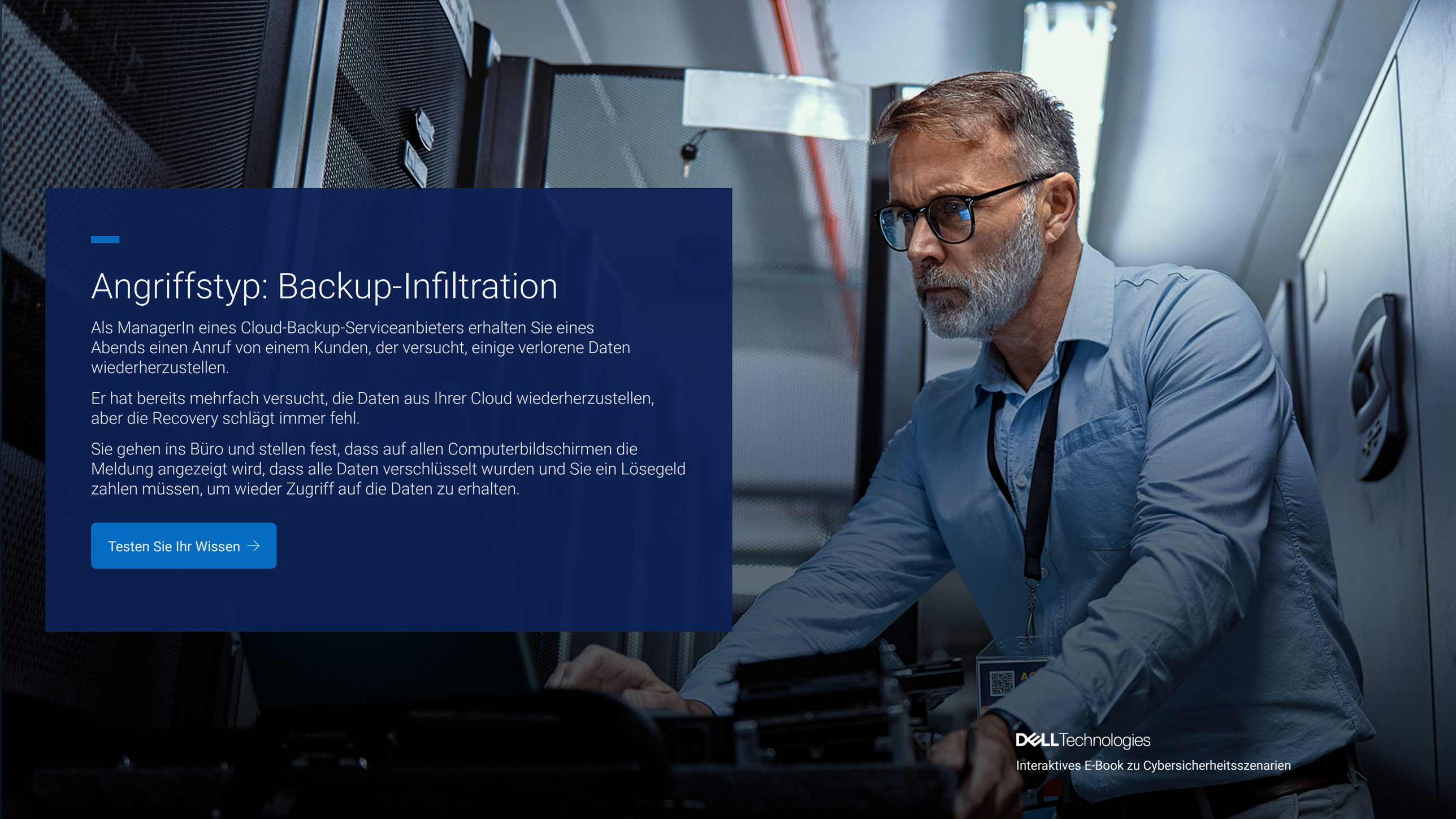
Das Engagement von Dell für Sicherheit steht im Mittelpunkt unseres Handelns. In Form von Erkenntnissen, Best Practices und innovativen Technologien soll dieses E-Book Ihnen die Tools und Kenntnisse vermitteln, die Sie benötigen, um neuen Cyberrisiken einen Schritt voraus zu sein.

Wählen Sie ein Angriffsszenario aus

Cybersicherheitsbedrohungen entwickeln sich ständig weiter und Unternehmen müssen effektiv reagieren, um ihre Daten zu schützen. Um Ihr Unternehmen optimal vorzubereiten, beschäftigen Sie sich intensiv mit realitätsnahen Simulationsübungen, die Ihnen dabei helfen, Ihre Cybersicherheitsstrategien zur Bekämpfung von Cyberangriffen zu optimieren.

Lernen Sie verschiedene Angriffstypen und branchenspezifische Herausforderungen in Sektoren wie Bundes-, Landes- und Kommunalbehörden, Finanzdienstleistungen und Gesundheitswesen kennen. Dabei erfahren Sie, wie die integrierten Sicherheitslösungen von Dell – von Laptops und Desktop-PCs bis hin zu Enterprise-Systemen – auf den Schutz vor diesen Bedrohungen ausgelegt sind.

- Backup-Infiltration →
- Ransomware →
- Distributed Denial of Service (DDoS) →
- Hardware in der Lieferkette →
- Bösartige Insider →
- Software in der Lieferkette →
- Man-in-the-Middle (MITM) →
- Zero-Day →
- Prompt-/SQL-Injection →



Angriffstyp: Backup-Infiltration

Als ManagerIn eines Cloud-Backup-Serviceanbieters erhalten Sie eines Abends einen Anruf von einem Kunden, der versucht, einige verlorene Daten wiederherzustellen.

Er hat bereits mehrfach versucht, die Daten aus Ihrer Cloud wiederherzustellen, aber die Recovery schlägt immer fehl.

Sie gehen ins Büro und stellen fest, dass auf allen Computerbildschirmen die Meldung angezeigt wird, dass alle Daten verschlüsselt wurden und Sie ein Lösegeld zahlen müssen, um wieder Zugriff auf die Daten zu erhalten.

Testen Sie Ihr Wissen →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Sie sind nicht sicher, welche Backupsysteme oder Kunden betroffen sind. Was sollte Ihr erster Schritt sein?

- [ ] Behörden benachrichtigen
- [ ] Alle Systeme herunterfahren
- [ ] Versuchen, die Bedrohung einzudämmen und zu isolieren
- [ ] Ermitteln, ob ein sauberes Backup zur Wiederherstellung verfügbar ist

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Sie sind nicht sicher, welche Backupsysteme oder Kunden betroffen sind. Was sollte Ihr erster Schritt sein?

- ✗ Behörden benachrichtigen
- ✗ Alle Systeme herunterfahren
- ✓ Versuchen, die Bedrohung einzudämmen und zu isolieren
- ✗ Ermitteln, ob ein sauberes Backup zur Wiederherstellung verfügbar ist

Die sofortige Eindämmung und Isolierung einer Bedrohung verhindert weitere Ausbreitung oder Schäden und verschafft Zeit, um das Ausmaß des Incidents zu beurteilen. Dadurch können die Auswirkungen aller Arten von Cyberangriffen, einschließlich solcher mit KI-Beteiligung, potenziell minimiert werden.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihre Priorität ist es, Ihren Kunden deren Daten schnell wieder zur Verfügung zu stellen. Wie können Sie das erreichen?

- [ ] Lösegeld zahlen
- [ ] Ransomware-Variante identifizieren
- [ ] Behörden benachrichtigen
- [ ] Kompromittierte Daten identifizieren

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihre Priorität ist es, Ihren Kunden deren Daten schnell wieder zur Verfügung zu stellen. Wie können Sie das erreichen?

- ✗ Lösegeld zahlen
- ✗ Ransomware-Variante identifizieren
- ✗ Behörden benachrichtigen
- ✓ Kompromittierte Daten identifizieren

Durch die Identifizierung der kompromittierten Daten können Sie die Recovery auf die Wiederherstellung der wichtigsten Kundeninformationen konzentrieren, eine schnellere Datenverfügbarkeit gewährleisten und unnötige Arbeit an nicht betroffenen Systemen vermeiden.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Sie stellen fest, dass ein Backup zur Wiederherstellung verfügbar ist. Was sollte der erste Schritt in Ihrem Prozess sein?

- [ ] Zuerst die Wiederherstellung kritischer Systeme priorisieren
- [ ] Mithilfe forensischer Analysen bestätigen, dass der Angriff vollständig eingedämmt ist
- [ ] Alle Kennwörter ändern und kompromittierte Zugangsdaten widerrufen
- [ ] Zero-Trust-Prinzipien umsetzen

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Sie stellen fest, dass ein Backup zur Wiederherstellung verfügbar ist. Was sollte der erste Schritt in Ihrem Prozess sein?

- ✗ Zuerst die Wiederherstellung kritischer Systeme priorisieren
- ✓ Mithilfe forensischer Analysen bestätigen, dass der Angriff vollständig eingedämmt ist
- ✗ Alle Kennwörter ändern und kompromittierte Zugangsdaten widerrufen
- ✗ Zero-Trust-Prinzipien umsetzen

Vor der Wiederherstellung von Systemen müssen Sie sicherstellen, dass der Angriff vollständig eingedämmt ist, um eine versehentliche erneute Infektion und weitere Schäden zu verhindern, damit fortgesetzte oder eskalierende Bedrohungen in Ihrer Umgebung vermieden werden können.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 — 2. — 3 — 4: Allgemeine Best Practices

Was sind potenzielle Möglichkeiten, das Risiko eines solchen Vorfalls in Zukunft zu mindern?

- [ ] Zero-Trust-Prinzipien nutzen
- [ ] EDR-Funktionen (Endpoint Detection and Response) aktivieren
- [ ] Unveränderliche Backups und Air-Gap-Backups implementieren
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Backup-Infiltration

1 2. 3 4: Allgemeine Best Practices

Was sind potenzielle Möglichkeiten, das Risiko eines solchen Vorfalls in Zukunft zu mindern?

- [x] Zero-Trust-Prinzipien nutzen
- [x] EDR-Funktionen (Endpoint Detection and Response) aktivieren
- [x] Unveränderliche Backups und Air-Gap-Backups implementieren
- [x] Alle oben genannten Antworten

Die Anwendung einer mehrschichtigen Verteidigungsstrategie kann das Risiko verringern, den Schaden minimieren und die organisatorische Resilienz erhöhen, da keine einzelne Maßnahme allein ausreicht.

Lösungen entdecken →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

ANGRIFFSTYP: BACKUP-INFILTRATION

Zusammenfassung

Eine Backup-Infiltration liegt vor, wenn Cyberkriminelle Sicherheitslücken in Backupsystemen ausnutzen, um wichtige Wiederherstellungsdaten zu kompromittieren, zu zerstören oder zu verschlüsseln. Diese ausgeklügelten Angriffe können mit anderen Vorfällen wie Ransomware oder Malware-Einsätzen zusammenfallen oder darauf folgen, was die betrieblichen und finanziellen Folgen noch verstärkt.

Wir bei Dell sind davon überzeugt, dass wir Unternehmen in die Lage versetzen können, angesichts sich entwickelnder Cyberbedrohungen resilient zu bleiben. Mit unseren hochmodernen Lösungen, Expertenservices und vertrauenswürdigen Partnerschaften unterstützen wir Sie dabei, das zu schützen, was am wichtigsten ist.

Erfahren Sie mehr über unsere Lösungen und darüber, wie wir die größten Cyberherausforderungen von heute bewältigen.

Kurzbeschreibung zu Backup-Infiltration lesen →

Zurück zu Szenarien

PowerProtect-Portfolio ›

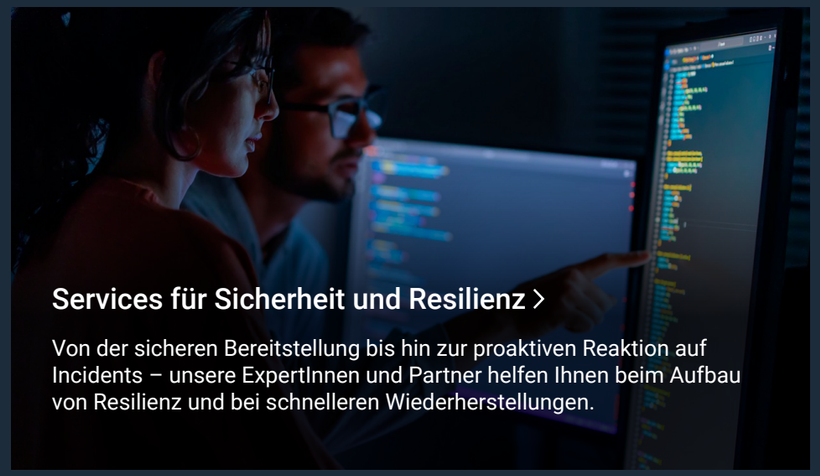
Unsere unveränderlichen, Air-Gap- und verschlüsselten Backup-Vaults, die auf KI-gestützten CyberSense-Analysen basieren, sorgen für eine schnelle Erkennung und Recovery, damit Sie resilient bleiben.

PowerEdge-Server ›

Mit Secure Boot, Hardware Root of Trust und Systemsperre bietet Dell die Infrastruktur, auf die Sie vertrauen können, um Ihre Backups zu schützen.

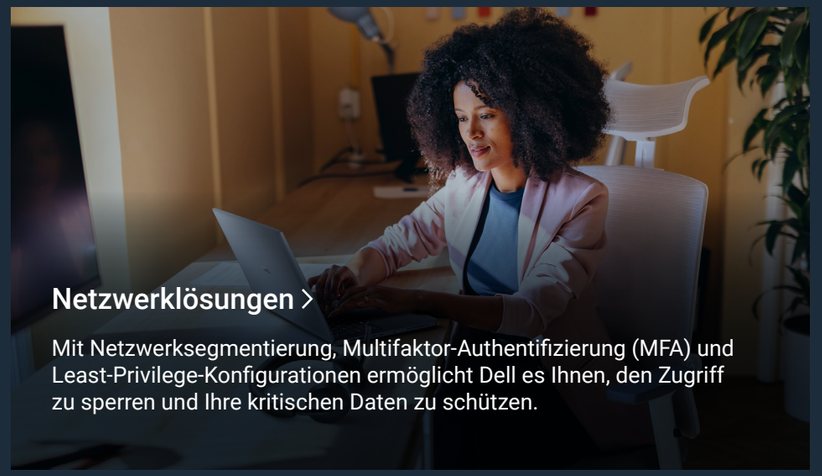
Vertrauenswürdiger Arbeitsplatz ›

SafeBIOS- und SafeData-Schutzmaßnahmen reduzieren Risiken und stellen sicher, dass Ihre Backupsysteme manipulationssicher und einsatzbereit sind, wenn Sie sie benötigen.



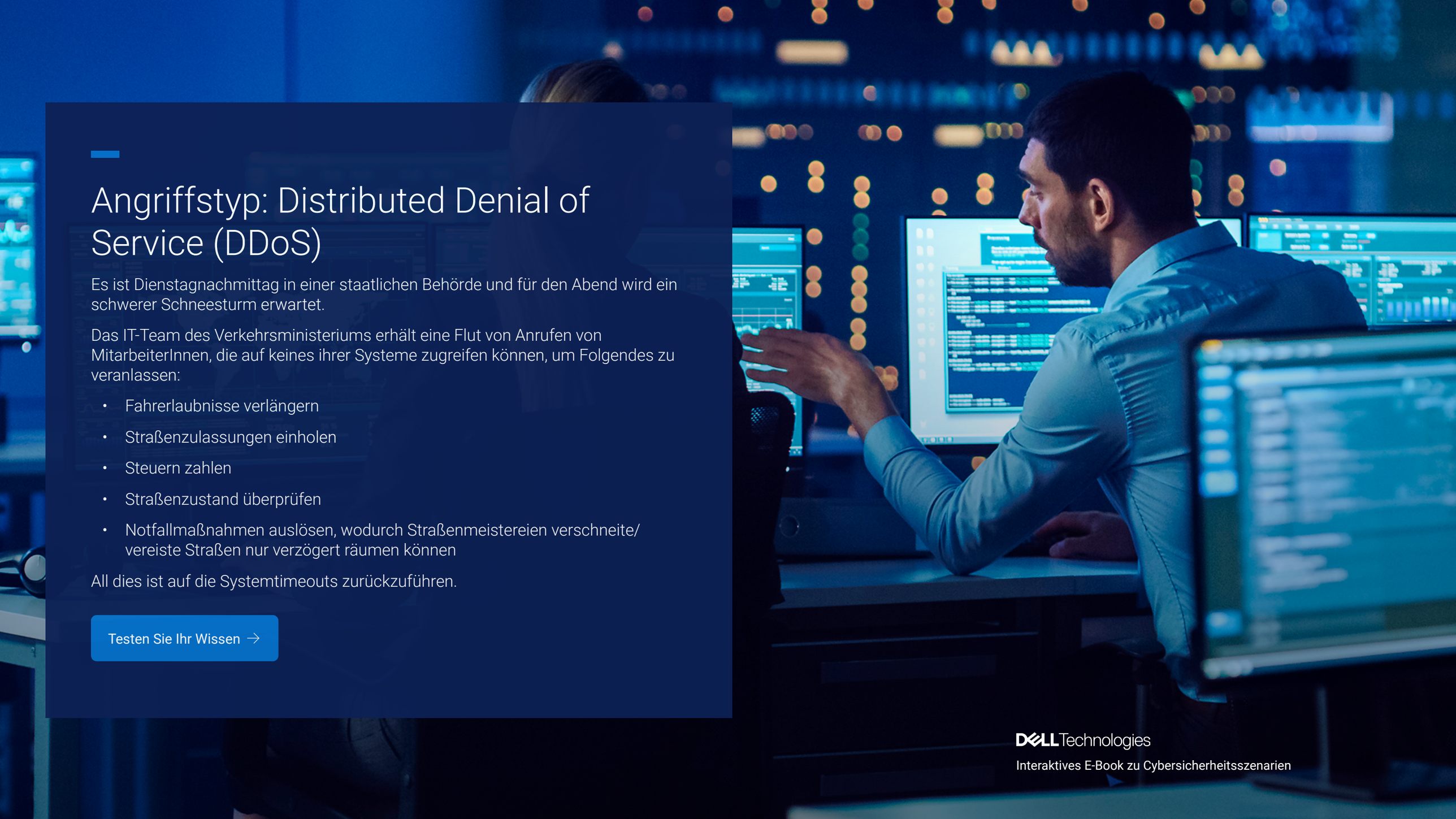
Services für Sicherheit und Resilienz ›

Von der sicheren Bereitstellung bis hin zur proaktiven Reaktion auf Incidents – unsere ExpertInnen und Partner helfen Ihnen beim Aufbau von Resilienz und bei schnelleren Wiederherstellungen.



Netzwerklösungen ›

Mit Netzwerksegmentierung, Multifaktor-Authentifizierung (MFA) und Least-Privilege-Konfigurationen ermöglicht Dell es Ihnen, den Zugriff zu sperren und Ihre kritischen Daten zu schützen.



Angriffstyp: Distributed Denial of Service (DDoS)

Es ist Dienstagnachmittag in einer staatlichen Behörde und für den Abend wird ein schwerer Schneesturm erwartet.

Das IT-Team des Verkehrsministeriums erhält eine Flut von Anrufen von MitarbeiterInnen, die auf keines ihrer Systeme zugreifen können, um Folgendes zu veranlassen:

- Fahrerlaubnisse verlängern
- Straßenzulassungen einholen
- Steuern zahlen
- Straßenzustand überprüfen
- Notfallmaßnahmen auslösen, wodurch Straßenmeistereien verschneite/vereiste Straßen nur verzögert räumen können

All dies ist auf die Systemtimeouts zurückzuführen.

Testen Sie Ihr Wissen →

Angriffstyp: Distributed Denial of Service (DDoS)

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Wo sollte zuerst nachgesehen werden, was passiert sein könnte?

- [ ] Netzwerkgeräte auf plötzliche, unerklärliche Spitzen beim eingehenden Datenverkehr prüfen
- [ ] Netzwerkgeräte auf ungewöhnlichen Datenverkehr von einer einzigen oder nur wenigen IP-Adressen
- [ ] Protokolle der Firewall oder der Netzwerktransparenztools auf übermäßig viele fehlgeschlagene Verbindungen oder Ereignisse prüfen, bei denen der Datenverkehr blockiert wurde
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Wo sollte zuerst nachgesehen werden, was passiert sein könnte?

- [x] Netzwerkgeräte auf plötzliche, unerklärliche Spitzen beim eingehenden Datenverkehr prüfen
- [x] Netzwerkgeräte auf ungewöhnlichen Datenverkehr von einer einzigen oder nur wenigen IP-Adressen
- [x] Protokolle der Firewall oder der Netzwerktransparenztools auf übermäßig viele fehlgeschlagene Verbindungen oder Ereignisse prüfen, bei denen der Datenverkehr blockiert wurde
- [x] Alle oben genannten Antworten

Um weitreichende Systemausfälle ordnungsgemäß zu diagnostizieren, müssen Sie gleichzeitig die Aktivitäten der Netzwerkgeräte und die Protokolle der Firewall oder der Transparenztools überprüfen, um ungewöhnliche Muster oder Blockierungsereignisse schnell zu erkennen. Dies ermöglicht eine schnellere und gezieltere Reaktion auf Vorfälle, da Sie zwischen Cyber-Incidents und Infrastrukturproblemen unterscheiden können.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Sie vermuten, dass es sich um einen DDoS-Angriff handelt. Was ist Ihr erster Schritt?

- [ ] Gesamten Netzwerkverkehr über einen DDoS-Abwehrservice umleiten
- [ ] WAF-Regeln (Web Application Firewall) aktivieren, um bösartige Muster herauszufiltern
- [ ] Überprüfen, ob die Datenverkehrsspitze auf legitime Quellen zurückzuführen ist
- [ ] Vorgänge intern und extern kommunizieren

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Sie vermuten, dass es sich um einen DDoS-Angriff handelt. Was ist Ihr erster Schritt?

- ✗ Gesamten Netzwerkverkehr über einen DDoS-Abwehrservice umleiten
- ✗ WAF-Regeln (Web Application Firewall) aktivieren, um bösartige Muster herauszufiltern
- ✓ Überprüfen, ob die Datenverkehrsspitze auf legitime Quellen zurückzuführen ist
- ✗ Vorgänge intern und extern kommunizieren

Vor dem Ergreifen von DDoS-Gegenmaßnahmen ist es wichtig, die Legitimität einer Datenverkehrsspitze zu überprüfen. Auf diese Weise können Sie vermeiden, dass echte NutzerInnen versehentlich blockiert werden, Störungen für wichtige StakeholderInnen verhindern und sicherstellen, dass weitere Schutzmaßnahmen angemessen und zielgerichtet sind – so können negative Auswirkungen auf den öffentlichen Betrieb und die allgemeine Business Continuity minimiert werden.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche Maßnahmen können Sie ergreifen, um in Zukunft einen DDoS-Angriff zu vermeiden?

- [ ] Betreffende IP-Adressen blockieren
- [ ] Regelmäßige Penetrationstests mit DDoS-Simulationen durchführen
- [ ] Alle Anwendungen in die Cloud verlagern, da Cloud-Anbieter in der Regel nicht Ziel von DDoS-Angriffen sind
- [ ] Zero-Trust-Prinzipien umsetzen

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche Maßnahmen können Sie ergreifen, um in Zukunft einen DDoS-Angriff zu vermeiden?

- ✗ Betreffende IP-Adressen blockieren
- ✓ Regelmäßige Penetrationstests mit DDoS-Simulationen durchführen
- ✗ Alle Anwendungen in die Cloud verlagern, da Cloud-Anbieter in der Regel nicht Ziel von DDoS-Angriffen sind
- ✓ Zero-Trust-Prinzipien umsetzen

Proaktive Penetrationstests mit DDoS-Simulationen identifizieren und schließen Lücken in Ihren Abwehrmaßnahmen, während Zero-Trust-Prinzipien darauf abzielen, Risiken zu minimieren, indem sie jederzeit einen Zugriff mit minimalen Berechtigungen erzwingen. Dies trägt dazu bei, das Risiko einer Unterbrechung wichtiger Systeme wie der Notfallkoordinierung oder der Echtzeitsteuerung von Ampelanlagen zu reduzieren, die auch während eines Angriffs funktionsfähig bleiben müssen.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Distributed Denial of Service (DDoS)

1 2. 3 4: Allgemeine Best Practices

Wen sollten Sie im Rahmen Ihres allgemeinen Notfall- und Wiederherstellungsplans benachrichtigen?

- [ ] Ihre Rechtsabteilung
- [ ] Ihren Cyberversicherungsanbieter
- [ ] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

Angriffstyp: Distributed Denial of Service (DDoS)

1 — 2. — 3 — 4: Allgemeine Best Practices

Wen sollten Sie im Rahmen Ihres allgemeinen Notfall- und Wiederherstellungsplans benachrichtigen?

- [x] Ihre Rechtsabteilung
- [x] Ihren Cyberversicherungsanbieter
- [x] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Alle oben genannten Antworten

Bei einem groß angelegten Cyber-Incident sollten Sie sich hinsichtlich Compliance, Schadensersatzansprüchen und Strafverfolgung mit Ihrer Rechtsabteilung, Ihrer Versicherung und den Regierungsbehörden abstimmen. Nachdem Sie sichergestellt haben, dass alle regulatorischen Anforderungen erfüllt sind, kann Ihre Organisation den Incident effektiv eindämmen, beheben und sich davon erholen.

Lösungen entdecken →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

ANGRIFFSTYP: DISTRIBUTED DENIAL OF SERVICE (DDOS)

Zusammenfassung

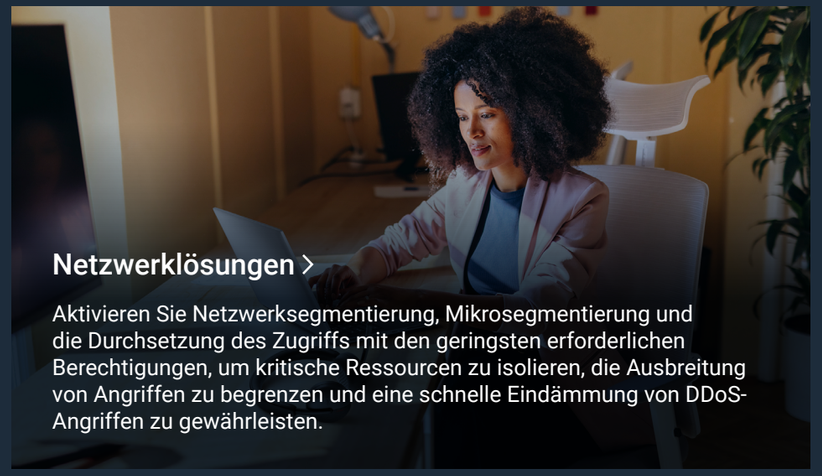
Bei einem DDoS-Angriff wird versucht, den normalen Betrieb eines Netzwerks, Dienstes oder Servers zu stören, indem dieser mit einer enormen Datenmenge aus mehreren Quellen überlastet wird. Diese Angriffe werden mithilfe von Botnets durchgeführt, also Netzwerken infizierter Geräte, die von AngreiferInnen ferngesteuert werden.

Wir bei Dell helfen Unternehmen dabei, widerstandsfähig gegen DDoS-Angriffe zu bleiben, indem wir fortschrittliche Erkennungs- und Abwehrtechnologien mit Expertenservices und einem Zero-Trust-Ansatz kombinieren, um eine schnelle Reaktion, minimale Unterbrechungen und verstärkte Abwehrmaßnahmen sicherzustellen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor DDoS-Angriffen schützen kann.

Kurzbeschreibung zu DDoS lesen →

Zurück zu Szenarien



Netzwerklösungen ›

Aktivieren Sie Netzwerksegmentierung, Mikrosegmentierung und die Durchsetzung des Zugriffs mit den geringsten erforderlichen Berechtigungen, um kritische Ressourcen zu isolieren, die Ausbreitung von Angriffen zu begrenzen und eine schnelle Eindämmung von DDoS-Angriffen zu gewährleisten.

PowerEdge-Server ›

Mit Hardware-Root-of-Trust, Secure Boot, Systemsperre und Manipulationsnachweis in Echtzeit bietet Dell einen resilienten, leistungsstarken DDoS-Schutz und eine beschleunigte Recovery.

Vertrauenswürdige Geräte ›

Integriertes SafeBIOS, SecureData und automatisierte Erkennung und Reaktion reduzieren die Angriffsfläche von Endpunkten um bis zu 70 %, sodass DDoS-basierte Ablenkungsmanöver nicht zu Sicherheitslücken führen.

PowerProtect-Portfolio ›

Verschlüsselte, unveränderliche und Air-Gap-Backupumgebungen, die auf KI-gestützten Bedrohungsanalysen basieren, sorgen für eine schnelle, validierte Wiederherstellung und Aufrechterhaltung der Business Continuity während DDoS-Unterbrechungen.

Services für Sicherheit und Resilienz ›

Managed Detection and Response (MDR), Incident Response and Recovery (IRR), Threat Hunting und Anleitungen für eine ausfallsichere Architektur verbessern die Vorbereitung auf DDoS-Angriffe und stärken die Abwehrfunktionen.

Angriffstyp: Böswilliger Insider

Es ist 8:00 Uhr an einem Dienstag. Der Arbeitstag für die MitarbeiterInnen in einem US-Gesundheitsunternehmen beginnt gerade erst.

Eine leitende Angestellte, die mit hochsensiblen Patientendaten arbeitet, meldet sich nach einer langen Nacht im Büro an.

Sie bemerkt Änderungen in einem Ordner, an dem sie in der Nacht zuvor gearbeitet hat. Nachdem sie dies mit ihrem Team besprochen hat, wendet sie sich mit einer Anfrage an das IT-Team.

Nach der Untersuchung stellt man fest, dass ein neues Mitglied des IT-Teams mit Verbindungen zu einem Verbrechersyndikat ein leitendes Teammitglied dazu gebracht hat, ein Rubber Ducky per USB mit dessen Gerät zu verbinden, wodurch das BIOS (Basic Input/Output System) auf eine anfällige Version heruntergestuft und das System kompromittiert wurde.

Testen Sie Ihr Wissen →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Böswilliger Insider

1: Verkleinerung der Angriffsfläche — 2 — 3. — 4 — 5.

Der böswillige Insider hat für diesen Angriff zwei Methoden genutzt, die im MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) Framework erfasst sind. Was genau?

- [ ] Vertrauensbeziehung + Replikation über Wechselmedien
- [ ] Social Engineering + Replikation über Wechselmedien
- [ ] Social Engineering + externe Remoteservices
- [ ] Vertrauensbeziehung + Hardware-Ergänzungen

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Böswilliger Insider

1: Verkleinerung der Angriffsfläche — 2 — 3. — 4 — 5.

Der böswillige Insider hat für diesen Angriff zwei Methoden genutzt, die im MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) Framework erfasst sind. Was genau?

- ✗ Vertrauensbeziehung + Replikation über Wechselmedien
- ✓ Social Engineering + Replikation über Wechselmedien
- ✗ Social Engineering + externe Remoteservices
- ✗ Vertrauensbeziehung + Hardware-Ergänzungen

Durch die Nutzung von MITRE ATT&CK-Methoden sowohl zur Manipulation von Menschen als auch zur Replikation über tragbare Speichermedien hat der/die AngreiferIn mit Social Engineering ein leitendes Teammitglied dazu gebracht, ein Rubber Ducky per USB anzuschließen, und so kompromittierte Daten über Wechselmedien übertragen.

Nächste Frage →

Angriffstyp: Böswilliger Insider

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4 — 5.

Warum musste der/die AngreiferIn beide Methoden verwenden?

- [ ] Sich Netzwerkzugriff als globaler Administrator verschaffen, um das BIOS (Basic Input/Output System) herunterzustufen
- [ ] Sich per Phishing Administratorzugriff verschaffen, um das BIOS herunterzustufen
- [ ] DNS-Anbieter (Domain Name System) des Geräts ändern, um für den einmaligen Netzwerkzugriff erforderliche Zugangsdaten zu erhalten
- [ ] Malware auf einem Gerät installieren, um für den dauerhaften Netzwerkzugriff erforderliche Zugangsdaten zu erhalten

Die richtige Antwort →

Angriffstyp: Böswilliger Insider

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4 — 5.

Warum musste der/die AngreiferIn beide Methoden verwenden?

- ✗ Sich Netzwerkzugriff als globaler Administrator verschaffen, um das BIOS (Basic Input/Output System) herunterzustufen
- ✗ Sich per Phishing Administratorzugriff verschaffen, um das BIOS herunterzustufen
- ✗ DNS-Anbieter (Domain Name System) des Geräts ändern, um für den einmaligen Netzwerkzugriff erforderliche Zugangsdaten zu erhalten
- ✓ Malware auf einem Gerät installieren, um für den dauerhaften Netzwerkzugriff erforderliche Zugangsdaten zu erhalten

Der/die AngreiferIn musste beide Methoden nutzen – die Installation von Malware über das Rubber Ducky per USB, um das Gerät zu kompromittieren, und die Zugangsdaten für den dauerhaften Netzwerkzugriff –, um eine dauerhafte, unbefugte Kontrolle über die Zielumgebung zu erlangen.

Nächste Frage →

Angriffstyp: Böswilliger Insider

1 2. 3: Erkennung von und Reaktion auf Cyberbedrohungen 4 5.

Was ist eine Möglichkeit, unregelmäßige Netzwerkaktivitäten zu erkennen?

- [ ] Anwendungskontrolle
- [ ] Extended Detection and Response (XDR)
- [ ] Virenschutz der nächsten Generation (NGAV)
- [ ] Endpunkt-Geofencing

Die richtige Antwort →

Angriffstyp: Böswilliger Insider

1 — 2. — 3: Erkennung von und Reaktion auf Cyberbedrohungen — 4 — 5.

Was ist eine Möglichkeit, unregelmäßige Netzwerkaktivitäten zu erkennen?

- ✗ Anwendungskontrolle
- ✓ Extended Detection and Response (XDR)
- ✗ Virenschutz der nächsten Generation (NGAV)
- ✗ Endpunkt-Geofencing

Wenn es um die umfassende, korrelierte Transparenz für die schnelle Erkennung von Bedrohungen geht, eignet sich XDR am besten zur Erkennung verdächtiger Netzwerkaktivitäten, da es die Aktivitäten über Endpunkte, Netzwerke und Cloud-Umgebungen hinweg kontinuierlich überwacht und analysiert.

Nächste Frage →

Angriffstyp: Böswilliger Insider

1 2. 3 4: Recovery nach einem Cyberangriff 5

Welche integrierte PC-Sicherheitsfunktion könnte verdächtige Aktivitäten frühzeitig in der Angriffskette erkennen?

- [ ] SIEM (Security Information and Event Management)
- [ ] Extended Detection and Response (XDR)
- [ ] Indicators of Attack (IOA)
- [ ] Rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC)

Die richtige Antwort →

Angriffstyp: Böswilliger Insider

1 2. 3 4: Recovery nach einem Cyberangriff 5

Welche integrierte PC-Sicherheitsfunktion könnte verdächtige Aktivitäten frühzeitig in der Angriffskette erkennen?

- ✗ SIEM (Security Information and Event Management)
- ✗ Extended Detection and Response (XDR)
- ✓ Indicators of Attack (IOA)
- ✗ Rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC)

IOA konzentriert sich darauf, Angreiferverhalten und verdächtige Aktivitätsmuster sofort zu erkennen, sodass Sicherheitsteams Bedrohungen früher als signaturbasierte Methoden identifizieren und eingreifen können, bevor erheblicher Schaden entsteht.

Nächste Frage →

Angriffstyp: Böswilliger Insider

1 2. 3 4 5: Allgemeine Best Practices

Welche Maßnahme könnten Sie nach der Ermittlung der ersten Zugriffsmethode ergreifen, um ähnliche zukünftige Sicherheitsverletzungen zu beheben und zu verhindern?

- [ ] BIOS auf die neueste Version aktualisieren
- [ ] Option zum BIOS-Downgrade deaktivieren
- [ ] USB-Anschlüsse deaktivieren
- [ ] Granulare Kontrolle implementieren, um die sichere Nutzung von USB-Geräten zu ermöglichen und die Verbreitung von Malware zu verhindern
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Böswilliger Insider

1 2. 3 4 5: Allgemeine Best Practices

Welche Maßnahme könnten Sie nach der Ermittlung der ersten Zugriffsmethode ergreifen, um ähnliche zukünftige Sicherheitsverletzungen zu beheben und zu verhindern?

- [x] BIOS auf die neueste Version aktualisieren
- [x] Option zum BIOS-Downgrade deaktivieren
- [x] USB-Anschlüsse deaktivieren
- [x] Granulare Kontrolle implementieren, um die sichere Nutzung von USB-Geräten zu ermöglichen und die Verbreitung von Malware zu verhindern
- [x] Alle oben genannten Antworten

Indem bestimmte Angriffsvektoren durch sichere Hardware und Blockierung von Downgrades beseitigt werden, können USB-basierte Bedrohungen eingedämmt und die Verbreitung von Malware an mehreren Stellen gestoppt werden. So wird eine umfassende, mehrschichtige Abwehr geschaffen, die betroffene Systeme wiederherstellt und vor zukünftigen Sicherheitsverletzungen schützt.

Lösungen entdecken →

ANGRIFFSTYP: BÖSWILLIGER INSIDER

Zusammenfassung

Ein Angriff durch böswillige Insider liegt vor, wenn eine Person innerhalb einer Organisation ihren Zugriff missbraucht, um Daten zu kompromittieren, Betriebsabläufe zu stören oder sensible Informationen für persönliche, finanzielle oder wettbewerbsbezogene Zwecke zu extrahieren. Bei dieser Person kann es sich um MitarbeiterInnen, AuftragnehmerInnen, PartnerInnen oder Personen mit legitimem Zugriff auf die Systeme und Netzwerke des Unternehmens handeln.

Dell schützt vor bösartigen Cyberangriffen durch Insider durch eine Kombination aus fortschrittlichen Technologien und strengen Sicherheitsprotokollen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor Angriffen durch böswillige Insider schützen kann.

Kurzbeschreibung zu böswilligen Insidern lesen →

Zurück zu Szenarien

Vertrauenswürdige Geräte und Infrastruktur ›

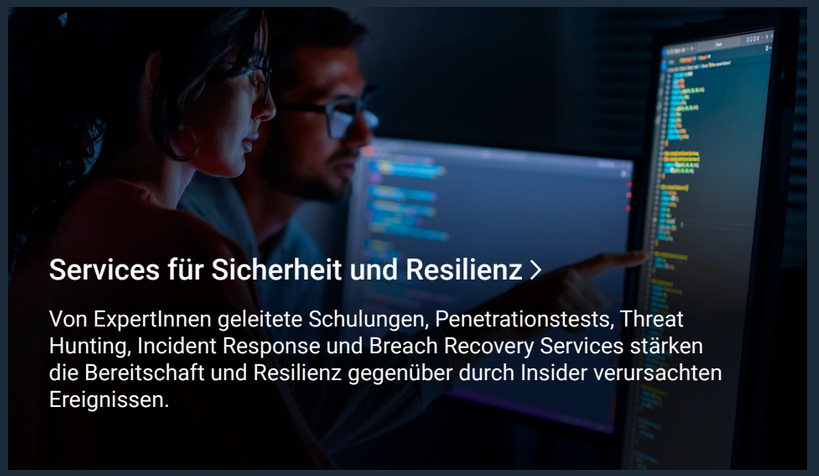
Integriertes Least-Privilege-Prinzip, Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrolle (RBAC), duale Authentifizierung und Zero-Trust-Schutzmaßnahmen sichern Endpunkte und Infrastruktur und reduzieren das Risiko von Insider-Bedrohungen.

PowerEdge-Server ›

Hardware-Root-of-Trust, Secure Boot, dynamisches USB-Anschlussmanagement und Systemsperre schützen vor Manipulationen und stoppen physische oder firmwarebasierte Insiderangriffe.

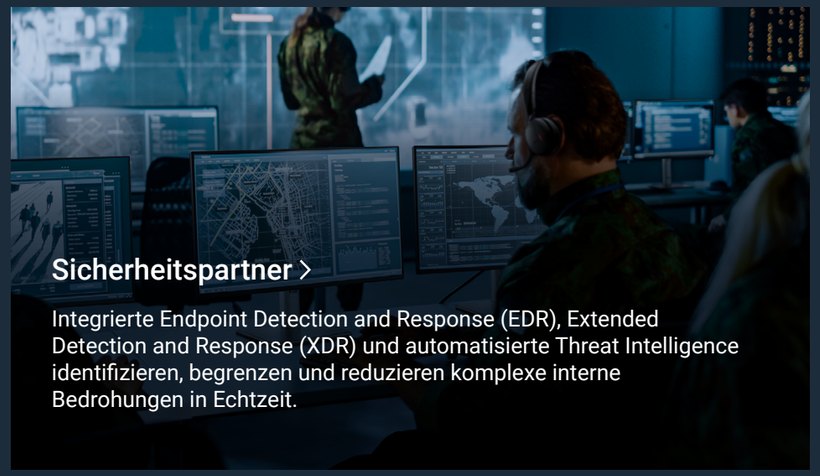
PowerProtect-Portfolio ›

Unveränderbare, isolierte Backups sorgen für Datenintegrität, schnelle Wiederherstellung und frühzeitige Erkennung von Datenmanipulationsversuchen und ermöglichen so die Recovery nach Insider-Incidents.



Services für Sicherheit und Resilienz ›

Von ExpertInnen geleitete Schulungen, Penetrationstests, Threat Hunting, Incident Response und Breach Recovery Services stärken die Bereitschaft und Resilienz gegenüber durch Insider verursachten Ereignissen.



Sicherheitspartner ›

Integrierte Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) und automatisierte Threat Intelligence identifizieren, begrenzen und reduzieren komplexe interne Bedrohungen in Echtzeit.

Angriffstyp: Man-in-the-Middle (MITM)

Eine ahnungslose Kundin nutzt eine Verbindung zu einem kostenlosen, ungesicherten WLAN in einem Café, um letzte Aktualisierungen an einem freigegebenen Teamdokument vorzunehmen.

Kurz darauf erhält die IT ihres Unternehmens Benachrichtigungen über ungewöhnliche Anmeldeversuche durch das Konto der Mitarbeiterin sowie über unbefugten Datenzugriff von mehreren Standorten weltweit.

Nach der Untersuchung stellt das IT-Team fest, dass die AngreiferInnen die drahtlose Verbindung abgefangen und manipuliert haben, um auf sensible Informationen zuzugreifen.

Testen Sie Ihr Wissen →

Angriffstyp: Man-in-the-Middle (MITM)

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Wo sollte das IT-Team als Erstes nach ungewöhnlichen Anmeldeversuchen nachforschen?

- [ ] Firewall, Intrusion Detection System (IDS), IPS-Protokolle (Intrusion Prevention System) und Extended Detection Response (XDR)
- [ ] Laptop der betroffenen Person
- [ ] Netzwerkverkehr im ungesicherten WLAN des Cafés
- [ ] Authentifizierungsprotokolle der Unternehmenssysteme

Die richtige Antwort →

Angriffstyp: Man-in-the-Middle (MITM)

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Wo sollte das IT-Team als Erstes nach ungewöhnlichen Anmeldeversuchen nachforschen?

- ✓ Firewall, Intrusion Detection System (IDS), IPS-Protokolle (Intrusion Prevention System) und Extended Detection Response (XDR)
- ✗ Laptop der betroffenen Person
- ✗ Netzwerkverkehr im ungesicherten WLAN des Cafés
- ✓ Authentifizierungsprotokolle der Unternehmenssysteme

Durch die Analyse dieser Firewall-, IDS/IPS- und Authentifizierungsprotokolle können IT-Teams unbefugte Zugriffsversuche verfolgen, kompromittierte Konten untersuchen und einen besseren Überblick über den Umfang des Incidents gewinnen.

Nächste Frage →

Angriffstyp: Man-in-the-Middle (MITM)

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Welche sofortigen Maßnahmen sollte das IT-Team ergreifen, nachdem der MITM-Angriff bestätigt wurde?

- [ ] Kompromittiertes Gerät sofort vom Netzwerk trennen und zur Analyse isolieren
- [ ] Firewallregeln und Netzwerkkonfigurationen aktualisieren, um weiteren unbefugten Zugriff zu verhindern
- [ ] Kennwörter für alle Mitarbeiterkonten zurücksetzen
- [ ] Betroffene Systeme deaktivieren, um Datenexfiltration zu verhindern

Die richtige Antwort →

Angriffstyp: Man-in-the-Middle (MITM)

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Welche sofortigen Maßnahmen sollte das IT-Team ergreifen, nachdem der MITM-Angriff bestätigt wurde?

- ✓ Kompromittiertes Gerät sofort vom Netzwerk trennen und zur Analyse isolieren
- ✓ Firewallregeln und Netzwerkkonfigurationen aktualisieren, um weiteren unbefugten Zugriff zu verhindern
- ✗ Kennwörter für alle Mitarbeiterkonten zurücksetzen
- ✗ Betroffene Systeme deaktivieren, um Datenexfiltration zu verhindern

Durch sofortiges Trennen und Isolieren des kompromittierten Geräts wird der Zugriff der AngreiferInnen gestoppt und es werden forensische Beweise gesichert, während durch die Aktualisierung der Firewall- und Netzwerkregeln weitere böswillige Verbindungen blockiert und das gesamte Netzwerk vor weiteren Kompromittierungen geschützt wird.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Man-in-the-Middle (MITM)

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche präventiven Maßnahmen hätten die Sicherheitslücke für den MITM-Angriff verkleinern können?

- [ ] Verwendung eines virtuellen privaten Netzwerks (VPN) für alle MitarbeiterInnen vorschreiben
- [ ] Zero-Trust-Sicherheitsprinzipien wie Multi-Faktor-Authentifizierung (MFA) implementieren
- [ ] Öffentliches WLAN vermeiden
- [ ] Per E-Mail verteilte sensible Dateien verschlüsseln

Die richtige Antwort →

Angriffstyp: Man-in-the-Middle (MITM)

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche präventiven Maßnahmen hätten die Sicherheitslücke für den MITM-Angriff verkleinern können?

- [x] Verwendung eines virtuellen privaten Netzwerks (VPN) für alle MitarbeiterInnen vorschreiben
- [x] Zero-Trust-Sicherheitsprinzipien wie Multi-Faktor-Authentifizierung (MFA) implementieren
- [ ] Öffentliches WLAN vermeiden
- [ ] Per E-Mail verteilte sensible Dateien verschlüsseln

Durch Vorschreiben der VPN-Nutzung über ungesicherte Netzwerke wird der Internetdatenverkehr der MitarbeiterInnen verschlüsselt, um Abfangen zu verhindern. Gleichzeitig wird Zero-Trust-Sicherheit implementiert und MFA sorgt dafür, dass jede Zugriffsanfrage kontinuierlich überprüft wird.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Man-in-the-Middle (MITM)

1 — 2. — 3 — 4: Allgemeine Best Practices

Welche langfristigen Strategien sollte Ihr Unternehmen nach der Behebung der Sicherheitsverletzung implementieren?

- [ ] Regelmäßige Audits und Patches von Systemen
- [ ] Netzwerksegmentierung erhöhen, um sensible Daten und Systeme zu isolieren
- [ ] EDR-Lösungen (Endpoint Detection and Response) und MDR-Lösungen (Managed Detection and Response) bereitstellen
- [ ] Intensive und regelmäßige Schulungen für MitarbeiterInnen durchführen
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

Angriffstyp: Man-in-the-Middle (MITM)

1 2. 3 4: Allgemeine Best Practices

Welche langfristigen Strategien sollte Ihr Unternehmen nach der Behebung der Sicherheitsverletzung implementieren?

- [x] Regelmäßige Audits und Patches von Systemen
- [x] Netzwerksegmentierung erhöhen, um sensible Daten und Systeme zu isolieren
- [x] EDR-Lösungen (Endpoint Detection and Response) und MDR-Lösungen (Managed Detection and Response) bereitstellen
- [x] Intensive und regelmäßige Schulungen für MitarbeiterInnen durchführen
- [x] Alle oben genannten Antworten

Zum Schutz vor verschiedenen Bedrohungen bilden diese langfristigen Strategien einen umfassenden, resilienten Sicherheitsstatus, der AngreiferInnen daran hindert, Schwachstellen auszunutzen, und eine schnelle, effektive Reaktion auf Sicherheitsverletzungen gewährleistet.

Lösungen entdecken →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

ANGRIFFSTYP: MAN-IN-THE-MIDDLE (MITM)

Zusammenfassung

Ein MITM-Angriff findet statt, wenn Cyberkriminelle heimlich die Kommunikation zwischen zwei Parteien abfangen, z. B. zwischen MitarbeiterInnen und einem Unternehmensserver oder Kunden und einer Unternehmenswebsite. Das Ziel der AngreiferInnen kann variieren, aber das Ergebnis ist dasselbe: ein Verlust von Vertrauen und Sicherheit.

Bei Dell bieten wir innovative, skalierbare Sicherheitslösungen, mit denen Unternehmen MITM-Bedrohungen neutralisieren, Ressourcen schützen und die Integrität ihres Geschäfts aufrechterhalten können – dank der Tools und dem Fachwissen, die erforderlich sind, um Bedrohungen zu erkennen, darauf zu reagieren und eine sichere Recovery durchzuführen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor MITM-Angriffen schützen kann.

Kurzbeschreibung zu MITM-Angriffen lesen →

Zurück zu Szenarien

Vertrauenswürdige Geräte >

Mit Hardwareauthentifizierung, Firmwareschutz wie SafeBIOS und SafeID, robuster Verschlüsselung und Zero-Trust-Frameworks schützt Dell Endpunkte und Daten während der Übertragung.

PowerEdge-Server >

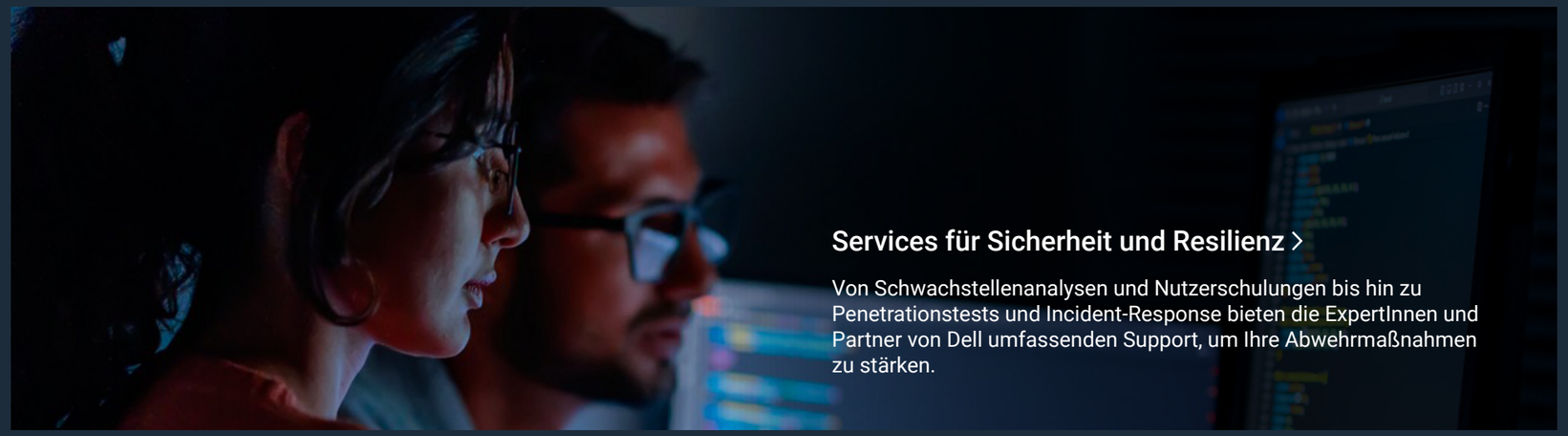
Secure Boot, Silicon Root of Trust, dynamisches USB-Anschlussmanagement und Systemsperren sorgen für Hardwareintegrität und schützen kritische Workloads vor netzwerkbasierten Bedrohungen.

Storage-Lösungen >

Verschlüsselte Daten im Ruhezustand und während der Übertragung sorgen in Kombination mit isolierten Snapshots und Funktionen für schnelle Recovery dafür, dass Dateien sicher bleiben und nach einem MITM-Angriff schnell wiederhergestellt werden können.

PowerProtect-Portfolio >

Unveränderbare, isolierte Backups und KI-gestützte CyberSense-Analysen ermöglichen eine schnelle Recovery und vertrauenswürdige Datenwiederherstellung im Falle eines MITM-Angriffs.



Services für Sicherheit und Resilienz >

Von Schwachstellenanalysen und Nutzerschulungen bis hin zu Penetrationstests und Incident-Response bieten die ExpertInnen und Partner von Dell umfassenden Support, um Ihre Abwehrmaßnahmen zu stärken.

Angriffstyp: Prompt-/SQL-Injection

Sie arbeiten im Kundenservice für eine Fluggesellschaft, die ihren Service überwiegend über einen Chatbot abwickelt.

Sie bemerken, dass Sie und Ihre KollegInnen zunehmend Anrufe von KundInnen erhalten, die berichten, dass sie sich nicht bei ihren Vielfliegerkonten anmelden können. Wenn es ihnen doch gelingt, sehen sie, dass ihre Flugmeilen verschwunden sind.

Testen Sie Ihr Wissen →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Prompt-/SQL-Injection

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Bei der Überprüfung werden einige Fehler in den Protokollen angezeigt: *Syntaxfehler in SQL-Anweisung (Structured Query Language) oder Ungültiger Spaltenname „admin“*. Um welche Art von Cyber-Incident handelt es sich?

- [ ] Gestohlene Zugangsdaten
- [ ] Prompt- oder SQL-Injection
- [ ] Man-in-the-Middle-Angriff
- [ ] Phishing

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Prompt-/SQL-Injection

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Bei der Überprüfung werden einige Fehler in den Protokollen angezeigt: *Syntaxfehler in SQL-Anweisung (Structured Query Language)* oder *Ungültiger Spaltenname „admin“*. Um welche Art von Cyber-Incident handelt es sich?

- ✗ Gestohlene Zugangsdaten
- ✓ Prompt- oder SQL-Injection
- ✗ Man-in-the-Middle-Angriff
- ✗ Phishing

„Prompt- oder SQL-Injection“ ist korrekt, da Protokollfehler wie „Syntaxfehler in SQL-Anweisung“ oder „Ungültiger Spaltenname „admin““ zeigen, dass AngreiferInnen die Eingabefelder des Chatbots mit bösartigem SQL-Code ausgenutzt haben, um auf Kundenkontodaten zuzugreifen oder diese zu ändern. Dies sind klare technische Indikatoren für einen SQL-Injection-Angriff, der mit der beschriebenen verdächtigen Aktivität übereinstimmt.

Nächste Frage →

Angriffstyp: Prompt-/SQL-Injection

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Sie haben festgestellt, dass Sie über Ihren Kundenservice-Chatbot Opfer eines Prompt-/SQL-Injection-Angriffs geworden sind. Wie sollten Sie vorgehen?

- [ ] Bot offline schalten
- [ ] Datenbankprotokolle auf unbefugten Zugriff und gestohlene, geänderte oder gelöschte Daten untersuchen
- [ ] Alle Gesetze zur Offenlegung von Datenschutzverletzungen einhalten
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Prompt-/SQL-Injection

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Sie haben festgestellt, dass Sie über Ihren Kundenservice-Chatbot Opfer eines Prompt-/SQL-Injection-Angriffs geworden sind. Wie sollten Sie vorgehen?

- [x] Bot offline schalten
- [x] Datenbankprotokolle auf unbefugten Zugriff und gestohlene, geänderte oder gelöschte Daten untersuchen
- [x] Alle Gesetze zur Offenlegung von Datenschutzverletzungen einhalten
- [x] Alle oben genannten Antworten

Als Reaktion auf einen Prompt-/SQL-Injection-Angriff müssen Sie den Chatbot offline schalten, Datenbankprotokolle auf unbefugten Zugriff untersuchen und die Einhaltung der Gesetze zur Offenlegung sicherstellen. Diese Schritte sind unerlässlich, um den Datenabfluss zu stoppen, den Schaden zu bewerten und behördliche und ethische Verpflichtungen zu erfüllen.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Prompt-/SQL-Injection

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche Funktionen sollten Sie einrichten, um Prompt-/SQL-Injection-Angriffe zu stoppen?

- [ ] Entwicklungsteams darin schulen, vorbereitete Aussagen und parametrisierte Abfragen als Codierungspraxis zu verwenden
- [ ] MDR-Tools (Managed Detection and Response)
- [ ] Zugriff mit den geringsten erforderlichen Berechtigungen implementieren, z. B. Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrolle (RBAC), Firewall für Webanwendungen (WAF) usw.
- [ ] Back-end-Datenbanken/Wissensdatenbanken segmentieren

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Prompt-/SQL-Injection

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Welche Funktionen sollten Sie einrichten, um Prompt-/SQL-Injection-Angriffe zu stoppen?

- ✓ Entwicklungsteams darin schulen, vorbereitete Aussagen und parametrisierte Abfragen als Codierungspraxis zu verwenden
- ✗ MDR-Tools (Managed Detection and Response)
- ✓ Zugriff mit den geringsten erforderlichen Berechtigungen implementieren, z. B. Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrolle (RBAC), Firewall für Webanwendungen (WAF) usw.
- ✗ Back-end-Datenbanken/Wissensdatenbanken segmentieren

Die Schulung von Entwicklungsteams im Umgang mit vorbereiteten Anweisungen und parametrisierten Abfragen blockiert SQL-Injection-Angriffe bereits an der Quelle. Durch die Einhaltung von Zugriffskontrollen mit minimalen Berechtigungen wie MFA, RBAC und WAF werden die Auswirkungen eines Injection-Versuchs eingeschränkt, indem verhindert wird, dass AngreiferInnen Berechtigungen eskalieren oder lateral verschieben können.

Nächste Frage →

Angriffstyp: Prompt-/SQL-Injection

1 2. 3 4: Allgemeine Best Practices

Welche Schritte würden Sie unternehmen, um die Daten der Kunden der Fluggesellschaft zurückzuerhalten?

- [ ] Gestohlene Daten verfolgen
- [ ] KundInnen bitten, ihre Profile neu zu erstellen
- [ ] Daten von den CyberangreiferInnen zurückkaufen
- [ ] Wiederherstellung aus dem letzten nicht kompromittierten Backup durchführen, um Flugmeilen wiederherzustellen, und KundInnen benachrichtigen, dass sie ihre Kennwörter ändern und ihre Kreditkarten überprüfen sollten

Die richtige Antwort →

Angriffstyp: Prompt-/SQL-Injection

1 — 2. — 3 — 4: Allgemeine Best Practices

Welche Schritte würden Sie unternehmen, um die Daten der Kunden der Fluggesellschaft zurückzuerhalten?

- ✗ Gestohlene Daten verfolgen
- ✗ KundInnen bitten, ihre Profile neu zu erstellen
- ✗ Daten von den CyberangreiferInnen zurückkaufen
- ✓ Wiederherstellung aus dem letzten nicht kompromittierten Backup durchführen, um Flugmeilen wiederherzustellen, und KundInnen benachrichtigen, dass sie ihre Kennwörter ändern und ihre Kreditkarten überprüfen sollten

Die Wiederherstellung verlorener Kontodaten aus dem letzten, nicht kompromittierten Backup trägt dazu bei, die Datenintegrität aufrechtzuerhalten und Ausfallzeiten zu reduzieren. Die sofortige Benachrichtigung der Kunden, ihre Kennwörter zurückzusetzen und Kreditkartenaktivitäten zu überwachen, unterstützt zusätzlich die Einhaltung gesetzlicher Vorschriften nach einem destruktiven Injection-Angriff.

Lösungen entdecken →

ANGRIFFSTYP: PROMPT-/SQL-INJECTION

Zusammenfassung

Prompt- und SQL-Injection-Angriffe haben sich wiederholt als eine der schädlichsten und am weitesten verbreiteten Methoden von Cyberkriminellen erwiesen. Diese Angriffe nutzen Sicherheitslücken in Nutzerabfragen- oder Datenbanksystemen aus und ermöglichen es böswilligen Akteuren, Server zu manipulieren, Daten zu stehlen oder Workflows zu unterbrechen.

Der Schutz Ihres Unternehmens vor sich weiterentwickelnden Prompt-/SQL-Injection-Bedrohungen und -Angriffen ist Teil des fortlaufenden Engagements von Dell für Cybersicherheit. Wir stellen die Tools und das Fachwissen bereit, die für die Erkennung, Reaktion und Recovery erforderlich sind.

Lernen Sie fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen kennen und erfahren Sie, wie Dell Ihre Organisation bei der Abwehr von Prompt- und SQL-Injection-Angriffen unterstützen kann.

Kurzbeschreibung zu Prompt-/SQL-Injection lesen →

Zurück zu Szenarien

Vertrauenswürdiger Arbeitsplatz und vertrauenswürdige Infrastruktur ›

Schützt Endpunkte und reduziert das Risiko, dass kompromittierte Zugangsdaten bei Injection-Angriffen ausgenutzt werden.

PowerEdge-Server ›

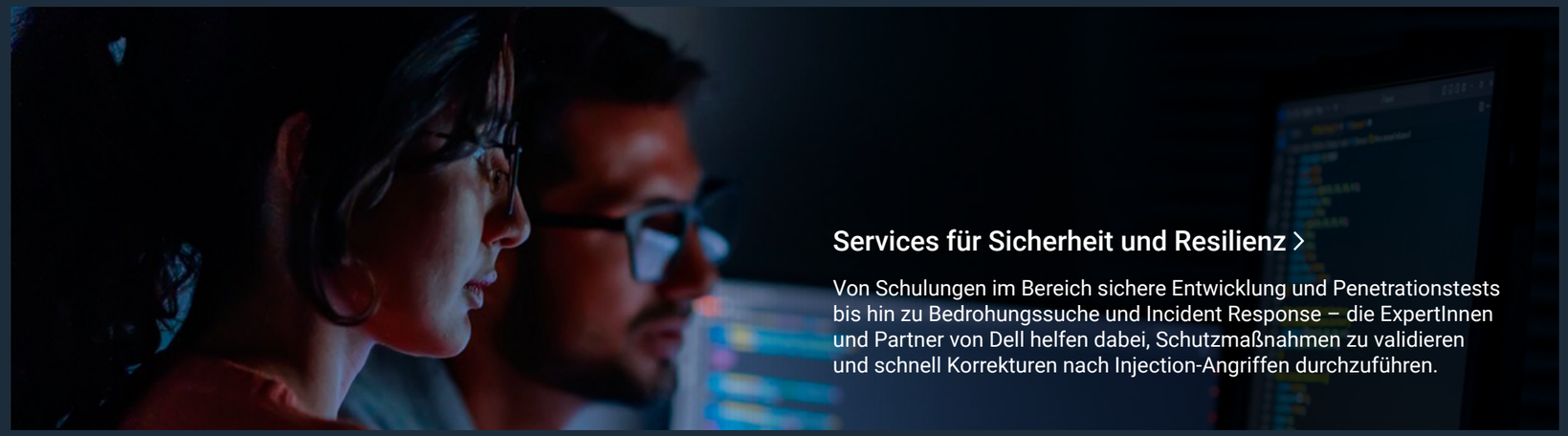
Dell PowerEdge-Server bieten Hardware-Root-of-Trust, Secure Boot, chipbasierte Sicherheit und Echtzeit-Konfigurationsvalidierung und gewährleisten eine manipulationssichere Infrastruktur, in der nur vertrauenswürdiger Code ausgeführt wird.

Sicherheitspartner ›

Mit detaillierter Zugriffskontrolle, Advanced Threat Intelligence sowie externer Erkennung und Reaktion helfen Dell Security-Partner dabei, SQL- und Prompt-Injection-Versuche zu identifizieren und abzuwehren.

PowerProtect-Portfolio ›

Die unveränderlichen Air-Gap-Backups von Dell und die erweiterten Cyber-Recovery-Analysen bieten vertrauenswürdige Wiederherstellungspunkte, die eine schnelle Recovery nach Datenbeschädigung oder -Exfiltration ermöglichen.



Services für Sicherheit und Resilienz ›

Von Schulungen im Bereich sichere Entwicklung und Penetrationstests bis hin zu Bedrohungssuche und Incident Response – die ExpertInnen und Partner von Dell helfen dabei, Schutzmaßnahmen zu validieren und schnell Korrekturen nach Injection-Angriffen durchzuführen.

Angriffstyp: Ransomware

Sie sind IT-Fachkraft in einem regionalen Krankenhaus, das für seine vernetzten medizinischen Systeme bekannt ist – darunter elektronische Patientenakten (EPA), intelligente Infusionspumpen und radiologische Bildgebung, die alle in ein zentrales Netzwerk eingebunden sind.

In der vergangenen Nacht sind mehrere Systeme gleichzeitig abgestürzt. Am Morgen melden die MitarbeiterInnen, dass sie keinen Zugriff mehr auf die Patientenakten haben.

Der folgende Lösegeldbescheid wird auf mehreren Terminals angezeigt:

„Ihre Dateien sind verschlüsselt. Zahlen Sie innerhalb von 72 Stunden 20 Bitcoins. Andernfalls werden die Patientendaten veröffentlicht."

Testen Sie Ihr Wissen →

Angriffstyp: Ransomware

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Der Helpdesk erhält mehr als 100 Berichte über Dateiverschlüsselungs- und Anwendungsfehler. Die Sicherheitsprotokolle zeigen ungewöhnliche Dateiumbenennungsaktivitäten über ein internes Domainkonto. Was ist Ihr erster Schritt?

- [ ] Lösegeld sofort zahlen, um kritische Services wiederherzustellen
- [ ] Strafverfolgungsbehörden und Rechtsberatung informieren
- [ ] Reimaging aller betroffenen Endpunkte starten
- [ ] Infizierte Systeme vom Netzwerk trennen

Die richtige Antwort →

Angriffstyp: Ransomware

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Der Helpdesk erhält mehr als 100 Berichte über Dateiverschlüsselungs- und Anwendungsfehler. Die Sicherheitsprotokolle zeigen ungewöhnliche Dateiumbenennungsaktivitäten über ein internes Domainkonto. Was ist Ihr erster Schritt?

- ✗ Lösegeld sofort zahlen, um kritische Services wiederherzustellen
- ✗ Strafverfolgungsbehörden und Rechtsberatung informieren
- ✗ Reimaging aller betroffenen Endpunkte starten
- ✓ Infizierte Systeme vom Netzwerk trennen

Das sofortige Trennen und Isolieren infizierter Krankenhaussysteme verhindert die Verbreitung von Ransomware und schützt kritische medizinische Geräte und sensible Patientendaten. Zudem können Sie Beweise für die Ermittlungen sichern und sich Zeit für eine koordinierte Reaktion und Recovery verschaffen.

Nächste Frage →

Angriffstyp: Ransomware

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Das Incident-Response-Team stellt fest, dass der Angriff wahrscheinlich von einem kompromittierten Konto gestartet wurde, das für den Zugriff auf einen Server ohne Multifaktor-Authentifizierung (MFA) verwendet wurde. Welcher der folgenden Faktoren hat am unmittelbarsten zu dem Angriff beigetragen?

- [ ] Veraltete Virenschutzdefinitionen
- [ ] Exponierte Datenbank für elektronische Gesundheitsakten (EPA)
- [ ] Fehlende MFA für Remotezugriffe
- [ ] Schwache E-Mail-Filterung

Die richtige Antwort →

Angriffstyp: Ransomware

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Das Incident-Response-Team stellt fest, dass der Angriff wahrscheinlich von einem kompromittierten Konto gestartet wurde, das für den Zugriff auf einen Server ohne Multifaktor-Authentifizierung (MFA) verwendet wurde. Welcher der folgenden Faktoren hat am unmittelbarsten zu dem Angriff beigetragen?

- ✗ Veraltete Virenschutzdefinitionen
- ✗ Exponierte Datenbank für elektronische Gesundheitsakten (EPA)
- ✓ Fehlende MFA für Remotezugriffe
- ✗ Schwache E-Mail-Filterung

Fehlende MFA für Remotezugriffe ermöglichte die Serververletzung, da sich AngreiferInnen ohne zusätzlichen Verifizierungsschritt mit gestohlenen oder erratenen Zugangsdaten anmelden konnten. Mit MFA ist selbst bei kompromittierten Konten ein zweiter Faktor erforderlich, was das Risiko von unbefugten Zugriffen drastisch reduziert.

Nächste Frage →

Angriffstyp: Ransomware

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Das medizinische Personal nutzt jetzt papierbasierte Workflows. PatientInnen, deren Operation für heute geplant ist, können im System nicht verifiziert werden. Was ist die beste kurzfristige Maßnahme zur Unterstützung des Krankenhausbetriebs?

- [ ] Core-Datenbankserver neu starten, um eine Neuinitialisierung zu versuchen
- [ ] Alle alten Backups aktivieren, auch wenn sie schon sechs Monate alt sind
- [ ] Manuelle Ausfallverfahren des Krankenhauses aktivieren und an das Notfallteam eskalieren
- [ ] Personal fallbasiert über das Vorgehen entscheiden lassen

Die richtige Antwort →

Angriffstyp: Ransomware

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Das medizinische Personal nutzt jetzt papierbasierte Workflows. PatientInnen, deren Operation für heute geplant ist, können im System nicht verifiziert werden. Was ist die beste kurzfristige Maßnahme zur Unterstützung des Krankenhausbetriebs?

- ✗ Core-Datenbankserver neu starten, um eine Neuinitialisierung zu versuchen
- ✗ Alle alten Backups aktivieren, auch wenn sie schon sechs Monate alt sind
- ✓ Manuelle Ausfallverfahren des Krankenhauses aktivieren und an das Notfallteam eskalieren
- ✗ Personal fallbasiert über das Vorgehen entscheiden lassen

Durch die Aktivierung manueller Ausfallverfahren und die Eskalation an das Notfallteam wird die sofortige Kontinuität kritischer klinischer Workflows sichergestellt, die Patientensicherheit gewährleistet und ein standardisierter Prozess für die Überprüfung und Dokumentation der Versorgung etabliert. Dieser Ansatz minimiert Fehler, managt Risiken und Ressourcen effizient und unterstützt Fachkräfte bei der sicheren Wiederherstellung digitaler Systeme.

Nächste Frage →

Angriffstyp: Ransomware

1 — 2. — 3 — 4: Allgemeine Best Practices

Die lokalen Medien haben bereits über den Vorfall berichtet. Führungskräfte möchten wissen, ob sie eine öffentliche Erklärung abgeben sollten, und die Rechtsabteilung fragt nach den Verpflichtungen gemäß dem Health Insurance Portability and Accountability Act (HIPAA). Was ist der am besten geeignete nächste Schritt?

- [ ] Vorfall öffentlich leugnen, bis weitere Informationen vorliegen
- [ ] Pressemitteilung veröffentlichen, in der Sie den IT-Drittanbieter für die Probleme verantwortlich machen
- [ ] Aufsichtsbehörden informieren und interne Verfahren zur Benachrichtigung über Verstöße anstoßen
- [ ] Sofort Lösegeld zahlen und öffentliche Aufmerksamkeit vermeiden

Die richtige Antwort →

Angriffstyp: Ransomware

1 — 2. — 3 — 4: Allgemeine Best Practices

Die lokalen Medien haben bereits über den Vorfall berichtet. Führungskräfte möchten wissen, ob sie eine öffentliche Erklärung abgeben sollten, und die Rechtsabteilung fragt nach den Verpflichtungen gemäß dem Health Insurance Portability and Accountability Act (HIPAA). Was ist der am besten geeignete nächste Schritt?

- ✗ Vorfall öffentlich leugnen, bis weitere Informationen vorliegen
- ✗ Pressemitteilung veröffentlichen, in der Sie den IT-Drittanbieter für die Probleme verantwortlich machen
- ✓ Aufsichtsbehörden informieren und interne Verfahren zur Benachrichtigung über Verstöße anstoßen
- ✗ Sofort Lösegeld zahlen und öffentliche Aufmerksamkeit vermeiden

Die unverzügliche Meldung von Verstößen gegen den Schutz von Gesundheitsdaten an Behörden und betroffene Personen, wie durch HIPAA und staatliche Gesetze vorgeschrieben, sorgt für die Einhaltung gesetzlicher Vorschriften, rechtlichen Schutz und Transparenz gemäß der Best Practices, um rechtliche Schäden und Reputationsschäden zu verhindern, obligatorische Offenlegungspflichten zu erfüllen und eine angemessene Kommunikation mit PatientInnen, MitarbeiterInnen und StakeholderInnen herzustellen.

Lösungen entdecken →

ANGRIFFSTYP: RANSOMWARE

Zusammenfassung

Ransomware ist eine Art von Malware, die den Zugriff auf ein Computersystem oder Daten blockiert, bis ein Lösegeld gezahlt wird. Es handelt sich um eine der disruptivsten Arten von Cyberangriffen. 50 % der Unternehmen weltweit waren im letzten Jahr mindestens einmal von Ransomware betroffen und die durchschnittliche Ausfallzeit nach einem Ransomwareangriff beträgt drei Wochen, was zu erheblichen Betriebsunterbrechungen führt.

Bei Dell legen wir sehr großen Wert auf den Schutz Ihres Unternehmens mit Zero-Trust-Frameworks, Endpunktschutz und Netzwerksegmentierung, um das Eindringen von Ransomware zu verhindern und deren Ausbreitung einzudämmen. Mit der von ExpertInnen geleiteten Incident-Response-Planung helfen wir Ihnen dabei, resilient zu bleiben und sich schnell von Angriffen zu erholen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor Ransomware-Angriffen schützen kann.

Kurzbeschreibung zu Ransomware-Angriffen lesen →

Zurück zu Szenarien

Vertrauenswürdige Infrastruktur ›

Blockieren Sie Ransomware auf Infrastrukturebene mit Hardwareauthentifizierung, Multi-Faktor-Authentifizierung (MFA), rollenbasierter Zugriffskontrolle (RBAC) und Zero-Trust-Frameworks.

Netzwerke und PowerEdge-Server ›

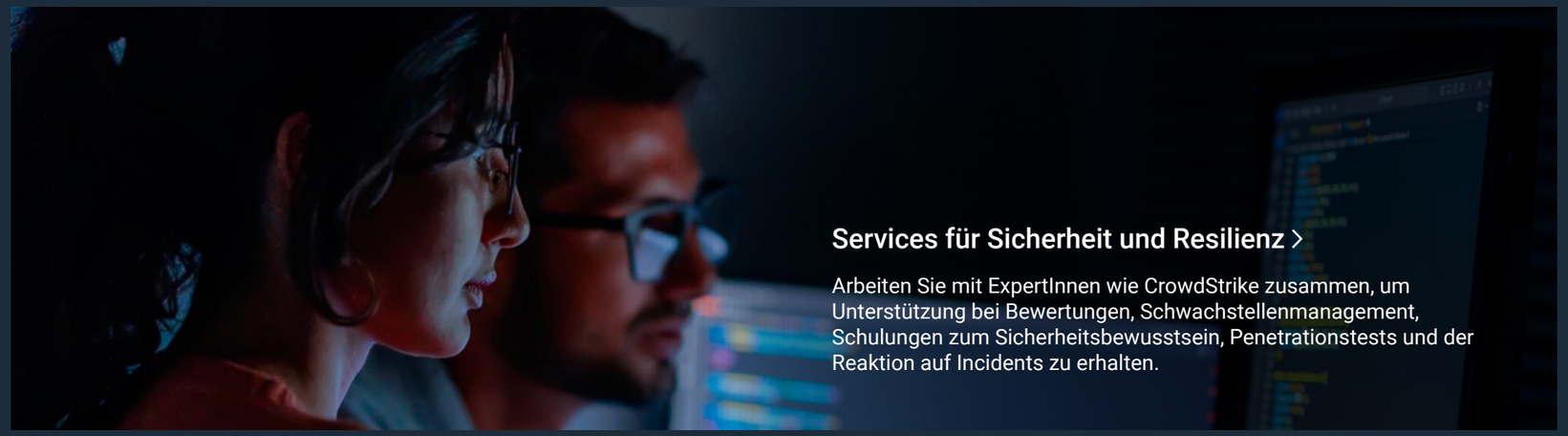
Begrenzen Sie die Verbreitung von Ransomware. Mit Netzwerksegmentierung, Secure Boot, Silicon Root of Trust, dynamischem USB-Anschlussmanagement und Systemsperre.

Vertrauenswürdiger Arbeitsplatz ›

Integrieren Sie SafeBIOS-, SafeID-, SafeData- und EDR-Tools (Endpoint Detection and Response), um proaktive Threat Intelligence, Echtzeiterkennung und automatisierte Eindämmung von Malware auf Geräteebene bereitzustellen.

PowerProtect-Portfolio ›

Schützen Sie kritische Daten mit unveränderbaren Air-Gap-Backups, intelligenten Cyber-Recovery-Analysen und schnellen Wiederherstellungsfunktionen, um Erpressung zu verhindern und Resilienz zu ermöglichen.



Services für Sicherheit und Resilienz ›

Arbeiten Sie mit ExpertInnen wie CrowdStrike zusammen, um Unterstützung bei Bewertungen, Schwachstellenmanagement, Schulungen zum Sicherheitsbewusstsein, Penetrationstests und der Reaktion auf Incidents zu erhalten.

Angriffstyp: Hardware in der Lieferkette

Ihr Unternehmen stellt 500 neue Laptops in seinen globalen Büros bereit. Um den Prozess zu beschleunigen, haben Sie Imaging und Hardwarevorbereitung an einen Drittanbieter für IT-Logistik ausgelagert. Dieser liefert die vorkonfigurierten Geräte direkt an die MitarbeiterInnen aus.

Innerhalb weniger Tage erhalten Sie mehrere Anrufe vom Außendienst mit folgenden Angaben:

- MFA-Anfragen (Multi-Faktor-Authentifizierung) werden umgangen und funktionieren nicht ordnungsgemäß.
- Das Sicherheitsteam stellt eine Reihe von unbefugten Administratoranmeldungen zu ungewöhnlichen Zeiten fest.
- Außerdem fällt VPN-Datenverkehr (Virtual Private Network) von NutzerInnen auf, die angeblich offline sind.

Testen Sie Ihr Wissen →

Angriffstyp: Hardware in der Lieferkette

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Eine Person meldet, sie habe Push-Benachrichtigungen zur Multifaktor-Authentifizierung (MFA) erhalten, obwohl sie nicht versucht hat, sich anzumelden. Das Sicherheits-Dashboard Ihres Unternehmens zeigt an, dass die Anmeldung von einem Gerät mit einem vom Unternehmen ausgestellten Bestands-Tag stammt. Was ist der logischste erste Schritt für das SOC-Team (Security Operations Center)?

- [ ] Das Konto der betreffenden Person deaktivieren und Daten des Laptops remote löschen
- [ ] Anmelde-IP-Adresse und Fingerabdruck des Geräts mit anderen bekannten kompromittierten NutzerInnen vergleichen
- [ ] Vorfall an die Personalabteilung eskalieren unter der Annahme, die betreffende Person hätte einen Fehler gemacht
- [ ] Unternehmensweite Warnmeldung ausgeben, um sofort alle Kennwörter ändern zu lassen

Die richtige Antwort →

Angriffstyp: Hardware in der Lieferkette

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Eine Person meldet, sie habe Push-Benachrichtigungen zur Multifaktor-Authentifizierung (MFA) erhalten, obwohl sie nicht versucht hat, sich anzumelden. Das Sicherheits-Dashboard Ihres Unternehmens zeigt an, dass die Anmeldung von einem Gerät mit einem vom Unternehmen ausgestellten Bestands-Tag stammt. Was ist der logischste erste Schritt für das SOC-Team (Security Operations Center)?

- ✗ Das Konto der betreffenden Person deaktivieren und Daten des Laptops remote löschen
- ✓ Anmelde-IP-Adresse und Fingerabdruck des Geräts mit anderen bekannten kompromittierten NutzerInnen vergleichen
- ✗ Vorfall an die Personalabteilung eskalieren unter der Annahme, die betreffende Person hätte einen Fehler gemacht
- ✗ Unternehmensweite Warnmeldung ausgeben, um sofort alle Kennwörter ändern zu lassen

Wenn Ihr SOC-Team ermittelt, ob verdächtige Aktivitäten Teil eines umfassenderen Angriffs oder eines isolierten Angriffs sind, um eine schnelle Mustererkennung zu ermöglichen, sind eine gezielte Reaktion auf Incidents und die Eindämmung weiterer Risiken der logische erste Schritt bei der Identifizierung eines Angriffs auf die Hardware in der Lieferkette.

Nächste Frage →

Angriffstyp: Hardware in der Lieferkette

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihr Incident Response-Team stellt fest, dass auf mehreren betroffenen Laptops SSD-Firmwareversionen ausgeführt werden, die nicht mit den offiziellen Versionshinweisen des Anbieters übereinstimmen. Das EDR-System (Endpoint Detection Response) zeigt keine bösartigen Prozesse an. Was bedeutet dies am wahrscheinlichsten?

- [ ] Konfigurationsfehler des IT-Anbieters
- [ ] Neuartige Ransomware, die sich selbst löscht
- [ ] Kompromittierung der Lieferkette auf Firmwareebene
- [ ] Normales Verhalten während des Imaging

Die richtige Antwort →

Angriffstyp: Hardware in der Lieferkette

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihr Incident Response-Team stellt fest, dass auf mehreren betroffenen Laptops SSD-Firmwareversionen ausgeführt werden, die nicht mit den offiziellen Versionshinweisen des Anbieters übereinstimmen. Das EDR-System (Endpoint Detection Response) zeigt keine bösartigen Prozesse an. Was bedeutet dies am wahrscheinlichsten?

- ✗ Konfigurationsfehler des IT-Anbieters
- ✗ Neuartige Ransomware, die sich selbst löscht
- ✓ Kompromittierung der Lieferkette auf Firmwareebene
- ✗ Normales Verhalten während des Imaging

Nicht autorisierte SSD-Firmware auf mehreren Laptops, die vom EDR-System nicht erkannt wurde und nicht mit offiziellen Versionen übereinstimmt, weist auf absichtliche Hardware- oder Firmwaremanipulationen hin – ein Zeichen für eine Kompromittierung der Lieferkette auf Firmwareebene.

Nächste Frage →

Angriffstyp: Hardware in der Lieferkette

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Sie haben 100 verdächtige Geräte mit nicht autorisierter SSD-Firmware isoliert. Sie müssen entscheiden, wie Sie vorgehen, ohne die AngreiferInnen zu alarmieren, die möglicherweise Remotezugriff haben. Was ist der beste nächste Schritt?

- [ ] Alle Geräte ausschalten und an die forensische Abteilung schicken
- [ ] Speicherabbilder live erstellen und untersuchen, während die Systeme ausgeführt werden
- [ ] Drittanbieter darüber informieren, dass er Opfer eines Angriffs geworden ist
- [ ] Daten aller Geräte löschen und weltweit für alle NutzerInnen neue Laptops bereitstellen

Die richtige Antwort →

Angriffstyp: Hardware in der Lieferkette

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Sie haben 100 verdächtige Geräte mit nicht autorisierter SSD-Firmware isoliert. Sie müssen entscheiden, wie Sie vorgehen, ohne die AngreiferInnen zu alarmieren, die möglicherweise Remotezugriff haben. Was ist der beste nächste Schritt?

- ✗ Alle Geräte ausschalten und an die forensische Abteilung schicken
- ✓ Speicherabbilder live erstellen und untersuchen, während die Systeme ausgeführt werden
- ✗ Drittanbieter darüber informieren, dass er Opfer eines Angriffs geworden ist
- ✗ Daten aller Geräte löschen und weltweit für alle NutzerInnen neue Laptops bereitstellen

Live-Speicherabbilder sind entscheidend für die Sicherung flüchtiger Beweise wie aktiver Malware und Rootkits. Sie ermöglichen eine gezielte Reaktion auf Incidents, indem versteckte Bedrohungen und Zugriffspunkte aufgedeckt werden, bevor sie verloren gehen oder AngreiferInnen benachrichtigt werden.

Nächste Frage →

Angriffstyp: Hardware in der Lieferkette

1 — 2. — 3 — 4: Allgemeine Best Practices

Ihr Chief Information Security Officer bittet um eine Zusammenfassung darüber, wie dieser Angriff in Ihre Umgebung gelangt ist. Sie müssen eine kurze Erklärung an das Führungsteam abgeben. Wie sollten Sie den Angriff erklären?

- [ ] Ein Virus wurde versehentlich über einen Phishing-Link heruntergeladen.
- [ ] Es lag eine Fehlkonfiguration des Netzwerks vor, die externen Zugriff ermöglichte.
- [ ] Bösartige Firmware wurde während der Bereitstellung von Laptops von einem kompromittierten Hardwareanbieter eingeführt.
- [ ] Ein Mitglied unseres Entwicklungsteams hat unsicheren Code in die Produktionsumgebung übertragen.

Die richtige Antwort →

Angriffstyp: Hardware in der Lieferkette

1 — 2. — 3 — 4: Allgemeine Best Practices

Ihr Chief Information Security Officer bittet um eine Zusammenfassung darüber, wie dieser Angriff in Ihre Umgebung gelangt ist. Sie müssen eine kurze Erklärung an das Führungsteam abgeben. Wie sollten Sie den Angriff erklären?

- ✗ Ein Virus wurde versehentlich über einen Phishing-Link heruntergeladen.
- ✗ Es lag eine Fehlkonfiguration des Netzwerks vor, die externen Zugriff ermöglichte.
- ✓ Bösartige Firmware wurde während der Bereitstellung von Laptops von einem kompromittierten Hardwareanbieter eingeführt.
- ✗ Ein Mitglied unseres Entwicklungsteams hat unsicheren Code in die Produktionsumgebung übertragen.

Die nicht übereinstimmenden Firmwareversionen und das Fehlen aktiver Malware bestätigen, dass es sich um einen Angriff auf Firmwareebene handelt, der vom Anbieter ausgeht und nicht von einem Nutzerfehler oder einer Fehlkonfiguration.

Lösungen entdecken →

ANGRIFFSTYP: HARDWARE IN DER LIEFERKETTE

Zusammenfassung

Angriffe auf die Lieferkette haben in den letzten Jahren erheblich zugenommen. Durch Manipulationen an physischen Geräten während der Produktion, des Versands oder der Bereitstellung oder durch das Auffinden von Schwachstellen bei Softwareanbietern erhalten AngreiferInnen die Möglichkeit, bösartige Komponenten oder Code einzuschleusen, Systeme zu beschädigen oder sensible Daten zu exfiltrieren. Die Opfer können von kleinen Unternehmen bis hin zu Weltkonzernen reichen. Die Folgen sind unter anderem schwere finanzielle Verluste, beeinträchtigtes Kundenvertrauen und rechtliche Konsequenzen.

Dell reduziert Angriffe auf Hardware in der Lieferkette durch die Integration strenger Risikobewertungen für Anbieter und die Einbindung von Zero-Trust-Prinzipien sowie durch kontinuierliche Gerätevalidierung und unabhängige Integritätsprüfungen. Wir stärken die Hardwareintegrität über den gesamten Lebenszyklus hinweg.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor Angriffen auf Hardware in der Lieferkette schützen kann.

Kurzbeschreibung zu Angriffen auf Hardware in der Lieferkette lesen →

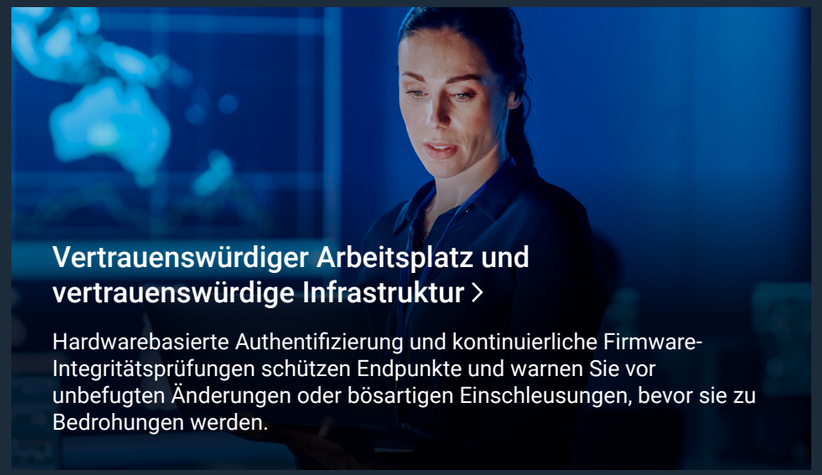
Zurück zu Szenarien

Sicherheit in der Lieferkette ›

Mit fortschrittlicher Herkunftsnachverfolgung, manipulationssicherer Logistik und transparenter Beschaffung sorgt die Lieferkette von Dell dafür, dass Hardware, Firmware und Lieferanten streng geprüft werden, bevor sie Ihr Unternehmen erreichen.

Sichere Komponentenverifizierung (Secured Component Verification, SCV) ›

Die kryptografische Verifizierung von PC-Komponenten im Werk und während der Installation sorgt für Authentizität, erkennt versteckte Änderungen und reduziert das Risiko von Manipulationen in der Lieferkette.

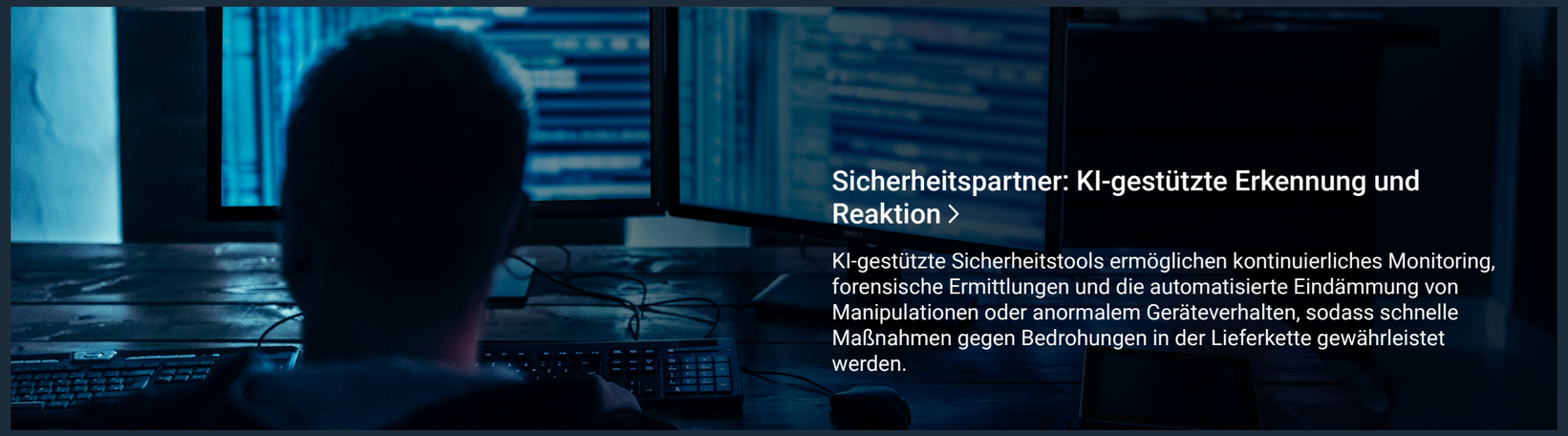


Vertrauenswürdiger Arbeitsplatz und vertrauenswürdige Infrastruktur ›

Hardwarebasierte Authentifizierung und kontinuierliche Firmware-Integritätsprüfungen schützen Endpunkte und warnen Sie vor unbefugten Änderungen oder bösartigen Einschleusungen, bevor sie zu Bedrohungen werden.

Bestandsnachverfolgung und ProSupport Suite mit SupportAssist ›

Umfassende Bestandsnachverfolgung, Echtzeitüberwachung der Geräteherkunft und proaktive Integritätsüberprüfung sorgen für eine schnelle Erkennung von Anomalien und Sicherheit in der gesamten Flotte.



Sicherheitspartner: KI-gestützte Erkennung und Reaktion ›

KI-gestützte Sicherheitstools ermöglichen kontinuierliches Monitoring, forensische Ermittlungen und die automatisierte Eindämmung von Manipulationen oder anormalem Geräteverhalten, sodass schnelle Maßnahmen gegen Bedrohungen in der Lieferkette gewährleistet werden.

Angriffstyp: Software in der Lieferkette

Ihr Unternehmen bietet cloudbasierte Analysesoftware an, die von Krankenhäusern verwendet wird. Ihre Back-end-Services basieren auf einer weit verbreiteten Open-Source-Protokollierungsbibliothek, die von einem vertrauenswürdigen Drittanbieter auf GitHub verwaltet wird.

Ohne das Wissen Ihres Entwicklungsteams haben AngreiferInnen das GitHub-Konto kompromittiert und ein bösartiges Update mit verstecktem Code installiert, der folgende Zwecke verfolgt:

- Exfiltrieren von Umgebungsvariablen, einschließlich API-Schlüsseln (Application Programming Interface) und JWT-Secrets (JSON Web Token)
- Erstellen einer Reverse Shell, wenn bestimmte IP-Adressen Anfragen stellen
- Inaktivität bis zur Remoteauslösung

Testen Sie Ihr Wissen →

Angriffstyp: Software in der Lieferkette

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Ihre API gibt plötzlich 500 Fehler an wichtige Clients zurück. Die Cloud-Überwachung zeigt ausgehende Verbindungen von Ihren containerbasierten Services zu einer bisher unbekannten Domain. Was ist Ihre erste Reaktion?

- [ ] Gesamten ausgehenden Netzwerkverkehr von Containern deaktivieren
- [ ] Betroffene Services neu starten, um eventuelle Speicherprobleme zu beheben
- [ ] GitHub-Repository auf aktuelle Code-Commits überprüfen
- [ ] Hostinganbieter der Domain kontaktieren

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Software in der Lieferkette

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Ihre API gibt plötzlich 500 Fehler an wichtige Clients zurück. Die Cloud-Überwachung zeigt ausgehende Verbindungen von Ihren containerbasierten Services zu einer bisher unbekannten Domain. Was ist Ihre erste Reaktion?

- ✓ Gesamten ausgehenden Netzwerkverkehr von Containern deaktivieren
- ✗ Betroffene Services neu starten, um eventuelle Speicherprobleme zu beheben
- ✗ GitHub-Repository auf aktuelle Code-Commits überprüfen
- ✗ Hostinganbieter der Domain kontaktieren

Die Deaktivierung des gesamten ausgehenden Netzwerkverkehrs von Containern verhindert sofort, dass AngreiferInnen sensible Daten exfiltrieren oder Remotezugriff über die kompromittierte Protokollierungsbibliothek erlangen. Dadurch können Sie Ihre Umgebung in Echtzeit isolieren und wichtige Zeit für die Untersuchung und die Sicherung von API-Schlüsseln und Secrets gewinnen sowie die Aktivierung ruhender Angriffsmechanismen verhindern.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Software in der Lieferkette

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihre IT-Abteilung bestätigt, dass die Anwendung drei Tage vor Beginn der Probleme automatisch Code von GitHub abgerufen hat. Diese Version ist in öffentlichen Datenbanken noch nicht als bösartig markiert. Was ist die verantwortungsvollste Sofortmaßnahme?

- [ ] Verwalter der Bibliothek direkt über GitHub kontaktieren
- [ ] Alle lokalen Projektabhängigkeiten löschen und neu erstellen
- [ ] Auf die Erkennung und Korrektur weit verbreiteter Sicherheitslücken und Risiken (Common Vulnerabilities and Exposures, CVEs) warten, bevor Sie weitere Maßnahmen ergreifen
- [ ] Rollback auf die letzte bekannte sichere Version des Codes durchführen

Die richtige Antwort →

Angriffstyp: Software in der Lieferkette

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Ihre IT-Abteilung bestätigt, dass die Anwendung drei Tage vor Beginn der Probleme automatisch Code von GitHub abgerufen hat. Diese Version ist in öffentlichen Datenbanken noch nicht als bösartig markiert. Was ist die verantwortungsvollste Sofortmaßnahme?

- ✗ Verwalter der Bibliothek direkt über GitHub kontaktieren
- ✗ Alle lokalen Projektabhängigkeiten löschen und neu erstellen
- ✗ Auf die Erkennung und Korrektur weit verbreiteter Sicherheitslücken und Risiken (Common Vulnerabilities and Exposures, CVEs) warten, bevor Sie weitere Maßnahmen ergreifen
- ✓ Rollback auf die letzte bekannte sichere Version des Codes durchführen

Durch das Zurücksetzen auf die letzte bekannte sichere Codeversion wird das kompromittierte Update sofort entfernt, der Zugriff für die AngreiferInnen entfernt und die betriebliche Integrität wiederhergestellt, um Risiken proaktiv einzudämmen und sensible Daten zu schützen.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Software in der Lieferkette

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Die Analyse bestätigt, dass die Bibliothek API-Schlüssel und Cloud-Anmeldedaten exfiltriert hat. Sie haben mehrere Container identifiziert, die mit der kompromittierten Version erstellt wurden. Welcher Schritt ist bei Ihrer Eindämmungsstrategie am wichtigsten?

- [ ] Alle Zugangsdaten für die betroffenen Umgebungen widerrufen und rotieren
- [ ] Neues Image der Container mithilfe eines aktualisierten Betriebssystem-Image erstellen
- [ ] Daten der Laptops des Entwicklungsteams löschen
- [ ] Entfernungsmeldung für das GitHub-Repository einreichen

Die richtige Antwort →

Angriffstyp: Software in der Lieferkette

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Die Analyse bestätigt, dass die Bibliothek API-Schlüssel und Cloud-Anmeldedaten exfiltriert hat. Sie haben mehrere Container identifiziert, die mit der kompromittierten Version erstellt wurden. Welcher Schritt ist bei Ihrer Eindämmungsstrategie am wichtigsten?

- ✓ Alle Zugangsdaten für die betroffenen Umgebungen widerrufen und rotieren
- ✗ Neues Image der Container mithilfe eines aktualisierten Betriebssystem-Image erstellen
- ✗ Daten der Laptops des Entwicklungsteams löschen
- ✗ Entfernungsmeldung für das GitHub-Repository einreichen

Das Widerrufen und Rotieren der Zugangsdaten ist der erste wichtige Schritt nach einer Cloud-Kompromittierung. Dadurch werden AngreiferInnen daran gehindert, auf Services zuzugreifen, Datendiebstahl wird gestoppt und die Systeme werden gesichert, unabhängig vom Umfang der Sicherheitsverletzung.

Nächste Frage →

Angriffstyp: Software in der Lieferkette

1 — 2. — 3 — 4: Allgemeine Best Practices

Sie werden gebeten, den Vorfall Ihrem Chief Technology Officer und Ihren Rechts-/Compliance-Teams zu erklären. Was ist die genaueste und deutlichste Erklärung? Wie können Sie den Vorfall zusammenfassen?

- [ ] Unsere internen Tools für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) haben versagt, sodass fehlerhafter Code bereitgestellt werden konnte.
- [ ] Eine Softwareabhängigkeit eines Drittanbieters wurde kompromittiert und durch unsere Automatisierung in die Produktionsumgebung übernommen.
- [ ] Ein Mitglied des Entwicklungsteams hat nicht getesteten Code in eine überstürzte Veröffentlichung aufgenommen.
- [ ] Es hat ein Brute-Force-Angriff auf unser GitHub-Repository stattgefunden.

Die richtige Antwort →

Angriffstyp: Software in der Lieferkette

1 — 2. — 3 — 4: Allgemeine Best Practices

Sie werden gebeten, den Vorfall Ihrem Chief Technology Officer und Ihren Rechts-/Compliance-Teams zu erklären. Was ist die genaueste und deutlichste Erklärung? Wie können Sie den Vorfall zusammenfassen?

- ✗ Unsere internen Tools für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) haben versagt, sodass fehlerhafter Code bereitgestellt werden konnte.
- ✓ Eine Softwareabhängigkeit eines Drittanbieters wurde kompromittiert und durch unsere Automatisierung in die Produktionsumgebung übernommen.
- ✗ Ein Mitglied des Entwicklungsteams hat nicht getesteten Code in eine überstürzte Veröffentlichung aufgenommen.
- ✗ Es hat ein Brute-Force-Angriff auf unser GitHub-Repository stattgefunden.

Die Ursache war ein Angriff auf die Lieferkette: AngreiferInnen haben eine Drittanbieter-Softwareabhängigkeit kompromittiert und der automatisierte Build-Prozess hat das bösartige Update direkt in die Produktion übernommen. Dadurch wurden die Anwendungsintegrität und sensible Umgebungen beeinträchtigt, wodurch das Risiko bösartiger Updates in vertrauenswürdigen externen Abhängigkeiten deutlich wurde.

Lösungen entdecken →

ANGRIFFSTYP: SOFTWARE IN DER LIEFERKETTE

Zusammenfassung

Cyberangriffe auf Software in der Lieferkette nutzen Sicherheitslücken in Softwareupdates, Integrationen von Drittanbietern und Entwicklungsumgebungen aus, um bösartigen Code einzubetten, der sich über Netzwerke verteilt. Diese Angriffe können zu weit verbreiteten Datenschutzverletzungen, Betriebsunterbrechungen und einer Gefährdung ganzer Umgebungen führen, was sich auf Unternehmen jeder Größe auswirkt.

Dell setzt sich für die Ausfallsicherheit bei Cyberangriffen ein, indem Transparenz, sichere Entwicklung und kontinuierliches Monitoring priorisiert und gleichzeitig ein robuster Incident-Response-Plan verfolgt wird, um eine schnelle Recovery und die Kommunikation mit Stakeholdern sicherzustellen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor Angriffen auf Software in der Lieferkette schützen kann.

Kurzbeschreibung zu Angriffen auf Software in der Lieferkette lesen →

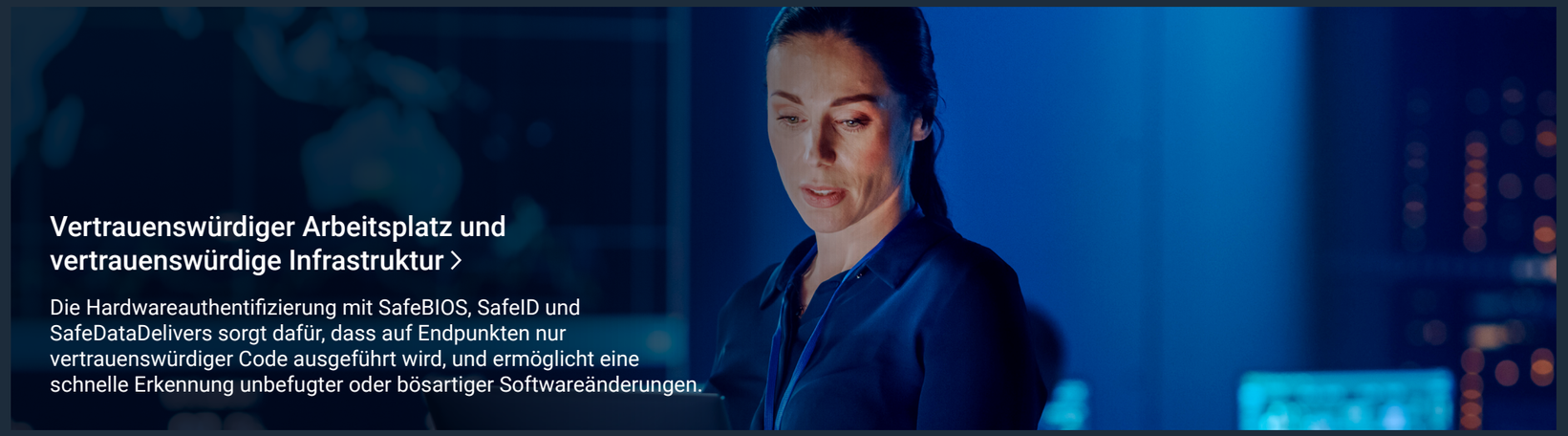
Zurück zu Szenarien

Sicherheit in der Lieferkette ›

Mit fortschrittlicher Herkunftsnachverfolgung, manipulationssicherer Logistik und transparenter Beschaffung sorgt die Lieferkette von Dell dafür, dass Hardware, Firmware und Lieferanten streng geprüft werden, bevor sie Ihr Unternehmen erreichen.

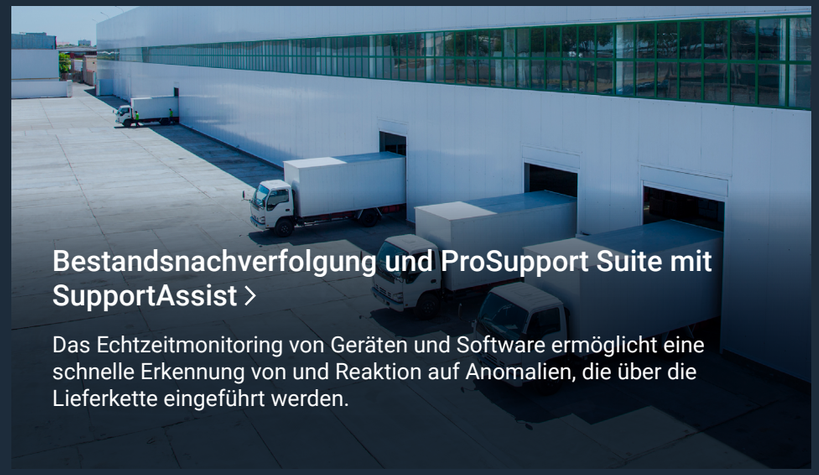
Secure Development Lifecycle (SDL) ›

Implementierung branchenführender sicherer Entwicklungspraktiken, um Risiken durch Abhängigkeiten von Drittanbietern zu reduzieren und softwarebasierte Angriffe über bereitgestellte Lösungen zu verhindern.



Vertrauenswürdiger Arbeitsplatz und vertrauenswürdige Infrastruktur ›

Die Hardwareauthentifizierung mit SafeBIOS, SafeID und SafeDataDelivers sorgt dafür, dass auf Endpunkten nur vertrauenswürdiger Code ausgeführt wird, und ermöglicht eine schnelle Erkennung unbefugter oder bösartiger Softwareänderungen.



Bestandsnachverfolgung und ProSupport Suite mit SupportAssist ›

Das Echtzeitmonitoring von Geräten und Software ermöglicht eine schnelle Erkennung von und Reaktion auf Anomalien, die über die Lieferkette eingeführt werden.

Sicherheitspartner: KI-gestützte Erkennung und Eindämmung ›

Aufdeckung, Blockierung und schnelle Korrektur von Angriffen über die Softwarelieferkette, einschließlich Angriffen über Open-Source- oder Drittanbietercode.

Angriffstyp: Zero-Day

Als SicherheitsanalystIn überwachen Sie die Authentifizierungsprotokolle eines Unternehmens. In letzter Zeit haben NutzerInnen unbefugte Zugriffe auf ihre Konten gemeldet, obwohl sie ihre Zugangsdaten nicht weitergegeben hatten.

Bei der Überprüfung der Protokolle finden Sie die folgende Aktivität:

```
[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
```

Gleichzeitig identifizieren SicherheitsforscherInnen eine Sicherheitslücke in der API (Application Programming Interface):

- JSON Web Token (JWT) laufen niemals ab.
- Token werden im lokalen Speicher anstelle von reinen HTTP-Cookies gespeichert.
- Es wird keine Multifaktor-Authentifizierung (MFA) erzwungen.

Testen Sie Ihr Wissen →

Angriffstyp: Zero-Day

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Da keine Warnsignale ausgelöst wurden, vermuten Sie als Sicherheitsteam, dass es sich um einen Zero-Day-Angriff handelt. Wie würden Sie vorgehen, um dies zu bestätigen?

- [ ] Alle NutzerInnen von ihren Systemen abmelden
- [ ] Wichtige anormale Authentifizierungsverhaltensweisen in Protokollen identifizieren
- [ ] Bekannte in anderen Unternehmen anrufen, um zu erfragen, ob sie dasselbe Problem haben
- [ ] Versuchen, einen Zusammenhang mit anderen ungewöhnlichen Sicherheitsaktivitäten herzustellen

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1: Verkleinerung der Angriffsfläche — 2 — 3 — 4.

Da keine Warnsignale ausgelöst wurden, vermuten Sie als Sicherheitsteam, dass es sich um einen Zero-Day-Angriff handelt. Wie würden Sie vorgehen, um dies zu bestätigen?

- ✗ Alle NutzerInnen von ihren Systemen abmelden
- ✓ Wichtige anormale Authentifizierungsverhaltensweisen in Protokollen identifizieren
- ✗ Bekannte in anderen Unternehmen anrufen, um zu erfragen, ob sie dasselbe Problem haben
- ✓ Versuchen, einen Zusammenhang mit anderen ungewöhnlichen Sicherheitsaktivitäten herzustellen

Durch Identifizieren von anormalem Authentifizierungsverhalten wie ungewöhnlichen Anmeldezeiten, Wiederverwendung von Anmeldedaten oder Zugriff von atypischen Geräten und Korrelieren dieser Verhaltensweisen mit anderen anormalen Sicherheitsaktivitäten wie Datenzugriffsanomalien oder Berechtigungseskalation kann ein koordinierter Zero-Day-Angriff bestätigt werden.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Da die Sicherheitslücke unbekannt ist, müssen Sicherheitsteams den Schaden während der Untersuchung begrenzen. Wie würden Sie dazu vorgehen?

- [ ] Alle Authentifizierungssitzungen systemweit ungültig machen
- [ ] Alle Ressourcen auf den Einstiegspunkt des Angriffs konzentrieren
- [ ] Nur Anmeldungen mit Multi-Faktor-Authentifizierung (MFA) zulassen
- [ ] Auf aktuelle statische Firewalls oder WAF-Regeln (Web Application Firewall) verlassen

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2: Erkennung von und Reaktion auf Cyberbedrohungen — 3 — 4.

Da die Sicherheitslücke unbekannt ist, müssen Sicherheitsteams den Schaden während der Untersuchung begrenzen. Wie würden Sie dazu vorgehen?

- ✓ Alle Authentifizierungssitzungen systemweit ungültig machen
- ✗ Alle Ressourcen auf den Einstiegspunkt des Angriffs konzentrieren
- ✓ Nur Anmeldungen mit Multi-Faktor-Authentifizierung (MFA) zulassen
- ✗ Auf aktuelle statische Firewalls oder WAF-Regeln (Web Application Firewall) verlassen

Gemeinsam stärken diese Maßnahmen die Sicherheit, minimieren Risiken und unterbinden gleichzeitig den Zugriff der AngreiferInnen, damit Sicherheitsteams die zugrunde liegende Sicherheitslücke untersuchen und beheben können.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Dell PCs verfügen über Technologien wie Secure Boot, Trusted Platform Modules (TPM), BIOS-Kennwortschutz (Basic Input/Output System) und SafeBIOS. Wie können diese bei einem Zero-Day-Angriff hilfreich sein?

- [ ] Schutz vor Credential-Dumping-Angriffen, bei denen API-Token (Application Programming Interface) gestohlen werden
- [ ] Verhinderung, dass AngreiferInnen mit physischem Zugriff die Betriebssystemsicherheit umgehen, um Malware zu installieren und so Authentifizierungstoken zu stehlen
- [ ] Sicherstellung, dass AngreiferInnen die BIOS-Einstellungen nicht manipulieren können, um die Sicherheit des Betriebssystems zu schwächen, was zu einer API-Sitzungsübernahme führen könnte
- [ ] Alle oben genannten Antworten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2. — 3: Recovery nach einem Cyberangriff — 4

Dell PCs verfügen über Technologien wie Secure Boot, Trusted Platform Modules (TPM), BIOS-Kennwortschutz (Basic Input/Output System) und SafeBIOS. Wie können diese bei einem Zero-Day-Angriff hilfreich sein?

- [x] Schutz vor Credential-Dumping-Angriffen, bei denen API-Token (Application Programming Interface) gestohlen werden
- [x] Verhinderung, dass AngreiferInnen mit physischem Zugriff die Betriebssystemsicherheit umgehen, um Malware zu installieren und so Authentifizierungstoken zu stehlen
- [x] Sicherstellung, dass AngreiferInnen die BIOS-Einstellungen nicht manipulieren können, um die Sicherheit des Betriebssystems zu schwächen, was zu einer API-Sitzungsübernahme führen könnte
- [x] Alle oben genannten Antworten

Dieser mehrschichtige Ansatz bietet umfassenden Schutz vor Zero-Day-Angriffen auf BIOS, Firmware, Zugangsdaten und Systemkonfigurationen. Durch die Verhinderung von Manipulationen, unbefugtem Zugriff und Diebstahl von Zugangsdaten bleiben diese Technologien auch dann effektiv, wenn neue Sicherheitslücken von Angreifern erkannt werden.

Nächste Frage →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2. — 3 — 4: Allgemeine Best Practices

Was ist die beste Möglichkeit, Zero-Day-Angriffe zu verhindern?

- [ ] Keine Open-Source-Software verwenden
- [ ] Zero-Trust-Prinzipien nutzen
- [ ] Alle Komponenten auf dem neuesten Stand halten, einschließlich Betriebssysteme (BS), Firmware, Anwendungsprogrammierschnittstellen (APIs), Bibliotheken und Container
- [ ] Unternehmenssysteme vollständig absichern, um AngreiferInnen fernzuhalten

Die richtige Antwort →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

Angriffstyp: Zero-Day

1 — 2. — 3 — 4: Allgemeine Best Practices

Was ist die beste Möglichkeit, Zero-Day-Angriffe zu verhindern?

- ✗ Keine Open-Source-Software verwenden
- ✓ Zero-Trust-Prinzipien nutzen
- ✗ Alle Komponenten auf dem neuesten Stand halten, einschließlich Betriebssysteme (BS), Firmware, Anwendungsprogrammierschnittstellen (APIs), Bibliotheken und Container
- ✗ Unternehmenssysteme vollständig absichern, um AngreiferInnen fernzuhalten

Wenn unbekannte Schwachstellen oder nicht gepatchte Systeme vorhanden sind, verhindern Zero-Trust-Prinzipien Zero-Day-Angriffe, indem sie das implizite Vertrauen von BenutzerInnen und Geräten entfernen, eine kontinuierliche Authentifizierung erzwingen, den Zugriff nur auf erforderliche Informationen beschränken und die Bewegungen von AngreiferInnen einschränken, um das Risiko für Unternehmen durch nicht erkannte Bedrohungen erheblich zu reduzieren.

Lösungen entdecken →

DELL Technologies

Interaktives E-Book zu Cybersicherheitsszenarien

ANGRIFFSTYP: ZERO-DAY

Zusammenfassung

Bei einem Zero-Day-Angriff wird eine nicht offengelegte Sicherheitslücke in Software oder Hardware ausgenutzt, bevor ein Patch oder eine Korrektur verfügbar ist. AngreiferInnen nutzen dieses Zeitfenster und verursachen oft weitreichende Unterbrechungen, bevor die Sicherheitslücke entdeckt und behoben wird.

Dell bewältigt Zero-Day-Angriffe mit Zero-Trust-Kontrollen, Netzwerksegmentierung, schneller Eindämmung und Nutzerschulung und stärkt die Abwehr von neuen Bedrohungen.

Erfahren Sie mehr über fortgeschrittene Strategien für die Ausfallsicherheit bei Cyberangriffen und darüber, wie Dell Ihre Organisation vor Zero-Day-Angriffen schützen kann.

Kurzbeschreibung zu Zero-Day-Angriffen lesen →

Zurück zu Szenarien

Vertrauenswürdiger Arbeitsplatz und vertrauenswürdige Infrastruktur ›

Schutz von Endpunkten und Infrastruktur Mit SafeBIOS, SafeID, SafeData-Schutzmaßnahmen und Zero-Trust-Frameworks wie Multi-Faktor-Authentifizierung (MFA) und rollenbasierter Zugriffskontrolle (RBAC) bietet Dell mehrschichtige Abwehrmaßnahmen, um Exploit-Pfade zu begrenzen und die Hardwareauthentifizierung sicherzustellen.

PowerEdge-Server ›

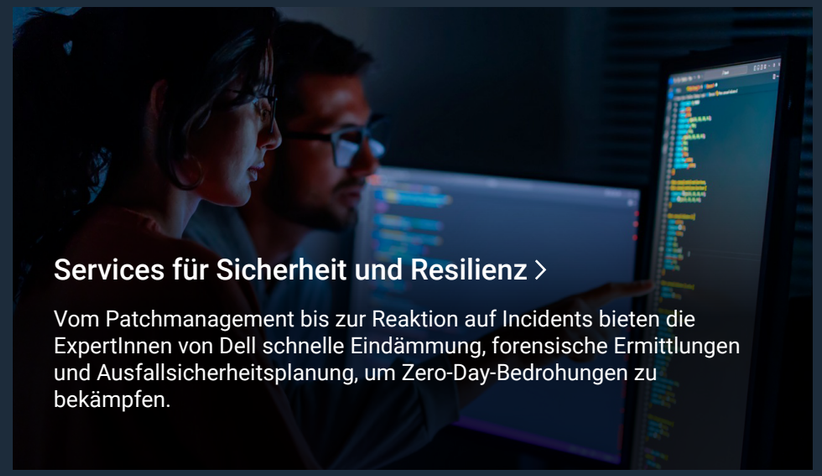
Secure Boot, Silicon Root of Trust und SmartFabric-Netzwerksegmentierung schränken laterale Bewegungen ein und stellen sicher, dass nur vertrauenswürdiger Code in Ihrer Infrastruktur ausgeführt wird.

Sicherheitspartner ›

Advanced Threat Intelligence, Management Detection and Response (MDR), Extended Detection and Response (XDR) und optimal abgestimmte Zugriffskontrollen helfen dabei, Zero-Day-Angriffe zu erkennen, aufzuspüren und einzudämmen, bevor sie sich ausbreiten können.

PowerProtect-Portfolio ›

Unveränderliche Backups, isolierte Cyber-Recovery-Vaults und KI-gestützte CyberSense-Analysen sorgen für eine schnelle Wiederherstellung und Ausfallsicherheit nach Zero-Day-Sicherheitsverletzungen.



Services für Sicherheit und Resilienz ›

Vom Patchmanagement bis zur Reaktion auf Incidents bieten die ExpertInnen von Dell schnelle Eindämmung, forensische Ermittlungen und Ausfallsicherheitsplanung, um Zero-Day-Bedrohungen zu bekämpfen.


DELL Technologies