

# FALLSTUDIE

IBM i Datenverschlüsselung & sicherer Dateischutz bei einem lateinamerikanischen Bankinstitut

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)



## Kundenprofil

|                        |                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Branche</b>         | Lateinamerikanisches Bankinstitut                                                                                               |
| <b>Region</b>          | Lateinamerika                                                                                                                   |
| <b>Umgebung</b>        | IBM i — 3 LPARs für Kernbankensysteme, Kundenkonten-Verwaltung, Zahlungsverkehr, Kreditverwaltung und regulatorisches Reporting |
| <b>Sicherheitsziel</b> | Datenverschlüsselung, Schutz sensibler Informationen, sicherer Dateitransfer und regulatorische Compliance                      |
| <b>Assessment Type</b> | Maßnahmen zur Verbesserung von Datenschutz und regulatorischer Compliance                                                       |

## Die Herausforderung

Die Bank verarbeitet und speichert große Mengen sensibler Kunden- und Finanzdaten innerhalb ihrer IBM-i-Umgebung. Zunehmende Cyberbedrohungen, Datenschutzvorschriften und regulatorische Anforderungen im Bankensektor machen stärkere Sicherheitsmaßnahmen erforderlich, um Daten sowohl im Ruhezustand (at rest) als auch während der Übertragung (in transit) zu schützen.

## Schutz sensibler Finanzdaten

Kritische Bankanwendungen enthalten vertrauliche Informationen wie Kundendaten, Kontoinformationen, Transaktionsdaten sowie personenbezogene Daten (PII – Personally Identifiable Information). Daher gehören zu den wesentlichen Herausforderungen:

- Gefährdung sensibler Kundendaten durch unbefugten Zugriff
- Schutz von Finanz- und Personendaten, die in IBM-i-Datenbanken gespeichert sind
- Einhaltung regulatorischer Anforderungen im Bankwesen sowie von Datenschutzvorschriften
- Risiken durch Insider-Bedrohungen und übermäßige Benutzerberechtigungen
- Zunehmende Konzentration von Auditoren auf Verschlüsselungskontrollen

Die Bank benötigte eine robuste Verschlüsselungsstrategie, die implementiert werden konnte, ohne bestehende Bankanwendungen zu beeinträchtigen.

## Absicherung von Dateiübertragungen und externer Kommunikation

Das Unternehmen tauscht regelmäßig Dateien mit sensiblen Finanzinformationen aus mit:

- Aufsichts- und Regulierungsbehörden
- Zahlungsdienstleistern und Zahlungsabwicklern
- Geschäftspartnern
- Clearing- und Settlement-Dienstleistern
- Internen regionalen Niederlassungen

Die bestehenden Dateiübertragungsprozesse verfügten nicht durchgängig über Verschlüsselungskontrollen, was Bedenken hinsichtlich Vertraulichkeit und regulatorischer Compliance aufwarf. Die Bank benötigte eine sichere Methode zur Verschlüsselung und zum Austausch von Dateien, ohne die betriebliche Effizienz einzuschränken.

## **Implementierte Lösung**

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

### **iSecurity Field Encryption**

Zur Absicherung sensibler Informationen innerhalb von IBM i wurde eine Verschlüsselung auf Feldebene (Field-Level Encryption) eingeführt, einschließlich:

- Verschlüsselung sensibler Kunden- und Finanzdaten
- Schutz personenbezogener Daten (PII)
- Granulare Kontrolle über verschlüsselte Datenbankfelder
- Sichere Schlüsselverwaltung
- Transparente Integration in bestehende Geschäftsanwendungen
- Reduzierung der Offenlegung vertraulicher Informationen

Die Lösung ermöglicht es dem Unternehmen, kritische Daten abzusichern, ohne umfangreiche Anpassungen an den Anwendungen vornehmen zu müssen.

### **iSecurity Encryption Open PGP**

Zur sicheren Dateiverschlüsselung und zum geschützten Datenaustausch mit externen Stellen wurde Open-PGP-Verschlüsselung implementiert, einschließlich:

- Automatisierter Ver- und Entschlüsselung von Dateien
- Schutz sensibler Informationen während der Übertragung
- Unterstützung sicherer Dateiübertragungen mit externen Partnern
- Einhaltung von Datenschutz- und Bankenanforderungen

Die Implementierung stellte sicher, dass sensible Dateien während des gesamten Übertragungsprozesses geschützt blieben.

## **Ergebnisse**

- Deutlich verbesserter Schutz sensibler Kunden- und Finanzinformationen
- Reduziertes Risiko eines unbefugten Zugriffs auf vertrauliche Daten
- Verbesserte Einhaltung regulatorischer Anforderungen im Bankwesen und von Datenschutzvorgaben
- Sichere Dateiübertragungen mit Aufsichtsbehörden, Partnern und Drittanbietern
- Verbesserter Schutz personenbezogener Daten (PII)
- Vereinfachte Verwaltung von Verschlüsselungsprozessen innerhalb der IBM-i-Umgebung
- Höheres Vertrauen von Auditoren in die implementierten Datenschutz- und Sicherheitskontrollen
- Implementierung ohne Beeinträchtigung des Bankbetriebs oder der Kundendienstleistungen.

Das Unternehmen hat seine Fähigkeit zum Schutz sensibler Informationen erheblich verbessert und erfüllt nun gleichzeitig regulatorische und Compliance-Anforderungen innerhalb seiner gesamten IBM-i-Infrastruktur.

## **Zentrale Rückmeldung des QSA\***

*„Datenschutz ist eine zentrale Anforderung im Bankensektor. Mit Encryption Field konnten wir sensible Kunden- und Finanzdaten direkt in unseren IBM-i-Datenbanken absichern, während Open PGP sicherstellte, dass Dateien im Austausch mit externen Unternehmen jederzeit geschützt blieben. Gemeinsam haben diese Lösungen unsere gesamte Datensicherheitsstrategie deutlich gestärkt.“*

— Chief Information Security Officer (sinngemäß wiedergegeben)

---

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