FALLSTUDIE

IBM i-Berechtigungen: Authority Inspector und Authority on Demand bei einer internationalen Bankengruppe

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

RAZ-LEE

Kundenprofil

Branche	Banken- und Finanzdienstleistungen
Region	Europa
Umgebung	IBM i — 8 LPARs für Kernbankensysteme, Zahlungsverkehr, Treasury-Operationen, Kundenkontenverwaltung, SWIFT-Anbindung und regulatorisches Reporting
Sicherheitsziel	Verwaltung privilegierter Zugriffe (PAM), Berechtigungskontrolle, Funktionstrennung (Segregation of Duties) und Compliance-Monitoring
Assessment Type	Projekt zur Stärkung der regulatorischen Compliance und der internen Security Governance

Die Herausforderung

Die Bankengruppe betreibt in mehreren Ländern eine komplexe IBM-i-Umgebung zur Unterstützung geschäftskritischer Finanzdienstleistungen. Regulatorische Anforderungen und interne Sicherheitsrichtlinien erforderten eine strenge Kontrolle privilegierter Zugriffe, während Administratoren gleichzeitig in der Lage sein mussten, notwendige betriebliche Aufgaben effizient auszuführen.

Zu weitreichende Benutzerberechtigungen

Im Laufe der Zeit hatten viele Benutzer Berechtigungen angesammelt, die ihre tatsächlichen täglichen Aufgaben deutlich überstiegen. Die Folge:

- Übermäßiger Zugriff auf sensible Bankanwendungen und Daten
- Schwierigkeit bei der Identifizierung von Benutzern mit erweiterten Berechtigungen
- Erhöhtes Risiko durch Insider-Bedrohungen und unautorisierte Aktivitäten
- Herausforderungen bei der Durchsetzung des Least-Privilege-Prinzips
- Eingeschränkte Transparenz hinsichtlich vererbter Berechtigungen und Sonderberechtigungen (Special Authorities)

Das Unternehmen benötigte eine umfassende Überprüfung der Benutzerrechte sowie eine sichere Strategie zur Reduzierung unnötiger Berechtigungen.

Permanente Administratorrechte

Administratoren und Support-Mitarbeiter verfügten dauerhaft über hoch privilegierte Zugriffsrechte, was sowohl Compliance- als auch Sicherheitsrisiken verursachte. Zu den Herausforderungen gehörten:

- Permanenter privilegierter Zugriff erhöht die Risikobelastung
- Schwierigkeiten bei der Durchsetzung zeitlich begrenzter Administrationsrechte
- Begrenzte Nachvollziehbarkeit der Nutzung erhöhter Berechtigungen
- Zunehmende Prüfungsanforderungen hinsichtlich privilegierter Konten
- Bedarf an stärkeren Kontrollen zur Funktionstrennung (Segregation of Duties)

Die Bank suchte nach einer Lösung, mit der permanente Privilegien reduziert werden konnten, ohne die Effizienz der IT-Teams zu beeinträchtigen.

Implementierte Lösung

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

iSecurity Authority Inspector

Zur Analyse von Berechtigungen und zur Bewertung von Zugriffsrechten wurde eine erweiterte Lösung zur Berechtigungsanalyse eingeführt. Zu ihren Funktionen gehören:

- Identifizierung übermäßiger und vererbter Berechtigungen
- Analyse von Benutzer-, Gruppen- und Objektberechtigungen
- Erkennung potenzieller Privilegien-Eskalationen
- Mehr Transparenz bei Sonderberechtigungen und Sicherheitsrisiken
- Unterstützung bei der Umsetzung von Least-Privilege-Initiativen
- Detaillierte Berichte für Auditoren und Compliance-Teams

Die Lösung ermöglicht es der Organisation, unnötige Berechtigungen innerhalb der gesamten IBM-i-Umgebung zu identifizieren und gezielt zu beseitigen.

iSecurity Authority on Demand

Zur kontrollierten und zeitlich begrenzten Vergabe erhöhter Berechtigungen wurde Authority on Demand implementiert. Zu den Funktionen gehören:

- Automatischer Entzug erhöhter Berechtigungen nach Ablauf einer definierten Zeitspanne
- Genehmigungsbasierte Workflows für die Vergabe zusätzlicher Rechte
- Detaillierte Protokollierung von Berechtigungsanfragen und deren Nutzung

Die Implementierung gewährleistet, dass erhöhte Zugriffsrechte ausschließlich für die Dauer der autorisierten Tätigkeit vergeben werden und nur dann, wenn sie tatsächlich benötigt werden.

Ergebnisse

- Reduzierung übermäßiger Berechtigungen auf den IBM-i-Systemen
- Konsequente Durchsetzung des Least-Privilege-Prinzips
- Beseitigung unnötiger permanenter Administratorrechte
- Verbesserte Funktionstrennung und Governance von Zugriffsrechten
- Höhere Transparenz bei Aktivitäten privilegierter Benutzer
- Verbesserte Einhaltung regulatorischer Anforderungen und Audit-Vorgaben im Bankensektor
- Reduziertes Risiko durch Insider-Bedrohungen und Missbrauch privilegierter Konten
- Implementierung ohne Beeinträchtigung des laufenden Bankbetriebs
- Deutliche Verbesserung des Privileged-Access-Managements bei gleichzeitiger Reduzierung von Sicherheitsrisiken und Stärkung der regulatorischen Compliance innerhalb der gesamten IBM-i-Umgebung

Zentrale Rückmeldung des QSA*

„Die Verwaltung privilegierter Zugriffe in einer Bankenumgebung erfordert die richtige Balance zwischen betrieblicher Effizienz und strengen Sicherheitskontrollen. Authority Inspector verschafft uns die notwendige Transparenz, um übermäßige Berechtigungen zu identifizieren, während Authority on Demand es uns ermöglicht, permanente Administratorrechte abzuschaffen und ein echtes Least-Privilege-Modell

umzusetzen. Das Ergebnis sind eine deutlich höhere Sicherheit und ein wesentlich reibungsloserer Audit-Prozess.“
Chief Information Security Officer (sinngemäß wiedergegeben);

*QSA = Qualified Security Assessor (zertifizierter PCI-DSS-Prüfer)