FALLSTUDIE

IBM i Network Access Control & Segmentation

Asiatisches Bankinstitut

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

Kundenprofil

Branche	Bankenwesen
Region	Asien
Umgebung	IBM i – 5 LPARs für Digital Banking, Zahlungssysteme und Finanzanwendungen
Sicherheitsziel	Netzwerkzugriffskontrolle und Netzwerksegmentierung für IBM i
Assessment Type	Maßnahmen zur Härtung der Systemsicherheit und Erfüllung regulatorischer Compliance-Anforderungen

Die Herausforderung

Die IBM i-Infrastruktur der Bank unterstütze geschäftskritische Bankprozesse und verarbeitee hochsensible Finanzdaten, auf die interne Benutzer, externe Anwendungen, Dienstleister und Partnersysteme zugreifen. Mit steigenden Anforderungen an Cybersicherheit und Compliance wurde deutlich, dass der Netzwerkzugriff auf IBM i-Dienste wesentlich granularer kontrolliert werden muss.

Fehlende granulare Netzwerkzugriffskontrolle für IBM i

Die Bank verfügte bislang nicht über die Möglichkeit,

- den Netzwerkzugriff anhand von Benutzerprofilen einzuschränken,
- Verbindungen auf Basis von IP-Adressen oder Subnetzen zu steuern,
- den Zugriff auf einzelne IBM i-Dienste und Netzwerkports gezielt zu begrenzen,
- produktive und administrative Zugriffswege voneinander zu trennen,
- temporäre oder Notfall-Zugriffsregeln kurzfristig bereitzustellen.

Dadurch konnte grundsätzlich jeder autorisierte Netzwerkbenutzer Verbindungen zu IBM i-Diensten wie FTP, ODBC, DRDA, DDM, Remote Command, Telnet oder nativen IBM i-Schnittstellen aufbauen.

Hohe Dynamik im operativen Betrieb

Die IT-Landschaft der Bank unterlag kontinuierlichen Veränderungen, unter anderem durch:

- neue Dienstleister und FinTech-Integrationen,
- temporäre Zugriffe im Rahmen von Projekten,
- Anforderungen an die Remote-Administration,
- regulatorische Vorgaben zur Netzwerksegmentierung.

Das IT-Sicherheitsteam benötigte daher eine Lösung, mit der sich Sicherheitsrichtlinien schnell erstellen und umsetzen lassen – ohne betriebliche Verzögerungen oder aufwendige Änderungen an der Netzwerkinfrastruktur.

Compliance- und Sicherheitsanforderungen

Die gesuchte Lösung sollte:

- nativ auf IBM i arbeiten,
- kurzfristige Richtlinienänderungen und die schnelle Bereitstellung neuer Zugriffsregeln
- unterstützen,
- den laufenden Bankbetrieb nicht beeinträchtigen,
- die Netzwerksegmentierung rund um sensible Finanzsysteme stärken,
- die Transparenz über Netzwerkaktivitäten auf IBM i verbessern.

Implementierte Lösung

Raz-Lee implementierte iSecurity Firewall auf sämtlichen IBM i-Partitionen.

iSecurity Firewall

Implementierung einer nativen Netzwerkzugriffskontrolle und Netzwerksegmentierung direkt auf der IBM i-Schnittstellenebene. Zu den Funktionen gehören:

- Einschränkung des Netzwerkzugriffs anhand von Benutzerprofil, IP-Adresse, Subnetz, Protokoll und Uhrzeit
- Kontrolle des Zugriffs auf IBM i-Dienste wie FTP, ODBC, DRDA, Telnet und Remote Command
- Echtzeitüberwachung eingehender Verbindungsversuche
- Umsetzung von Segmentierungsrichtlinien für geschäftskritische Bankanwendungen und sensible Finanzdaten
- Erstellung neuer Zugriffsregeln innerhalb weniger Minuten
- Schnelle Bereitstellung temporärer Zugriffsberechtigungen für Dienstleister oder Projekte
- Anpassung von Sicherheitsrichtlinien ohne Änderungen an Anwendungen
- Sofortige Reaktion auf neue Bedrohungen oder betriebliche Anforderungen
- Umsetzung granularer Zugriffskontrollen ohne Abhängigkeit von externen Firewall-Administratoren

Diese Flexibilität reduzierte operative Engpässe erheblich und verkürzte die Reaktionszeiten bei sicherheitsrelevanten Anforderungen deutlich.

Ergebnisse

- Deutlich verbesserte Netzwerksegmentierung und Zugriffskontrolle für IBM i
- Reduziertes Risiko unautorisierter Netzwerkverbindungen innerhalb der Bankensysteme
- Höhere Transparenz über Netzwerkaktivitäten und Zugriffsversuche auf IBM i
- Schnellere Umsetzung neuer Sicherheitsrichtlinien und temporärer Zugriffsregeln
- Hohe Reaktionsfähigkeit auf betriebliche und sicherheitsrelevante Anforderungen
- Implementierung ohne Beeinträchtigung des produktiven Bankbetriebs

Die Bank konnte die Netzwerksicherheit ihrer IBM i-Umgebung nachhaltig verbessern und gleichzeitig die Flexibilität bewahren, die in einem dynamischen Bankenumfeld erforderlich ist.

Feedback des QSA

"Einer der größten Vorteile für unser Team war die Geschwindigkeit und Einfachheit bei der Erstellung neuer Zugriffsregeln. Granulare Zugriffskontrollen für IBM i konnten innerhalb weniger Minuten umgesetzt werden, anstatt langwierige Änderungsprozesse für Netzwerk-Firewalls abwarten zu müssen. Mit der Raz-Lee Firewall haben wir sowohl unsere Sicherheit als auch unsere operative Flexibilität deutlich verbessert."

— Infrastructure Security Manager (sinngemäß wiedergegeben)