Backup-Infiltration: Stärkung der Cybersicherheit und Resilienz mit Dell Technologies

Zusammenfassung

Backup-Infiltration stellt eine wachsende Bedrohung für Unternehmen in jedem Sektor dar und nutzt Sicherheitslücken in den Systemen aus, die darauf ausgelegt sind, kritische Informationen zu schützen. Diese Angriffe gefährden die Datenwiederherstellungssysteme, untergraben das Vertrauen und gefährden die Betriebsabläufe. Von erheblichen finanziellen Verlusten bis hin zu längeren Ausfallzeiten und Reputationsschäden können die Folgen schwerwiegend sein.

Dell Technologies bietet eine End-to-End-Suite an Abwehrmaßnahmen, um sensible Daten zu schützen und diese Angriffe zu verhindern, darunter Dell Trusted Devices, Dell Trusted Infrastructure und umfassende Sicherheitsfunktionen, die in alle unsere Lösungen integriert sind. Durch strategische Partnerschaften und professionelle Dienstleistungen unterstützt Dell Unternehmen beim Aufbau eines robusten, mehrschichtigen Sicherheitsframeworks, um Vorfälle von Backup-Infiltration effizient zu erkennen, zu verhindern und zu beheben.

Durch die Implementierung der innovativen Lösungen und des fachkundigen Supports von Dell sind Unternehmen besser darauf vorbereitet, ihre Infrastruktur zu sichern und die betriebliche Kontinuität aufrechtzuerhalten.

Steigende Bedrohung durch Backup-Infiltration

Backup-Systeme sind für die Gewährleistung der Geschäftskontinuität unerlässlich und spielen eine entscheidende Rolle bei der Wiederherstellung nach Cyber-Vorfällen wie Ransomware-Angriffen oder Hardwareausfällen. Leider werden gerade diese Lebenswege zunehmend von Cyberkriminellen angegriffen. Durch Backup-Infiltrationen werden Backup-Daten beschädigt oder gelöscht, sodass sie gerade dann nicht mehr zugänglich sind, wenn sie am dringendsten benötigt werden.

Diese sich entwickelnden Bedrohungen erfordern proaktive Maßnahmen. Wenn Backupsysteme nicht geschützt werden, wird der Betrieb gefährdet und sensible Daten werden offengelegt. Unternehmen jeder Größe, von kleinen Firmen bis hin zu multinationalen Konzernen, sind potenzielle Ziele, wobei Branchen wie Gesundheitswesen, Finanzen und Fertigung besonders gefährdet sind.

Dell Technologies erkennt die Dringlichkeit der Verstärkung von Backupumgebungen und bietet erweiterte Tools und Anleitungen, um diesen ausgefeilten Angriffen entgegenzuwirken.

Backup-Infiltrationsangriffe

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.

So funktionieren Backupangriffe

1. **Anfängliche Sicherheitsverletzung:** AngreiferInnen verschaffen sich unbefugten Zugriff auf das Netzwerk, häufig durch Phishing, schwache Anmeldedaten oder ungepatchte Sicherheitslücken.
2. **Laterale Ausbreitung:** Sobald sie sich im Netzwerk befinden, nutzen AngreiferInnen Tools, um sich unentdeckt zu bewegen und Backup-Repositorys und kritische Datensätze anzugreifen.
3. **Backup-Kompromittierung:** Zu den wichtigsten Taktiken gehören die Verschlüsselung von Backupdateien, das Löschen von Recovery-Punkten und die Beschädigung von Daten.

Gängige Techniken

- **Diebstahl von Anmeldedaten:** Durch den Diebstahl von Anmeldedaten für Administratorkonten wird ein vollständiger Zugriff auf Backupsysteme ermöglicht.
- **Ransomware** verschlüsselt sowohl Live-Daten als auch Backups, um eine Zahlung für die Entschlüsselung zu erzwingen.
- **Zeitgesteuerte Beschädigung:** Backups werden schrittweise kompromittiert, um einer Entdeckung zu entgehen, während Unternehmen bei einer erforderlichen Recovery ungeschützt bleiben.

Solche Techniken verdeutlichen die Raffinesse und Schwere dieser Bedrohungen und erfordern vorbeugende Maßnahmen.

Auswirkungen auf Unternehmen

Finanzielle Verluste

Backup-Infiltration erhöht die Recovery-Kosten und Ausfallzeiten und verdoppelt oder verdreifacht oft die Reaktionskosten. Die Recovery verschlüsselter oder kompromittierter Backups kann Zahlungen an AngreiferInnen, neue Infrastruktur oder teure Beratung erfordern.

Betriebsunterbrechung

Ohne funktionsfähige Backups sehen sich Unternehmen mit langen Recovery-Zeiten konfrontiert, die zu Serviceunterbrechungen, Projektverzögerungen und dem Ausfall kritischer Funktionen führen.

Reputationsfolgen

Dauerhafter Datenverlust oder längere Ausfallzeiten untergraben das Vertrauen von StakeholderInnen und beeinträchtigen potenziell die langfristige Rentabilität eines Unternehmens.

Praxisbeispiel

Ein globaler Anbieter im Gesundheitswesen hat festgestellt, dass seine Backups während eines Ransomwareangriffs beschädigt wurden. Trotz Zahlung des Lösegelds gingen Patientendaten aus drei Wochen dauerhaft verloren, was zu Verzögerungen bei den Betriebsabläufen und zu Rechtsstreitigkeiten führte. Die Gesamtkosten für die Recovery überstiegen **50 Millionen USD.**

Alarmierende Statistiken

Aktuelle Studien schätzen, dass die durchschnittlichen finanziellen Schäden durch ein kompromittiertes Backupsystem **4,45 Millionen USD**[1] übersteigen, einschließlich Bußgeldern, Ausfallzeiten und Wiederherstellungskosten. Besonders alarmierend ist die zunehmende Häufigkeit solcher Vorfälle. Globale Berichte zeigen einen Anstieg der Backupbedrohungen **um 39 %** im Vergleich zum Vorjahr.

57 %
der Angriffe auf Backups dringen erfolgreich in Backup-Repositorys ein.

Quelle: 2024: Index Engines

Bekämpfung der Backup-Infiltration mit Dell Technologies

Dell Technologies bietet eine robuste Suite an Tools und Services, die die besonderen Herausforderungen von Backup-Infiltrationsangriffen angehen, sodass Unternehmen diese effektiv verhindern, erkennen und wiederherstellen können.

Server- und Storage-Sicherheitslösungen

Die Server- und Storage-Lösungen von Dell bieten eine beispiellose Resilienz gegenüber Angriffen auf Backups. Integrierte Funktionen sorgen dafür, dass Backups sicher bleiben und Snapshots nicht kompromittiert werden.

- **Unveränderliche Backups/Snapshots** erstellen manipulationssichere Wiederherstellungspunkte.
- **Air-Gap Recovery** isoliert Daten von Live-Netzwerken, um Beschädigungen zu vermeiden.

[1] Ponemon – Cost of a Data Breach Report 2024

Sichern Sie Ihre Dell Data Protection Appliances

Dell Data Protection Appliances verfügen über integrierte Funktionen wie Dell SafeBIOS für Firmwareintegrität und SafeData für sichere Verschlüsselung, um vor Backupangriffen zu schützen. Darüber hinaus bieten diese Lösungen Funktionen wie Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrollen (RBAC) und doppelte Authentifizierung, um AngreiferInnen fernzuhalten.

Erweiterte Bedrohungserkennung mit CrowdStrike

Bei der Integration von CrowdStrike und Dell Data Protection liegt der Fokus auf der Verbesserung der Sicherheit und Überwachung von Data-Protection-Umgebungen durch eine Reihe fortschrittlicher Funktionen.

1. **Endpunktschutz und Data Protection:** Dell integriert die Endpoint Security und Extended Detection and Response (EDR/XDR) von CrowdStrike in seine Data-Protection-Lösungen. Dazu gehören die Erfassung von Telemetriedaten aus Dell PowerProtect Data Manager und PowerProtect Data Domain sowie Sicherheitsinformationen aus der CrowdStrike Falcon-Konsole und der SIEM-Software der nächsten Generation.
2. **Monitoring und Reaktion:** Der Managed Detection and Response (MDR)-Service von Dell verwaltet die CrowdStrike-Software im Auftrag von Kunden, erfasst Protokolle und untersucht alle Indikatoren für Kompromittierungen (IoC) oder erkannte Anomalien. Diese Integration ermöglicht es Dell, ein kontinuierliches Monitoring bereitzustellen und mit dem SOC des Kunden zusammenzuarbeiten, um eine schnelle und effektive Abwehr von Bedrohungen sicherzustellen.
3. **Echtzeit-Transparenz und Kontrolle der Datenbewegungen:** Die CrowdStrike Falcon Data Protection-Plattform bietet Echtzeiteinblicke in die Datenbewegungen über verschiedene Quellen und Kanäle hinweg und klassifiziert Daten sowohl nach Inhalt als auch nach Kontext. Dies trägt dazu bei, Datendiebstahl zu verhindern und sicherzustellen, dass Datenschutzrichtlinien durch die Kombination von Inhalten mit kontextbezogenen Analysen effektiv durchgesetzt werden.
4. **Einheitliches Management und vereinfachte Bereitstellung:** Die Integration ermöglicht die Verwaltung von Endpunktschutz und Data Protection über eine einzige Plattform und einen einzigen Agenten, wodurch die Komplexität und der Betriebsaufwand reduziert werden. Dies wird durch den schlanken und cloudnativen Ansatz der CrowdStrike Falcon-Plattform erleichtert, der eine schnelle Bereitstellung und minimale Unterbrechungen ermöglicht.

Die Integration zwischen CrowdStrike und Dell Data Protection nutzt fortschrittliche EDR/XDR-Funktionen, Echtzeitmonitoring und umfassendes Datenmanagement, um die allgemeine Sicherheit und Resilienz von Data-Protection-Umgebungen zu verbessern.

Ein führendes Finanzinstitut hat kürzlich PowerProtect Cyber Recovery implementiert und so verhindert, dass AngreiferInnen während eines Angriffs auf 90 % der kritischen Backups zugreifen konnten, was eine nahtlose Wiederherstellung ohne Lösegeldzahlungen ermöglichte.

Dell PowerProtect-Lösungen für Backupintegrität

Dell PowerProtect bietet umfassenden Backupschutz und nutzt Unveränderlichkeit, Isolierung und Komprimierung, um Kompromittierungen des Backupsystems zu verhindern. Durch die Integration in Tools zur Erkennung von Ransomware stellt PowerProtect sicher, dass verdächtige Änderungen Warnmeldungen auslösen, sodass sofortige Maßnahmen ergriffen werden können.

Mehrschichtiger Sicherheitsansatz

Der Schutz von Daten erfordert koordinierte, facettenreiche Sicherheitsstrategien. Dell unterstützt Unternehmen bei der Implementierung von branchenspezifischen Best Practices, um eine ausfallsichere Backupumgebung aufzubauen.

Wichtige Schritte zur Verbesserung der Verteidigung

- **Anwendung von Zero-Trust-Prinzipien:** Kontinuierliche Validierung aller NutzerInnen, Geräte und Prozesse, wodurch das Risiko unbefugter Zugriffe reduziert wird.
- **Verschlüsselung aller Backups:** Stellen Sie sicher, dass Daten sowohl während der Übertragung als auch im Ruhezustand unlesbar bleiben, auch wenn sie kompromittiert werden.
- **Schulung der MitarbeiterInnen:** Bringen Sie Ihren MitarbeiterInnen bei, Phishing-Versuche und andere Social-Engineering-Taktiken zu erkennen, die zu ersten Sicherheitsverletzungen führen.
- **Regelmäßige Schwachstellenprüfungen:** Durch häufige Tests können Unternehmen Schwachpunkte identifizieren und beheben, bevor AngreiferInnen diese ausnutzen.

Dell kombiniert diese Praktiken mit hochmodernen Lösungen und schafft so eine robuste und reaktionsschnelle Infrastruktur, die für die Bewältigung neuer Herausforderungen gerüstet ist.

Strategische Partnerschaften zur Verbesserung der Sicherheit

Dell arbeitet mit führenden Anbietern im Bereich Cybersicherheit wie Microsoft, CrowdStrike und Secureworks zusammen. Jede Partnerschaft ergänzt die Lösungen von Dell und bietet Kunden unübertroffene Schutzfunktionen wie erweiterte Bedrohungsdaten, Endpunktüberwachung und umfassende Reaktionsstrategien.

Nutzung von Dell Professional Services

Die Professional Services von Dell Technologies bieten Fachwissen und Beratung, um Unternehmen dabei zu unterstützen, komplexe Herausforderungen im Bereich Cybersicherheit effektiv zu bewältigen. Von der Erstellung von Incident-Response-Plänen bis zur Implementierung von Zero-Trust-Architekturen sorgen die SpezialistInnen von Dell dafür, dass Kundenumgebungen gegenüber modernen Bedrohungen wie Backup-Infiltration resilient bleiben.

Aufbau der geschäftlichen Ausfallsicherheit mit Dell

Wenn Sie sich für Dell Technologies entscheiden, können Unternehmen raffinierte AngreiferInnen überlisten und gleichzeitig die betriebliche Kontinuität aufrechterhalten. Durch Innovation, Partnerschaften und Fachwissen stellt Dell sicher, dass Unternehmen selbst die schwersten Backup-Infiltrationsangriffe verhindern, erkennen und sich davon erholen können.

Unternehmen Sie den nächsten Schritt

Wenden Sie sich noch heute an Dell Technologies, um Ihr Unternehmen zu schützen. Gemeinsam sichern wir Ihre kritischen Ressourcen, schützen Ihren Ruf und schaffen eine resiliente Zukunft.

Dell setzt sich weiterhin dafür ein, Vertrauen in das digitale Zeitalter zu fördern und Unternehmen die Tools, das Wissen und den Support zur Verfügung zu stellen, die sie benötigen, um sicher zu arbeiten und erfolgreich zu sein.

Backup-Resilienz beginnt mit Dell Technologies. Handeln Sie jetzt, um Ihre Abläufe zukunftssicher zu gestalten und Vertrauen in Ihre Cybersicherheitsstrategie aufzubauen.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **Dell.com/SecuritySolutions**

Weitere Informationen zu Dell Lösungen

Kontaktieren Sie die Dell Technologies ExpertInnen.

Weitere Ressourcen anzeigen

Kommen Sie ins Gespräch über #HashTag

DELL Technologies