FALLSTUDIE

IBM i File Integrity Monitoring mit FileScope

Asiatischer Versicherungsanbieter

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

Kundenprofil

Branche	Versicherungen
Region	Asien-Pazifik
Umgebung	IBM i — IBM i – 4 LPARs für Policenverwaltung, Schadenbearbeitung, Kundenmanagement, Finanzsysteme und regulatorisches Reporting
Sicherheitsziel	File Integrity Monitoring (FIM), Schutz sensibler Daten, Compliance-Monitoring und Erkennung von Änderungen
Assessment Type	Maßnahmen zur Reduzierung von Cyberrisiken und zur Erfüllung regulatorischer Compliance-Anforderungen

Die Herausforderung

Der Versicherungsanbieter setzt IBM i-Systeme für die Verarbeitung hochsensibler Kunden-, Versicherungs-, Schaden- und Finanzdaten ein. Mit zunehmenden regulatorischen Anforderungen und einer sich ständig wandelnden Bedrohungslage im Bereich der Cybersicherheit entstand der Bedarf nach einer besseren Transparenz bei Änderungen an kritischen Dateien, Verzeichnissen und sensiblen Datenbeständen.

Eingeschränkte Transparenz bei Datei- und Datenänderungen

Den Sicherheits- und Compliance-Teams fehlte eine zentrale Lösung zur Überwachung von Änderungen innerhalb kritischer IBM i-Dateisysteme. Zu den wesentlichen Herausforderungen gehörten:

- Unbefugte Änderungen an sensiblen Geschäftsdaten
- Schwierige Nachvollziehbarkeit, wer kritische Dateien wann geändert hat
- Eingeschränkte Transparenz beim Anlegen, Löschen, Umbenennen und Ändern von Dateien
- Erschwerte Erkennung verdächtiger oder unerwarteter Änderungen
- Längere Analysezeiten bei Sicherheitsvorfällen

Benötigt wurde eine Lösung zur kontinuierlichen Überwachung, die Änderungen auf Dateiebene zuverlässig erkennt und meldet, sobald geschäftskritische Informationen betroffen sind.

Steigende regulatorische und Compliance-Anforderungen

Aufsichtsbehörden und interne Revisionen forderten wirksamere Kontrollen zur Sicherstellung der Datenintegrität und einer lückenlosen Überwachung. Zu den Anforderungen zählen:

- Nachweis der Verantwortlichkeit für Änderungen an sensiblen Dateien
- Lückenlose Audit-Trails für geschäftskritische Informationen
- Erkennung unbefugter Zugriffe oder Änderungen
- Unterstützung interner Untersuchungen sowie Compliance-Prüfungen

- Verringerung des Risikos von Datenmanipulationen oder unbeabsichtigten Änderungen

Der Versicherer benötigte eine Lösung, die kritische Dateien kontinuierlich überwacht und bei unautorisierten Aktivitäten automatisch aussagekräftige Warnmeldungen erzeugt.

Implementierte Lösung

Raz-Lee implementierte die folgenden iSecurity-Module in der gesamten IBM i-Umgebung:

iSecurity FileScope

Implementierung einer kontinuierlichen File-Integrity-Monitoring-Lösung (FIM) für kritische IBM i-Dateien, Verzeichnisse und sensible Datenbestände. Zu den Funktionen gehören:

- Echtzeitüberwachung des Anlegens, Änderns, Löschens und Umbenennens von Dateien
- Erkennung unbefugter Änderungen an geschäftskritischen Dateien
- Lückenlose Zuordnung dateibezogener Aktivitäten zu einzelnen Benutzern
- Automatische Warnmeldungen bei verdächtigen oder unerwarteten Änderungen
- Zentrale Berichterstellung und Erstellung vollständiger Audit-Trails
- Überwachung sensibler Datenbereiche und geschäftskritischer Verzeichnisse
- Unterstützung regulatorischer und Compliance-bezogener Berichtspflichten

Durch die Implementierung erhielten die Sicherheitsteams einen unmittelbaren Überblick über sämtliche Änderungen an kritischen Informationsbeständen innerhalb der IBM i-Umgebung.

Ergebnisse

- Deutlich bessere Transparenz hinsichtlich der Integrität von Dateien und Daten in geschäftskritischen Versicherungssystemen
- Schnellere Erkennung unbefugter oder verdächtiger Dateiänderungen
- Verbesserter Schutz von Versicherungs-, Kunden- und Schadendaten
- Höhere Audit-Bereitschaft und verbesserte Compliance-Berichterstattung
- Verkürzte Untersuchungszeiten bei Sicherheitsvorfällen und Compliance-Prüfungen
- Höhere Nachvollziehbarkeit dateibezogener Aktivitäten
- Verbesserte Überwachung sensibler Geschäftsinformationen
- Implementierung ohne Beeinträchtigung des laufenden Versicherungsbetriebs

Der Versicherer konnte den Schutz seiner geschäftskritischen Informationsbestände erheblich verbessern und gleichzeitig seine Compliance sowie die operativen Sicherheitsmaßnahmen nachhaltig stärken.

Feedback des QSA

"Der Schutz der Integrität unserer Versicherungs- und Schadendaten ist eine grundlegende Voraussetzung für unser Geschäft. FileScope verschafft uns die Transparenz und Kontrolle, die wir benötigen, um unbefugte Änderungen sofort zu erkennen, regulatorische Anforderungen zuverlässig zu erfüllen und das Vertrauen in die Integrität unserer IBM i-Umgebung nachhaltig zu stärken."

— Information Security Manager (sinngemäß wiedergegeben)