

Referenzprojekt



Cecabank automatisiert Mainframe-Administrationsaufgaben und der Sicherheitsverwaltung für RACF-Ereignisse

Die Informationssicherheit ist ein fundamentaler Aspekt bei der Cecabank und die Technologie ist der Schlüssel zur Optimierung ihrer Informationssysteme. Die Cecabank verbindet modernste Technologie mit der strikten Einhaltung von Vorschriften und hohen Standards in Bezug auf die Informationssicherheit. Das starke Engagement der Cecabank für technologische Innovationen hat dieses Projekt mit Beta Systems vorangetrieben und die Automatisierung und Effizienz im Bereich der Informationssicherheit signifikant verbessert. Mit der Technologie von Beta Systems hat die Cecabank ihr Mainframe-Sicherheits- und Cybersecurity-Risikomanagement automatisiert, um Risiken zu reduzieren und zu minimieren, die Effizienz des zOS/RACF-Managements zu stärken und zusätzliche Funktionen für die Erkennung von Angriffen oder Bedrohungen sowie die Einhaltung der GDPR-Vorschriften und Überwachungsanforderungen bereitzustellen.

In den letzten vier Jahren hat die Cecabank intensiv an den Plänen zur digitalen Transformation gearbeitet und bei deren Umsetzung und Weiterentwicklung erhebliche Fortschritte erzielt. Um das Niveau, die Qualität und die Sicherheit der Dienstleistungen zu gewährleisten, muss die gesamte Hard- und Software die digitale Transformation unterstützen.

Die Cybersecurity Abteilung muss sowohl die Sicherheit erhöhen als auch die Compliance-Anforderungen gemäß GDPR erfüllen und den Anforderungen der internen Revision gerecht werden. Jeder Mitarbeiter erhält nur die Berechtigungen in IT-Systemen, die er zur Erfüllung seiner Aufgaben benötigt, um ein adäquates Maß an Sicherheit zu erreichen.

Die Cecabank entschied sich für _beta access admin von Beta Systems, weil es ihre Anforderungen nicht nur erfüllte, sondern sogar übertroffen hat, indem es eine einzige vereinfachte und dennoch zuverlässige Gesamtlösung für zOS-Sicherheit Verwaltung und Audit bietet. Ein zusätzlicher Bonus war die Integration mit dem SIEM-System, die alles deutlich vereinfachte.

Über Cecabank

Die Cecabank ist die führende spanische Großhandelsbank für Wertpapierdienstleistungen. Sie unterstützt die Geschäftsprojekte verschiedener Finanzinstitute. Als Spezialist für Treasury, Zahlungsverkehr und digitale Lösungen bietet sie finanzielle und technologische Lösungen, die auf die Bedürfnisse ihrer Kunden zugeschnitten sind, und ist auf den größten europäischen Märkten vertreten. Als führender Fondsverwahrer und einer der Hauptakteure im Bereich der Verwahrung und Abrechnung von Wertpapieren verfügt sie im März 2021 über ein verwahrtes Vermögen von mehr als 189.202 Millionen Euro und mehr als 210.800 Millionen Euro an verwahrten Vermögenswerten. Im Jahr 2020 wurde die Cecabank zum vierten Mal in Folge von der Fachzeitschrift Global Banking and Finance Review zur besten Depotbank in Spanien gewählt.

Die Cecabank ist ebenfalls im Vereinigten Königreich, der Schweiz, Deutschland und Portugal vertreten.

Vor der Einführung von _beta access verarbeitete die Cecabank die vom Mainframe ausgehenden Sicherheitsereignisse (RACF SMF-Ereignisse) im Batch-Modus, d.h. mit einer täglichen Belastung. Die Verwaltung von Benutzern, der Zugriff auf Ressourcen, der Schutz von Ressourcen und die Zuordnung zwischen ihnen erfolgte mit den vom Betriebssystem zur Verfügung gestellten Tools.

Der Zugriff auf Audit-Daten erforderte einen zusätzlichen Aufwand für das zOS-Administrationsteam, da es mit der Umgebung vertraut war und über ausreichende Zugriffsrechte verfügte. Dies stellte eine Herausforderung dar, da die Warnmeldungen das SIEM nicht in Echtzeit erreichten, und auch die Verwaltung war aufwändig - die Administratoren mussten die Audit-Aufgaben ausführen und kontrollieren, um die Informationen an die Auditoren zu liefern.



"Wir können nun problemlos Sicherheitslücken im RACF-System erkennen und die Compliance-Vorschriften erfüllen. Selbst technisch nicht erfahrene Benutzer können die erforderlichen Audit-Berichte generieren."

*Sela Santamaría
Direktorin für IT-Systeme bei Cecabank*

Mit der Implementierung von _beta access hat die Cecabank viele Vorteile erreicht. Die IT-Abteilung ist nun in der Lage, eine komfortable Windows-Oberfläche zur Verfügung zu stellen, die es Auditoren ermöglicht, das System ohne besondere RACF- oder zOS-Kenntnisse zu bedienen. Die Lösung ermöglicht es auch technisch nicht erfahrenen Benutzern, das RACF-System zu überprüfen und Audit-Berichte zu erstellen. Sie können über eine benutzerfreundliche Windows-Oberfläche schnelle Audits durchführen und vorkonfigurierte Audit-Berichte erstellen, die auf den tatsächlichen Anforderungen und den Best Practices der Branche basieren.

Mit der neuen Echtzeit-Überwachung erhält der Benutzer eine Warnmeldung in Echtzeit, sobald ein Kritisches RACF- oder sicherheitsrelevantes Ereignis eintritt. Daher können Sicherheitsverletzungen viel schneller erkannt werden.

Dies führt zu einer sofortigen Eskalation dieser an vordefinierte Empfänger oder Betriebsüberwachungssysteme. Die Cybersecurity-Abteilung ist nun in der Lage, frühzeitig Warnungen und Alarmer zu erhalten. _beta access admin liefert mit seiner benutzerfreundlichen ISPF-Oberfläche Funktionen für die zentrale RACF-Verwaltung. Ein umfassendes Set an Funktionen ermöglicht die Pflege von RACF-Profilen und bietet gleichzeitig einen transparenten Überblick über alle im RACF-System zu verwaltenden Informationen.

Die Vorteile der Lösung:

- ✓ Steigerung der Effizienz bei der Verwaltung und dem Management von zOS-Benutzern, Ressourcen und Zugriff
- ✓ Ermittlung von Sicherheitslücken im RACF-System und Einhaltung der Vorschriften.
- ✓ Erstellen und Anzeigen von Berichten über Zugangsberechtigungen und Systemkonfigurationen.
- ✓ Echtzeit-Überwachungstool alarmiert die verantwortlichen Mitarbeiter über kritische RACF-Ereignisse, z. B. wenn auf sensible Daten zugegriffen wird oder wenn kritische Benutzerattribute geändert werden.
- ✓ Schnelle Alarmer bei Zwischenfällen in der Mainframe-RACF-Umgebung, die Fähigkeit, Alarmer und Warnungen in nahezu "Echtzeit" an SIEM zu senden.
- ✓ Überprüfen Sie sicherheitsrelevante Verstöße und stellen Sie sicher, dass die konfigurierten RACF Einstellungen ihr System ordnungsgemäß schützen..

© Beta Systems DCI Software AG. All rights reserved.

Kontaktieren Sie uns!

Beta Systems DCI Software AG

Alt-Moabit 90d
10559 Berlin | Germany

Telefon: +49 (0) 30 726 118-640
insidesales-dci@betasystems.com

_betasystems

www.betasystems-dci.com