# FALLSTUDIE

IBM i Session Monitoring und Aufzeichnung von Benutzeraktivitäten

Finanzdienstleistungsunternehmen in Asien

*(Die Fallstudie wurde auf Kundenwunsch anonymisiert)*

## Kundenprofil

| | |
|---|---|
| **Branche** | Branche Finanzdienstleistungen |
| **Region** | Asien-Pazifik |
| **Umgebung** | IBM i — 5 LPARs für Kundenservices, Transaktionsverarbeitung, Finanzoperationen und regulatorisches Reporting |
| **Sicherheitsziel** | Überwachung der Benutzeraktivität, Session Recording, Erkennung von Insider-Bedrohungen und Compliance-Unterstützung |
| **Assessment Type** | Maßnahmen zur Sicherheitsüberwachung und Verbesserung der operativen Transparenz |

## Ausgangssituation

Das Unternehmen verarbeitet innerhalb seiner IBM i-Umgebung hochsensible Finanz- und Kundendaten. Mit der zunehmenden Professionalisierung von Cyberbedrohungen und steigenden regulatorischen Anforderungen wächst der Bedarf nach einer besseren Transparenz über Benutzeraktivitäten auf geschäftskritischen Systemen.

### Eingeschränkte Transparenz bei Benutzeraktivitäten

Zwar waren Benutzeranmeldung und Audit-Protokollierung bereits vorhanden, den Sicherheitsteams fehlte jedoch häufig der notwendige Kontext, um nachvollziehen zu können, welche konkreten Aktionen Anwender während einer IBM i-Sitzung durchgeführt hatten.

Dies führte zu folgenden Herausforderungen:

- Erschwerte Untersuchung verdächtiger Benutzeraktivitäten
- Begrenzte Transparenz bei privilegierten Benutzerkonten
- Zeitaufwändige forensische Analysen
- Eingeschränkte Möglichkeiten zur Rekonstruktion von Benutzersitzungen
- Erhöhte Schwierigkeiten bei der Erkennung von Insider-Bedrohungen

Die Sicherheitsverantwortlichen benötigten eine effizientere Lösung zur Überwachung und Analyse von Benutzeraktivitäten innerhalb geschäftskritischer IBM i-Anwendungen.

### Regulatorische- und Governance-Anforderungen

Interne Revisionen und Compliance-Teams forderten stärkere Kontroll- und Überwachungs-mechanismen für sensible Systeme und privilegierte Benutzerkonten.

Besondere Anforderungen waren:

- Nachweis einer wirksamen Kontrolle privilegierter Benutzer
- Unterstützung interner Untersuchungen

- Höhere Nachvollziehbarkeit sensibler Aktivitäten
- Lückenlose Dokumentation von Benutzeraktionen
- Verbesserung der Compliance mit regulatorischen Anforderungen im Finanzsektor

Gesucht wurde eine Lösung, die Benutzeraktivitäten aufzeichnen, wiedergeben und umfassend überwachen kann.

## Implementierte Lösung

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

### iSecurity Capture

Mit iSecurity Capture wurde eine umfassende Lösung zur Überwachung und Aufzeichnung von Benutzersitzungen eingeführt.

Funktionen:

- Aufzeichnung von Benutzersitzungen und Aktivitäten
- Überwachung privilegierter und besonders risikobehafteter Benutzerkonten
- Detaillierte Wiedergabe von Benutzeraktionen für Untersuchungen
- Verbesserte Transparenz operativer Abläufe
- Unterstützung forensischer Analysen und Incident-Response-Prozesse
- Zentrale Auswertung und Analyse von Benutzerverhalten
- Erweiterte Überwachung sensibler Geschäftsprozesse

Durch die Implementierung erhielten Sicherheits- und Compliance-Teams einen umfassenden Einblick in die Aktivitäten innerhalb der IBM i-Umgebung.

## Ergebnisse

- Verbesserte Transparenz der Aktivitäten von Benutzern und Administratoren
- Schnellere Sicherheitsuntersuchungen und Reaktion auf Vorfälle
- Erweiterte Überwachung privilegierter Benutzerkonten
- Deutlich verbesserte Erkennung potenzieller Insider-Bedrohungen
- Höhere Audit-Bereitschaft und bessere Unterstützung von Compliance-Anforderungen
- Verbesserte Nachvollziehbarkeit von Verantwortlichkeiten in kritischen Geschäftsprozessen
- Reduzierter Aufwand bei der Rekonstruktion sicherheitsrelevanter Ereignisse
- Implementierung ohne Beeinträchtigung des laufenden Produktivbetriebs

Das Unternehmen konnte seine Fähigkeiten zur Überwachung, Analyse und Nachvollziehbarkeit von Benutzeraktivitäten erheblich verbessern und gleichzeitig die Sicherheits- und Governance-Strukturen innerhalb seiner IBM i-Infrastruktur nachhaltig stärken.

## Kundenfeedback

*„Herkömmliche Protokolle zeigen uns, was passiert ist – aber nicht immer, wie es passiert ist. Mit Capture können wir Benutzeraktivitäten im Kontext nachvollziehen und bei Bedarf vollständig wiedergeben. Dadurch haben sich Untersuchungen, Compliance-Prüfungen und die Kontrolle privilegierter Benutzer deutlich verbessert. Die Lösung ist heute ein zentraler Bestandteil unserer IBM i-Überwachungsstrategie.“*

— Leiter Cybersecurity Operations (sinngemäß wiedergegeben)