FALLSTUDIE

IBM i Command Protection & Administrative Control

Lateinamerikanische Versicherungsgruppe

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

Kundenprofil

Branche	Versicherungsgruppe in Lateinamerika
Region	Lateinamerika
Umgebung	IBM i — 4 LPARs für Policenverwaltung, Schadenbearbeitung, Kundenmanagement, Finanzprozesse und regulatorisches Reporting
Sicherheitsziel	Command Protection, Kontrolle privilegierter Zugriffe, administrative Sicherheit und Compliance-Monitoring
Assessment Type	Maßnahmen zur Härtung der Systemsicherheit und Reduzierung von Risiken durch privilegierte Benutzer

Die Herausforderung

Die Versicherungsgruppe nutzt IBM i zur Unterstützung geschäftskritischer Prozesse rund um Versicherungsdaten, Schadensbearbeitung, Finanztransaktionen und regulatorisches Reporting. Mit der steigenden Zahl von Administratoren, Operatoren und externen Support-Mitarbeitern erkannte das Unternehmen zunehmende Risiken durch einen uneingeschränkten Zugriff auf die Kommandozeile.

Übermäßig privilegierte Zugriffsrechte

Benutzer mit erweiterten Berechtigungen konnten leistungsstarke IBM i-Befehle ausführen, mit denen sich Systemkonfigurationen ändern, vertrauliche Daten aufrufen und geschäftskritische Abläufe beeinflussen lassen. Zu den wesentlichen Risiken gehörten:

- Unbefugte Ausführung sicherheitskritischer Befehle
- Übermäßige Berechtigungen für operative Mitarbeiter
- Risiko unbeabsichtigter Systemänderungen
- Möglicher Missbrauch administrativer Berechtigungen
- Eingeschränkte Kontrolle über leistungsstarke native IBM i-Befehle

Gesucht wurde eine Lösung, die eine deutlich strengere Kontrolle der Befehlsausführung ermöglicht, ohne die Produktivität autorisierter Administratoren einzuschränken.

Compliance- und Audit-Anforderungen

Interne Revisoren und regulatorische Prüfer forderten stärkere Kontrollen für Aktivitäten privilegierter Benutzer. Zu den Herausforderungen zählten:

- Nachweis einer wirksamen Kontrolle administrativer Funktionen
- Reduzierung der Risiken durch privilegierte Benutzer
- Durchsetzung der Funktionstrennung (Separation of Duties)
- Einschränkung des Zugriffs auf kritische Systemfunktionen
- Verbesserte Nachvollziehbarkeit und Verantwortlichkeit bei der Ausführung von Systembefehlen

Das Unternehmen suchte nach einer Lösung, mit der sich die Nutzung von IBM i-Befehlen zentral steuern, einschränken und überwachen lässt.

Implementierte Lösung

Raz-Lee implementierte das folgende iSecurity-Modul in der gesamten IBM i-Umgebung:

iSecurity Command

Bereitstellung einer leistungsfähigen Lösung für Command Protection und administrative Zugriffskontrolle auf IBM i. Zu den Funktionen gehören:

- Einschränkung des Zugriffs auf sicherheitskritische IBM i-Befehle
- Benutzer- und gruppenbasierte Richtlinien für die Befehlsautorisierung
- Verhinderung der Ausführung nicht autorisierter Befehle
- Granulare Steuerung administrativer Aktivitäten
- Durchsetzung der Funktionstrennung (Separation of Duties)
- Zentrale Verwaltung von Berechtigungen für Systembefehle
- Detaillierte Protokollierung aller Zugriffsversuche auf geschützte Befehle

Durch die Implementierung konnte das Unternehmen seine betriebliche Flexibilität erhalten und gleichzeitig die Risiken privilegierter Zugriffe deutlich reduzieren.

Ergebnisse

- Deutlich geringeres Risiko unautorisierter administrativer Aktivitäten
- Verbesserte Kontrolle über leistungsstarke IBM i-Systembefehle
- Stärkere Umsetzung der Funktionstrennung innerhalb des IT-Betriebs
- Reduziertes Risiko unbeabsichtigter oder vorsätzlicher Systemänderungen
- Verbesserte Erfüllung interner Governance- und Compliance-Anforderungen
- Höhere Nachvollziehbarkeit privilegierter Benutzeraktivitäten
- Größere Transparenz bei der Ausführung von Systembefehlen
- Erfolgreiche Implementierung ohne Beeinträchtigung des Versicherungsbetriebs

Das Unternehmen konnte die Kontrolle über administrative Zugriffe deutlich verbessern und gleichzeitig seine Security Governance in der gesamten IBM i-Umgebung nachhaltig stärken.

Feedback des QSA

"Administrative Berechtigungen sind für den Betrieb unserer IBM i-Systeme unverzichtbar. Ein uneingeschränkter Zugriff auf Systembefehle stellt jedoch ein unnötiges Sicherheitsrisiko dar. Mit iSecurity Command konnten wir präzise Kontrollen für sicherheitskritische Befehle umsetzen, unsere Compliance-Anforderungen besser erfüllen und das Risiko durch privilegierte Benutzer erheblich reduzieren – ohne die betriebliche Effizienz zu beeinträchtigen."

— IT Security Manager (sinngemäß wiedergegeben)