COHESITY

MERKBLATT

5 Wege, wie Schutz, Erkennung und Wiederherstellung die Cyber-Resilienz erhöhen

Überblick

Die Daten werden angegriffen. Der Anstieg der Ransomware-Bedrohungen um 1.070 % im Vergleich zum Vorjahr beweist dies[1]. Und die bösartigen Akteure von heute verschlüsseln nicht nur Daten. Sie zerstören die Datensicherung und schmuggeln Daten, um davon zu profitieren und gleichzeitig den Ruf der Marke zu schädigen. Das vergrößert den Explosionsradius der Ransomware. Lassen Sie die Ransomware-Angreifer nicht gewinnen. Verstärken Sie stattdessen Ihre Umgebung und verbessern Sie Ihre Reaktionsstrategie mit Funktionen zum Schutz, zur Erkennung und Wiederherstellung.

Die weltweiten Schadenskosten durch Ransomware, einschließlich Umsatz- und Produktivitätsverlusten, werden bis 2031 auf über 265 Milliarden US-Dollar geschätzt.[2]

1. Schutz Ihrer Backup-Daten und Ihres Systems

Legacy-Datensicherungen sind nicht für den Schutz von Daten vor Ransomware ausgelegt. Aus diesem Grund zahlen Unternehmen immer noch Lösegeld. Was wir brauchen, sind in die Datensicherung integrierte Sicherheitsvorkehrungen, die das Vertrauen der Kunden und den Wettbewerbsvorteil erhalten. Suchen Sie nach einer Lösung mit nativen, unveränderlichen Datensicherungs-Snapshots, da diese nicht verschlüsselt, geändert oder gelöscht werden können und die Authentizität Ihrer Daten schützen. Sie können den Schutz noch weiter erhöhen, indem Sie sicherstellen, dass Ihre Datensicherung über eine software-basierte WORM-Verschlüsselung (Write Once, Read Many) und eine FIPS-zertifizierte Verschlüsselung verfügt. Erfüllen Sie Ihre Wiederherstellungsziele und Unternehmens-SLAs mit moderner, flexibler Datenisolierung vor Ort und in Public Clouds. Und schließlich sollten Sie nach fehlertoleranten Lösungen suchen, die es Ihnen ermöglichen, trotz einer ausgefallenen Komponente weiterzuarbeiten und automatische Sicherheitskontrollen wie Auditing und Scanning zu konfigurieren, um menschliche Fehler auszuschließen.

2. Verringerung des Risikos eines unbefugten Zugriffs

Die Kompromittierung von Benutzeranmeldeinformationen ist zu einem der wichtigsten Angriffsvektoren für böswillige Akteure geworden, die auf der Suche nach Geld sind. Eine Datenmanagementplattform mit strengen Zugriffskontrollfunktionen verhindert effektiver, dass Unbefugte die Vorteile kompromittierter Anmeldedaten nutzen. Versuchen Sie, Hackern und internen Bedrohungen mit Zero-Trust-Prinzipien zu begegnen. Dazu gehören rollenbasierte Zugriffskontrollen, Multifaktor-Authentifizierung, Quorum-Genehmigung, um einseitige administrative Änderungen zu verhindern, und Überwachung mit automatischer Sicherheitsbewertung Ihrer Umgebung.

3. Stoppen von Eindringlingen und Erkennen von Angriffen

Nach Angaben der Experten von Cybersecurity Ventures wird heute alle 11 Sekunden ein Unternehmen Opfer eines Ransomware-Angriffs.[1] Kein Unternehmen hat genügend Mitarbeiter, um darauf zu reagieren. Daher benötigen Sie eine KI/ML-basierte Erkennung, um neue Angriffe und ungewöhnliche Aktivitäten zu erkennen und sensible Daten zu beleuchten. Suchen Sie nach einer Lösung mit integrierter Analytik, die es Ihrem Team ermöglicht, sensible Daten automatisch zu erkennen und zu klassifizieren und die Vorteile der Echtzeit-Bedrohungserkennung zu nutzen. Mithilfe der Basisinformationen der Lösung kann Ihr Team auf prädiktive Analysen gestützte Warnungen erhalten und frühzeitig Einblick in Anomalien bei laufenden Verschlüsselungs- und Datenexfiltrationsangriffen gewinnen.

4. Nahtlose Integration in bestehende Sicherheitssysteme

Die Ransomware-Bedrohung wird nicht verschwinden und entwickelt sich ständig weiter. Damit sind Ihre internen Teams – Infrastruktur und Betrieb (I & O), Sicherheitsbetrieb (SecOps) und Governance/Compliance – gefordert, besser zusammenzuarbeiten, um Verstöße zu verhindern und schnell darauf zu reagieren. Suchen Sie nach einer Datenmanagementlösung, die Ihnen hilft, Datensilos und funktionale Barrieren zu überwinden. Setzen Sie auf eine integrierte und erweiterbare Lösung, die Ihr Unternehmen in die Lage versetzt, Bedrohungen schneller zu erkennen, zu untersuchen und darauf zu reagieren. Die Lösung, für die Sie sich entscheiden, sollte es Ihnen ermöglichen, die Vorteile führender Sicherheitstools zu nutzen und Ihren Entwicklern eine Vielzahl von RESTful-APIs zur Verfügung zu stellen, damit sie weiterhin Mehrwert schaffen und gleichzeitig Bedrohungen abwehren können.

5. Schnelle Wiederherstellung Ihrer Daten im großen Maßstab

Da Cyber-Erpresser erfinderisch sind, ist der schlimmste Fall möglich. Deshalb brauchen Sie eine Datenmanagementlösung, die Ihnen eine schnelle Wiederherstellung ermöglicht, während Sie sich weigern, Lösegeld zu zahlen. Was wir brauchen, ist eine Lösung, die Hunderte von VMs, große Datenbanken und große Mengen unstrukturierter Daten sofort und in großem Umfang zu jedem beliebigen Zeitpunkt und an jedem beliebigen Ort wiederherstellt. Um sicherzugehen, dass Sie Ihre Umgebung nicht erneut mit Malware infizieren, sollten Sie sich eine Lösung suchen, die eine Snapshot-Zustandsbewertung bietet und es Ihnen ermöglicht, eine saubere und vorhersehbare Datenwiederherstellung direkt vor Ort auf derselben Plattform durchzuführen, wodurch Sie Ressourcen und Zeit sparen.

Stärken Sie Ihre Cyber-Resilienz mit Cohesity

Die Suche nach einer Lösung zur Bekämpfung von Ransomware wird zur geschäftlichen Notwendigkeit. Das Next-Gen Data Management bietet die Funktionen für Datensicherheit, Ransomware-Wiederherstellung und Cyber-Resilienz, die Ihr Unternehmen benötigt, um wettbewerbsfähig zu bleiben und die Zahlung von Lösegeld zu verweigern.

1. FortiGuard Labs Halbjahresbericht 2021 zur globalen Bedrohungslandschaft
2. Cybersecurity Ventures

Erfahren Sie mehr über Next-Gen Data Management unter Cohesity.com/de

COHESITY