splunk>

CASE STUDY

Splunk® im Einsatz bei der Finanz Informatik GmbH & Co.KG

Optimiertes Security-Management mit einer einheitlichen SIEM-Lösung

finanz informatik

"Splunk Enterprise ist eine sehr durchdachte Lösung. Die Software ist für Entwicklung und Betrieb konzipiert und kann in einer Vielzahl von Bereichen umgehend Ergebnisse liefern."

Irena Wagner-Osterloh,
Abteilungsleiterin
Berechtigungstechnologien
Finanz Informatik GmbH & Co. KG

ÜBERBLICK

BRANCHE
- Finanzdienstleistungen

SPLUNK USE CASES
- Security
- Compliance

BUSINESS IMPACT
- Plattform- und Funktionsübergreifende Lösung für schnellere und umfassendere Identifizierung potentieller Sicherheitsvorfälle und der Unterstützung bei der Behebung
- Optimierter Schutz von Kundendaten

DATENQUELLEN
- Maschinendaten (Logfiles) der Plattformen Mainframe
- Unix, Windows
- Netzwerk-Systeme
- Middleware-Komponenten (z.B. Datenbanken und Applikationsserver)

Das Unternehmen

Die Finanz Informatik, zentraler IT-Dienstleister der Sparkassen-Finanzgruppe, mit Sitz in Frankfurt am Main zählt bundesweit 416 Sparkassen, acht Landesbanken, die DekaBank, zehn Landesbausparkassen sowie weitere Unternehmen im Verbund der Sparkassen-Finanzgruppe zu ihren Kunden. Das Angebot umfasst das gesamte IT-Spektrum – von der Entwicklung und Bereitstellung von IT-Anwendungen, Netzwerken und technischer Infrastruktur über den Rechenzentrumsbetrieb bis hin zu Beratung, Schulung und Support. Mit der leistungsfähigen Gesamtbanklösung OSPlus stellt das Unternehmen heute eines der führenden IT-Systeme für den deutschen Bankenmarkt. Tochterunternehmen wie die Finanz Informatik Technologie Service, die Finanz Informatik Solutions Plus, die Star Finanz und die inasys ergänzen mit ihren Leistungsangeboten das IT-Portfolio. Auf den Systemen von Finanz Informatik werden jährlich 98 Milliarden technischer Transaktionen durchgeführt, der Finanzdienstleister übernimmt damit den Service für rund 125 Millionen Konten.

Die Herausforderung

Bei der Finanz Informatik (FI) waren unterschiedliche Security Information und Event Management(SIEM)-Systeme für die Umgebungen Mainframe, Netze, Unix und Windows im Einsatz. Um eine bessere, plattformübergreifende Übersicht und Auswertung zu erzielen, wurde eine einheitliche SIEM-Plattform gesucht, die als unternehmensweite Lösung in der Finanz Informatik eingesetzt wird.

Neben hohen technischen Anforderungen an Datenintegrität, Skalierbarkeit, Hochverfügbarkeit und Support stand für die FI die plattformübergreifende Eventkorrelation im Vordergrund. Zusätzlich musste sich die neue Lösung nahtlos in die vorhandene IT-Infrastruktur der Finanz Informatik integrieren lassen und mandantenfähig für den Einsatz bei den angeschlossenen Kunden sein.

Splunk in der Praxis - Implementierung

Als Ergebnis einer Marktevaluierung beschloss die Finanz Informatik, die Software Splunk Enterprise einzusetzen.

Splunk Enterprise indexiert und analysiert täglich die Protokolldateien mehrerer tausend IT-Systeme (Server, Netzwerk- und Middleware-Komponenten) für ein plattformübergreifendes Berechtigungs-Monitoring. Die Lösung überwacht den Zugriff auf kritische Konfigurationen und Daten.

Sowohl in Echtzeit als auch historisch kann mit Splunk Enterprise überprüft werden, wer, wann und wo auf kritische Konfigurationen und Daten zugegriffen hat. Auf Basis von Reports und Alarmen werden Sicherheitsfehler, Verstöße und auffällige Aktionen identifiziert, gemeldet und bewertet.

Splunk Enterprise ist eine Plattform, die die Anforderungen der Finanz Informatik an ein ganzheitliches Sicherheitsinformationssystem erfüllt und auch in anderen Einsatzfeldern Mehrwerte bringen kann.

Kostenloser Download

Splunk Enterprise: Laden Sie Splunk Enterprise kostenlos herunter. Sie erhalten eine Splunk Enterprise Lizenz für 60 Tage und können bis zu 500 Megabyte an Daten pro Tag indizieren. Während bzw. am Ende des Testzeitraums von 60 Tagen können Sie sich für eine ständige Splunk Free-Lizenz entscheiden oder aber eine Splunk Enterprise-Lizenz erwerben, indem Sie sich an dach_sales@splunk.com wenden.

Errungenschaften

Optimierte Sicherheit durch schnellere Fehler-Identifizierung und -Behebung

Splunk Enterprise ersetzt die bisherigen SIEM-Tools und bietet für die FI eine einheitliche Lösung für ein plattformübergreifendes Security Information und Event Management. Die Analyse der Maschinendaten (Protokolldateien der IT-Infrastruktur) wird deutlich erleichtert. Daten werden komfortabler, schneller und vor allem plattformübergreifend zur Analyse von potentiellen Sicherheitsvorfällen ausgewertet.

Mit Splunk Enterprise als Basis der neuen, zentralen SIEM-Lösung kann die FI den Schutz der verarbeiteten Daten in ihren Rechenzentren weiter verbessern bei gleichzeitiger Reduktion von Komplexität, Fehleranfälligkeit und Herstellkosten.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | dach_sales@splunk.com +49 (0)89 90 405 998 apps.splunk.com

Item#71813_SPLUNK_DATA_SHEET_GERMAN_Proof2