CONSIST PROJEKT REFERENZ

Sicherheit für den Bankbetrieb – Ein Fall für Splunk

Die Story in Kürze

Von einfachen Zahlungsströmen über Außenhandelsfinanzierungen bis hin zur Risikoabsicherung auf der Währungs- oder Zinsseite: Unternehmen erwarten eine jederzeit verfügbare und schnelle Abbildung dieser Dienstleistungen von ihrer Bank.

Im Hintergrund des Bankgeschäftes laufen daher komplexe IT-Systeme und -Prozesse, die beispielsweise Kennzahlen für Risikomanagement und Controlling aggregieren, aufbereiten und melden oder spezielle Algorithmen im Trading einsetzen. Die Folge ist ein Datenhype, für den zu jeder Tages- und Nachtzeit Integrität, Verfügbarkeit und Sicherheit gewährleistet sein muss – Big Data im Big Business.

Diese Masse an Datenströmen bringt die Gefahr mit sich, an vielen Stellen fehlgeleitet, angezapft oder falsch bedient werden zu können. Banken stehen daher vor der Aufgabe, jeden einzelnen Systemzugriff durch ein gezieltes Monitoring überwachen zu müssen.

Innerhalb der Finanzbranche konnte Consist nun in einem Kundenprojekt das dafür nötige zentrale Sicherheitsinformations- und Ereignismanagement (SIEM) installieren, das nicht manipulierbar ist und in Echtzeit operieren kann. Alle Anwenderprozesse, selbst für privilegierte Nutzer, sind dadurch revisionsfest und nach den neuesten Sicherheitsbedingungen von EZB und BaFin in den Bankalltag integriert.

Vom reibungslosen Projektablauf waren alle Beteiligten rund um die zertifizierten Spezialisten von Consist begeistert. So konnten sämtliche Schritte von der Beratung über die Implementierung bis hin zur Übernahme in die Managed Services von Consist in time und in budget realisiert werden.

Die Aufgabe

- Monitoring privilegierter User / Admins
- Ablösung heterogener Sicherheitssysteme durch ein zentrales Sicherheitsinformationsmanagement

Die Herausforderung

- Besonderheit: Mehr als 40 heterogene Systeme mit sehr hohem Schutzbedarf einschließlich SAP vorhanden, die eingebunden und überwacht werden müssen
- Etablierung eines zentralen aktuellen Standardsystems, jederzeit erweiterbar um neue Anwendungen
- Implementierung eines nicht manipulierbaren, in Echtzeit operierenden Meldesystems

Die Lösung mit Consist

- Proof of Concept
- Projektteam mit internen Spezialisten (Projektleitung und Fachanwendungsbetreuer) und externen Spezialisten von Consist (zertifizierte Splunk- und Security-Berater)
- Beratung und Unterstützung hinsichtlich der Architektur, Systemauslegung und des Betriebs
- Aufsetzen und Inbetriebnahme eines Standardsystems inkl. Einbettung in die kundentypischen Entwicklungs-, Test-, und Produktivsetzungsprozesse (z. B. durch Staging)

Funktionalitäten des SIEM

- Effiziente Standardanbindung mit flexiblem Customizing auf Basis der Splunk Enterprise Plattform und Splunk Enterprise Security
- Anbindung von bankfachlichen Kauf- und Individualanwendungen (inkl. SAP)
- Alert- und Dokumentationsfunktion

Besondere Stärken von Consist

- Hohe Big-Data- und Mainframe-Expertise
- Zertifizierte Splunk-Spezialisten
- Methodik der agilen Softwareentwicklung
- Abschluss des Projekts in time und in budget
- Fließender Übergang in die Anwendungsbetreuung mit Managed Services

Kundennutzen

- Risikominimierung durch Einbindung auch hoch-privilegierter Nutzer ins Monitoring und durch
- Aufdeckung von Inside Threats
- Revisionsfestes, nicht manipulierbares Sicherheitssystem, das in Echtzeit agiert
- Erfüllung der BSI-, EZB- und BaFin-Sicherheitsanforderungen

CONSIST
Business Information Technology

We do IT for you.

Ihr Kontakt:
Joscha Sternadel
sternadel@consist.de
0431 3993-775
Consist Software Solutions GmbH
Christianspries 4, 24159 Kiel
www.consist.de