FALLSTUDIE

IBM i-EDR-Transparenz & Reaktion auf Sicherheitsbedrohungen
Europäisches Bankinstitut

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

Kundenprofil

Branche	Bankenwesen
Region	Europa
Umgebung	IBM i — 4 LPARs für Kernbankensysteme, Transaktionsverarbeitung und Kundendienstleistungen
Sicherheitsziel	Endpoint Detection & Response (EDR), Transparenz für IBM i
Assessment Type	Maßnahmen zur Modernisierung der Cybersicherheit und Integration in Security Operations

Die Herausforderung

Das Security Operations Center (SOC) des Kunden verfügte bereits über eine unternehmensweite EDR-Abdeckung für Windows-, Linux- und Cloud-Infrastrukturen. Die IBM-i-Umgebung stellte jedoch eine erhebliche Transparenzlücke innerhalb des Cybersecurity-Monitorings dar. Da auf den IBM-i-Systemen geschäftskritische Bankanwendungen und sensible Finanzdaten gehostet werden, führte das Fehlen IBM-i-spezifischer Überwachungs- und Reaktionsmöglichkeiten zu operativen sowie regulatorischen Risiken.

Fehlende Transparenz in der Sicherheitsüberwachung

Die im Unternehmen eingesetzten klassischen EDR-Plattformen konnten keine ausreichende Transparenz für IBM i bereitstellen. Insbesondere fehlten:

- Echtzeitüberwachung von Benutzeraktivitäten auf IBM i
- Erkennung verdächtiger Befehlsausführungen
- Transparenz über privilegierte Aktivitäten
- Nachverfolgung unautorisierter Zugriffsversuche
- Korrelation von IBM-i-Ereignissen innerhalb der zentralen SOC-Umgebung

Dem SOC fehlten damit die für moderne Bedrohungserkennung erforderlichen IBM-i-spezifischen Telemetriedaten.

Erkennung von- und Reaktion auf Bedrohungen

Das Unternehmen benötigte die Möglichkeit,

- ungewöhnliche oder unautorisierte Aktivitäten auf IBM i in Echtzeit zu erkennen,
- Versuche zur Privilegien-Eskalation zu identifizieren,
- Änderungen an sensiblen Objekten und Systemkonfigurationen zu überwachen,
- automatische Warnmeldungen und Reaktionen auszulösen,
- IBM-i-Sicherheitsereignisse in bestehende SIEM-Prozesse des Unternehmens zu integrieren.

Ohne IBM-i-spezifische Sicherheitsinformationen konnte das Security-Team keine durchgängige Erkennungs- und Reaktionsstrategie für die gesamte IT-Landschaft umsetzen.

Compliance- und Betriebsanforderungen

Die Lösung musste:

- nativ auf IBM i betrieben werden und keine Änderungen an bestehenden Anwendungen erfordern,
- in die zentrale SIEM-Plattform der Bank integriert werden können,
- eine schnelle Implementierung über mehrere LPARs hinweg unterstützen,
- die Auswirkungen auf produktive Bankensysteme auf ein Minimum beschränken.

Implementierte Lösung

Raz-Lee implementierte die folgenden iSecurity-Module auf allen IBM-i-Partitionen:

iSecurity Audit

Zur zentralen Echtzeitüberwachung und Protokollierung von IBM-i-Sicherheitsereignissen wurde iSecurity Audit eingeführt. Zu seinen Funktionen gehören:

- Überwachung von Benutzeranmeldungen und Authentifizierungs-Aktivitäten
- Nachverfolgung von Befehlsausführungen und privilegierten Operationen
- Überwachung von Datei- und Objektzugriffen
- Erkennung von Verstößen gegen Sicherheitsrichtlinien
- Echtzeitwarnungen bei verdächtigen oder unautorisierten Aktivitäten

Diese Lösung stellt die für SOC- und Sicherheitsteams erforderliche Transparenz über sämtliche IBM-i-Aktivitäten bereit.

iSecurity Action

Zur automatisierten Reaktion auf Sicherheitsvorfälle und zur Durchsetzung von Sicherheitsrichtlinien wurde iSecurity Action implementiert. Dadurch konnte das Unternehmen aktive Abwehr- und Reaktionsmechanismen bei Bedrohungen innerhalb der IBM-i-Umgebung etablieren.

iSecurity SIEM

Mit iSecurity SIEM wurden IBM-i-Sicherheitsereignisse in die zentrale SIEM-Plattform der Bank integriert. Die Implementierung ermöglicht es, IBM i vollständig in die unternehmensweiten Cybersecurity- und Security-Operations-Prozesse einzubinden.

Ergebnisse

- Erreichen einer unternehmensweiten EDR-Transparenz für IBM-i-Umgebungen
- Integration von IBM-i-Ereignissen in die zentrale SOC-Überwachung und SIEM-Korrelation
- Verbesserte Erkennung verdächtiger Benutzeraktivitäten und privilegierter Aktionen
- Verkürzte Reaktionszeiten auf Sicherheitsvorfälle durch automatisierte Warnmeldungen und Gegenmaßnahmen
- Beseitigung der bisherigen Transparenzlücken von IBM i innerhalb der Security Operations
- Implementierung ohne Änderungen an Anwendungen oder Beeinträchtigung produktiver Systeme

Das Unternehmen konte seine Überwachungs- und Reaktionsfähigkeiten für IBM i erheblich stärken und seine IBM-i-Systeme in Einklang mit den unternehmensweiten Cybersecurity-Standards bringen.

Zentrale Rückmeldung des QSA

„Über viele Jahre hinweg befand sich IBM i außerhalb des Sichtfelds unserer unternehmensweiten EDR- und SOC-Prozesse. Mit Raz-Lee konnten wir IBM i vollständig in unsere zentrale Strategie für Bedrohungserkennung und Incident Response integrieren – einschließlich Echtzeitüberwachung, aussagekräftigen Warnmeldungen und SIEM-Korrelation.“

Leiter Cybersecurity Operations (sinngemäß wiedergegeben)