FALLSTUDIE

IBM i Compliance Automation & Security Governance

Europäisches Großhandelsunternehmen (anonymisiert)

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

Kundenprofil

Branche	Großhandel und Distribution
Region	Europa
Umgebung	IBM i — 5 LPARs für ERP, Lagerverwaltung, Beschaffung, Logistik, Finanzwesen und Kundenprozesse
Sicherheitsziel	Compliance Management, Kontrolle von Sicherheitskonfigurationen, Risikobewertung und Audit Readiness
Assessment Type	Maßnahmen zur regulatorischen Compliance und internen Security Governance

Ausgangssituation

Das Unternehmen nutzt IBM i als zentrale Plattform für die Verwaltung von Lagerbeständen, Lieferkettenprozessen, Kundenaufträgen und Finanztransaktionen. Mit der Expansion in mehrere europäische Märkte wurde es zunehmend anspruchsvoller, regulatorische Anforderungen sowie interne Sicherheitsrichtlinien konsistent umzusetzen und nachzuweisen.

Komplexe Compliance-Anforderungen

Das Unternehmen muss die Einhaltung verschiedener interner Richtlinien sowie externer regulatorischer Vorgaben nachweisen. Dabei bestehen folgende Herausforderungen:

- Schwierige Überprüfung von IBM i-Sicherheitskonfigurationen anhand unternehmensweiter Standards
- Zeitaufwändige manuelle Compliance-Bewertungen
- Begrenzte Transparenz hinsichtlich Sicherheitsrisiken und Konfigurationslücken
- Uneinheitliche Compliance-Berichte über mehrere IBM i-Umgebungen hinweg
- Hoher Aufwand bei der Vorbereitung von Audits

Die IT- und Compliance-Teams benötigten einen stärker automatisierten Ansatz zur Bewertung und Aufrechterhaltung der Compliance.

Fehlende kontinuierliche Security Governance

Die Sicherheitsadministratoren benötigten eine bessere Kontrolle über kritische Systemeinstellungen, um die dauerhafte Einhaltung von Richtlinien sicherzustellen. Zu den zentralen Herausforderungen gehörten:

- Unautorisierte Änderungen sicherheitsrelevanter Systemeinstellungen
- Abweichungen von Konfigurationen zwischen einzelnen IBM i-Partitionen
- Erschwerte Nachverfolgung von Korrektur- und Verbesserungsmaßnahmen
- Begrenzte Möglichkeiten zum Nachweis kontinuierlicher Compliance
- Erhöhtes Risiko von Audit-Feststellungen und Sicherheitslücken

Gesucht wurde eine zentrale Lösung zur kontinuierlichen Überwachung, Bewertung und Steuerung von Compliance-Anforderungen innerhalb der IBM i-Landschaft.

Implementierte Lösungen

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

iSecurity Compliance Evaluator

Automatisierte Bewertung und Überprüfung der Compliance auf IBM i.

iSecurity Compliance Manager

Zentrale Verwaltung von Compliance-Anforderungen sowie Nachverfolgung von Korrekturmaßnahmen.

iSecurity System Control

Kontinuierliche Überwachung und Kontrolle kritischer IBM i-Sicherheitseinstellungen.

Gemeinsam bilden diese Lösungen ein umfassendes Framework zur Sicherstellung von Compliance und zur Stärkung der Security Governance innerhalb der gesamten IBM i-Umgebung. Wesentliche Funktionen:

- Kontinuierliche Compliance-Überwachung
- Detaillierte Compliance-Bewertungen und Berichterstattung
- Beschleunigte Audit-Vorbereitung
- Überwachung sicherheitskritischer Systemwerte
- Erkennung von Konfigurationsabweichungen
- Identifikation von Richtlinienverstößen
- Verbesserte Governance von IBM i-Sicherheitskontrollen

Ergebnisse

- Deutlich reduzierter Aufwand für Compliance-Bewertungen und Audit-Vorbereitungen
- Verbesserte Transparenz über den Sicherheitsstatus aller IBM i-LPARs
- Schnellere Identifikation und Behebung von Compliance-Lücken
- Stärkere Kontrolle und Governance sicherheitsrelevanter Systemkonfigurationen
- Höhere Konsistenz von Sicherheitsrichtlinien und Kontrollen in der gesamten Umgebung
- Verbesserte Reporting-Möglichkeiten für Auditoren und Management
- Reduzierter operativer Aufwand im Compliance Management
- Implementierung ohne Beeinträchtigung von Lager-, Logistik- oder ERP-Prozessen

Das Unternehmen konnte seine Fähigkeit zur Einhaltung regulatorischer Anforderungen deutlich verbessern, Sicherheitsrichtlinien konsequenter durchsetzen und eine kontinuierliche Governance innerhalb seiner IBM i-Infrastruktur etablieren.

Kundenfeedback

„Die Einhaltung von Compliance-Anforderungen über mehrere IBM i-Systeme hinweg wurde zunehmend ressourcenintensiv. Compliance Evaluator, System Control und Compliance Manager verschafften uns die notwendige Transparenz, Automatisierung und Governance, um unseren Sicherheitsstatus kontinuierlich zu bewerten und die Vorbereitung auf Audits erheblich zu vereinfachen.“
— Director IT Governance & Compliance (sinngemäß wiedergegeben)