Cyberresilienz beginnt mit proaktiver Bedrohungserkennung

Cyberangriffe entwickeln sich kontinuierlich weiter und erhöhen den Druck auf Unternehmen, ihre Daten und Systeme zuverlässig zu schützen. Moderne Sicherheitslösungen unterstützen dabei mit Funktionen zur proaktiven Bedrohungserkennung sowie erweiterten Schutzmechanismen im Active Directory-Umfeld. Diese Kombination schafft eine stabile Grundlage für widerstandsfähige IT-Strukturen.

Die Bedrohungslage für Unternehmen war nie komplexer als heute. Cyberkriminelle nutzen ausgefeilte Methoden wie Ransomware, Supply-Chain-Angriffe oder gezieltes Spear-Phishing. Neben klassischen IT-Infrastrukturen geraten zunehmend auch hybride und Cloud-Umgebungen ins Visier der Angreifer. Die Herausforderung besteht nicht mehr nur darin, Angriffe abzuwehren, sondern sie frühzeitig zu erkennen, ihre Auswirkungen zu begrenzen und eine schnelle Wiederherstellung zu ermöglichen. Commvault, bekannt für leistungsfähige Datenmanagement- und Backup-Lösungen, hat sein Portfolio um Sicherheitsfunktionen erweitert, die genau hier ansetzen. Mit Commvault ThreatWise und Commvault Threat Scan stellt das Unternehmen Werkzeuge bereit, die Organisationen dabei unterstützen, Bedrohungen frühzeitig zu erkennen und darauf zu reagieren – bevor es zu gravierenden Schäden kommt. Ergänzt wird dies durch erweiterte Schutzmechanismen für Identitäten und Zugriffsrechte in Microsoft Active Directory und Entra ID.

Commvault ThreatWise – proaktive Verteidigung durch Täuschungstechnologien

Traditionelle Sicherheitssysteme wie Firewalls oder Intrusion Detection Systeme arbeiten reaktiv: Sie melden verdächtiges Verhalten,

welches auf einen Angriff hindeuten kann. Das Problem daran: Oft vergeht wertvolle Zeit, in der Angreifer sich weiter im Netzwerk ausbreiten können.
ThreatWise setzt auf einen anderen Ansatz: proaktive Täuschung. Mithilfe sogenannter «Deception-Technologien» wird eine Art digitaler Köder ausgelegt – also realistisch wirkende, aber künstlich erzeugte Ressourcen, die für Angreifer wie attraktive Ziele erscheinen. Dazu gehören fingierte Datenbanken, Dateiserver oder Anwendungen, die im Netzwerk so positioniert werden, dass sie von Angreifern zwangsläufig entdeckt werden. Sobald ein Angreifer versucht, mit diesen Ressourcen zu interagieren, schlägt ThreatWise Alarm. Der grosse Vorteil: Diese Interaktionen deuten auf tatsächliche Angriffsversuche hin, nicht auf ein Fehlverhalten legitimer Nutzer. Unternehmen erhalten dadurch hochpräzise Warnungen ohne Fehlalarme – ein entscheidender Faktor, da Security-Teams oft mit zu vielen Alarmen überlastet sind. Darüber hinaus liefert ThreatWise wertvolle Informationen über die Angriffswege und -methoden, die ein Angreifer wählt. Diese Erkenntnisse können genutzt werden, um die Verteidigungsstrategie kontinuierlich zu verbessern. Auf diese Weise verwandelt sich eine vermeintliche Schwäche – der erste Angriff – in eine Gelegenheit, die eigene Sicherheitsarchitektur gezielt zu optimieren.

Commvault Threat Scan – Integrität der Daten sicherstellen

Ein weiterer zentraler Baustein einer zuverlässigen Cyberresilienz ist die Gewissheit, dass Backupdaten nicht bereits unbemerkt kompromittiert wurden. Threat Scan greift genau hier ein. Während Backups lange als «letzte Verteidigungslinie» galten, zeigt die Praxis: Schadsoftware wie Ransomware oder Viren können auch über Sicherungen in Systeme zurückgelangen, wenn diese zuvor unentdeckt infiziert wurden. Threat Scan untersucht deshalb aktiv gesicherte Daten, Snapshots und Backups auf potenzielle Bedrohungen. Dabei kommen Methoden wie Signaturvergleiche, Heuristik und KI-gestützte Mustererkennung zum Einsatz. Ziel ist es, versteckte Schadsoftware oder manipulierte Dateien zuverlässig aufzuspüren – bevor sie im Rahmen einer Wiederherstellung in die Produktionsumgebung zurückgeführt werden. Die Lösung geht aber über eine reine Virenprüfung hinaus: Sie erkennt auch untypische Anomalien im Datenbestand, die auf Manipulationen hindeuten könnten. Beispielsweise, wenn Dateistrukturen verändert wurden oder wenn unübliche Zugriffsmuster auf sensible Daten erkennbar sind. Besonders in regulierten Branchen wie dem Finanzwesen oder Gesundheitssektor unterstützt Threat Scan damit die Compliance-Anforderungen, die zunehmend fordern, dass Unternehmen die Integrität gesicherter Daten jederzeit nachweisen können.

Active Directory und Entra ID – Sicherheit für die Schaltzentrale der IT

Das Active Directory (AD) ist das Herzstück fast jeder Unternehmens-IT: Es verwaltet Benutzerkonten, Gruppenrichtlinien, Authentifizierungen und Zugriffsrechte. Damit ist es nicht nur ein kritischer Baustein, sondern auch ein bevorzugtes Angriffsziel. Ein kompromittiertes AD verschafft Angreifern weitreichende Rechte – bis hin zur vollständigen Kontrolle über die IT-Infrastruktur. Angriffe auf das AD erfolgen meist verdeckt: Cyberkriminelle versuchen, Administrator-Accounts zu übernehmen, Rechte zu eskalieren oder Replikationen zu manipulieren. Die Folgen sind gravierend – von unbefugtem Zugriff auf sensible Daten bis hin zur vollständigen Lahmlegung des Unternehmensnetzwerks. Commvault integriert spezielle Schutzmechanismen für Active Directory in seine Sicherheitsarchitektur. Dazu zählen Funktionen für die kontinuierliche Sicherung und die schnelle Wiederherstellung von AD-Daten. Ob durch Malware oder Insider-Aktivitäten – bei Manipulationen können Unternehmen ihr Active Directory auf einen bekannten, sauberen Zustand zurücksetzen und so ihre Handlungsfähigkeit rasch wiederherstellen. Für Unternehmen bedeutet das, dass ihre Identitäts- und Zugriffsverwaltung resilient bleibt – selbst im Falle eines Angriffs. Da AD häufig die Basis für Single Sign-On und Cloud-Integration bildet, schützt dieser Ansatz nicht nur lokale Systeme, sondern auch hybride und Multi-Cloud-Umgebungen.

Ganzheitliche Sicherheitsstrategie

Die drei Komponenten – ThreatWise, Threat Scan und Active Directory – zeigen, wie Commvault das klassische Backup in eine umfassende Sicherheitslösung transformiert. Während ThreatWise potenzielle Angriffe bereits im Entstehen erkennt, stellt Threat Scan sicher, dass nur saubere Daten in Wiederherstellungsprozesse gelangen. Mit dem Schutz für Active Directory wird zudem die Basis der Unternehmens-IT zuverlässig gesichert. Damit adressiert Commvault einige der grössten Herausforderungen einer zuverlässigen Cyberresilienz:

- Früherkennung: Angriffe in Echtzeit sichtbar machen
- Datenintegrität: Kompromittierte Datenbestände identifizieren
- Schutz: Kritische Infrastrukturen wie Active Directory absichern
- Compliance: Anforderungen von Gesetzgebern und Branchenstandards erfüllen

Fazit

Die Zeiten, in denen eine Backup-Lösung sich nur um die Datensicherung kümmert, sind vorbei. Unternehmen benötigen eine Sicherheitsarchitektur, die präventiv, analytisch und reaktiv zugleich agiert. Commvault hat diese Notwendigkeit erkannt und liefert mit ThreatWise, Threat Scan und Active Directory-Schutz Werkzeuge, die weit über klassisches Backup hinausgehen. In einer Welt, in der Cyberangriffe zunehmend professionell orchestriert werden, schaffen diese Lösungen den entscheidenden Vorteil: mehr Transparenz, mehr Kontrolle – und die Sicherheit, auch im Ernstfall handlungsfähig zu bleiben. ■

LC Systems-Engineering AG
Zum See 1, CH-9320 Arbon
✆ +41 (0)58 360 80 60
info@lcsystems.ch, www.lcsystems.ch