Wüstenrot-Gruppe

Kundenprofil
- Großes österreichisches Finanzdienstleistungsunternehmen mit Bauspar- und Versicherungsbereich

Branche
- Finanzdienstleister

IT-Umgebung
- 3.500 Mitarbeiter

Anforderung
- Bisherige SIEM-Lösung konnte die neuen Anforderungen des Unternehmens nicht erfüllen

McAfee-Lösung
- McAfee Enterprise Security Manager

Ergebnisse
- Implementierung innerhalb von nur 15 Tagen
- Hochleistungsfähige und zuverlässige Protokollierung von Daten aus 100 Quellen
- Verarbeitung von mehr als 1.000 Ereignissen pro Minute
- Zuverlässige Protokollarchivierungs- und Verschlüsselungsfunktionen
- Konfigurierbare Dashboards unterstützen eine große Zahl an Datentypen und Berichten

McAfee ESM bietet Sicherheitstransparenz für das Bank- und Versicherungsunternehmen

Die Wüstenrot-Gruppe ist mit mehr als 3.500 Mitarbeitern und 3,5 Millionen Kunden einer der größten Finanzdienstleister Österreichs. Das Unternehmen besitzt zwei Bereiche: die Bausparkasse Wüstenrot AG für Bankdienstleistungen und Baukredite für Eigenheime sowie die Wüstenrot Versicherungs-AG. Wüstenrot verfügt über Niederlassungen in Tschechien, Ungarn, Slowenien und Kroatien.

Herausforderung für das Unternehmen: Sichere Bank- und Versicherungsgeschäfte

Die Daten- und Netzwerksicherheit ist ein wichtiger Erfolgsfaktor für jedes Unternehmen, das im Bank- und Versicherungssektor aktiv ist. Zum Schutz der Reputation und des Kundenvertrauens hat sich Wüstenrot verpflichtet, die maximal mögliche Sicherheit zu gewährleisten. Dies gilt insbesondere für vertrauliche Kundendaten sowie die Verwaltung der Bankensysteme und -netzwerke.

Bislang setzte Wüstenrot zur Verarbeitung und Analyse von Sicherheitsereignisprotokollen auf IBM Tivoli Compliance Insight Manager. Diese Lösung konnte jedoch nicht mit dem Wachstum und der Entwicklung des Unternehmens Schritt halten. Aus diesem Grund legte Wüstenrot mehrere Anforderungen für eine SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management) fest. Das Unternehmen suchte nach einer sofort einsatzbereiten Lösung, die Hardware und Betriebssystem umfasste und vereinfachte Berichterstellung, agentenlose Protokollerfassung sowie Kontrollvorschriften wie BASEL II, PCI DSS und ISO 27002 unterstützen sollte. Zudem benötigte Wüstenrot eine Lösung, die alle Ereignisse der letzten fünf Tage sofort darstellen und Daten von Oracle HPUX, Windows Server, Microsoft SQL Server, CheckPoint und McAfee ePolicy Orchestrator (ePO) protokollieren kann. Ebenso suchte Wüstenrot nach einem SIEM-Anbieter, der keine Lizenzbeschränkungen bei der Anzahl der Protokollquellen erhob und eine Garantie für die Wartungskosten gewährte.

Gründe für McAfee: Hochleistungs-SIEM-Lösung

Aufgrund dieser Anforderungen erklärte Wüstenrot die Lösung McAfee Enterprise Security Manager (ESM) zum Hauptfavoriten. Das Unternehmen beschloss jedoch, vor der endgültigen Entscheidung Tests mit einer Proof-of-Concept-Implementierung durchzuführen. Im Rahmen dieser Testimplementierung sollte McAfee ESM Daten von jeder Quelle in der Umgebung protokollieren und diese Informationen sowie ihre Performance anhand interner Wüstenrot-Spezifikationen bewerten. Die Systemintegratoren Auriga Systems und COMGUARD konnten McAfee ESM in weniger als einem Tag implementieren. Dazu gehörten auch eine kurze Schulung zu den fortschrittlichen Möglichkeiten der Lösung sowie eine gemeinsame Festlegung von Kennwerten für eine erfolgreiche Konzeptstudie. Innerhalb von vier Wochen Betrieb stellte McAfee ESM die Möglichkeiten unter Beweis, alle erforderlichen Protokollquellen miteinander zu verknüpfen.

Die Lösung von McAfee

Auf Grundlage der erfolgreichen Konzeptstudie sowie einem günstigen Preisvorschlag von McAfee entschied sich Wüstenrot für das McAfee ESM-Modell ETM-4600-ELM. Dank der Möglichkeiten zur Protokollierung von mindestens 1.000 Ereignissen pro Sekunde (EPS) war McAfee ESM die ideale Wahl für Wüstenrot.

In Zusammenarbeit mit den Systemintegratoren konnte das Wüstenrot-IT-Team McAfee ESM in nur 15 Arbeitstagen implementieren. Die Lösung rief Informationen aus 100 verschiedenen Protokollquellen ab und demonstrierte eine sehr hohe Protokollanalysegenauigkeit sowie -leistung.

„McAfee Enterprise Security Manager ist eine sehr flexible und effektive Lösung, dank der wir die Ereignisse aus mehreren Monaten innerhalb von Sekunden verarbeiten und sofort auf die relevanten Informationen zugreifen können. Die Dashboards sind sehr intuitiv und unterstützen mein Sicherheitsteam und mich bei der Arbeit. Dadurch kann ich Probleme schnell identifizieren und sie zeitnah beheben."

– Bc. Jiří Dolejš,
Security Manager,
Wüstenrot

Im Anschluss an die vollständige Implementierung der Protokollquellen konfigurierte das Implementierungsteam Dashboards und Berichte anhand zuvor vereinbarter Spezifikationen in mehreren wichtigen Bereichen. Dazu gehörten Änderungen an den Berechtigungsstufen für Active Directory, Abstürze und Neustarts von Servern sowie Diensten, Virenschutzereignisse in der gesamten Infrastruktur und neu entdeckte Geräte im Netzwerk.

Der McAfee-Technik-Support stellte für das einzige während der Implementierung aufgetretene Problem – ein inkompatibles Zeitstempelformat des Audit-Protokolls der Oracle-Datenbank – eine schnelle und effektive Lösung bereit. Dazu entwickelte McAfee in der nativen Oracle-Umgebung ein spezielles Zeitstempelformat.

Pläne für die Zukunft

McAfee ESM übertrifft bei Weitem die ursprünglichen Anforderungen von Wüstenrot – sofortige Verfügbarkeit von Ereignissen der letzten fünf Tage. Jetzt können aggregierte Protokollinformationen von bis zu einem ganzen Jahr sofort verarbeitet werden.

In Phase 1 der Implementierung wurde das SIEM-System implementiert und mit Daten gefüllt. Nun ist Wüstenrot damit beschäftigt, Analyse-Dashboards für ausgewählte Bereiche zu implementieren, auf die die Sicherheitsabteilung dauerhaften Zugriff benötigt. Außerdem passt Wüstenrot Korrelationsregeln so an, dass False-Positives für Standardregeln vermieden werden.

Die Archivierung von Protokollen in ihrer ursprünglichen Form wird nur durch die verfügbare Speichermenge eingeschränkt. Wüstenrot hat hohe Standards für die Integrität und Vertraulichkeit der archivierten Protokolle festgelegt. Aus diesem Grund hat das Unternehmen ein dediziertes Speicher-Hardware-Array für die Protokolle bereitgestellt, das die zertifizierten Verschlüsselungsfunktionen von McAfee ELM nutzt. Wüstenrot hat sich das Ziel gesetzt, die Protokolle für ein Jahr zu archivieren und bereitet derzeit die entsprechenden Speicher-Arrays vor. Im nächsten Schritt soll die Protokollarchivierungsfunktion zusammen mit der Indizierung für die Volltextsuche mit McAfee Enterprise Log Manager aktiviert werden.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

61188cs_wustenrot_0614