PLUSCARD: LOGDATENMANAGEMENT REVISIONSSICHER UND EFFIZIENT MIT IBM QRADAR SIEM

AUF EINEN BLICK

Aufgabe
PLUSCARD unterliegt den Vorgaben des PCI-DSS. Das vorhandene Logmanagement konnte das wachsende Datenvolumen nicht mehr effizient und den Standards entsprechend bewältigen. Eine SIEM-Lösung sollte hierbei Abhilfe schaffen.

Leistungsumfang
Analyse, Proof-of-Concept und Implementierung der SIEM-Lösung IBM QRadar.

Vorteile
> Stabiles und auditsicheres Logdatenmanagement
> Erhöhung der Effizienz durch Wegfall manueller Arbeitsschritte
> Korrelation von Ereignissen und deren Alarmierungen in Echtzeit
> Erfüllung von Compliance-Anforderungen

Die im Jahr 1996 in Saarbrücken gegründete PLUSCARD übernimmt für Banken und Sparkassen umfangreiche Dienstleistungen rund um Kreditkarten von Mastercard und Visa. Service über dem Standard und persönliche Betreuung sind selbst gesteckte Leitlinien, die PLUSCARD als Impulsgeber für den Kreditkarten- und Processing-Markt auszeichnen. Insgesamt werden bereits über sechs Millionen Kreditkarten von PLUSCARD betreut: Tendenz steigend.

Das Unternehmensziel von PLUSCARD ist es, Finanzinstitute und deren Kunden mit hochwertigen und attraktiven Dienstleistungspaketen rund um das Produkt Karte zu bedienen. Das Leistungsspektrum reicht von der Produktentwicklung über die Antragserfassung und den 24-Stunden-Service des Callcenters bis hin zur Zahlungsreklamation.

PCI-DSS STELLT ANFORDERUNGEN AN DIE FINANZBRANCHE

Sofern ein Unternehmen Kreditkartentransaktionen speichert, übermittelt oder abwickelt, unterliegt es den Vorgaben des „Payment Card Industry Data Security Standard“ (PCI-DSS). Dieser internationale IT-Sicherheitsstandard muss von allen Instituten, Partnern und Dienstleistern, die Kreditkartendaten verarbeiten, umgesetzt und eingehalten werden. In der Anforderung Nummer 10 des PCI-DSS ist die Notwendigkeit von umfassenden Logauswertungen definiert. Die Einhaltung dieser Vorgaben wird in jährlich stattfindenden mehrtägigen Audits in den betroffenen Unternehmen überprüft. PLUSCARD erfüllt seit dem Jahr 2008 den PCI-DSS Standard.

Auf Dauer konnte das von PLUSCARD eingesetzte Logdatenmanagement das wachsende Datenvolumen jedoch nicht mehr effizient und den Sicherheitsstandards entsprechend bewältigen. PLUSCARD musste viele Ressourcen einsetzen, um die Logdaten täglich manuell zu kontrollieren. Diesen Umstand galt es zu beheben. Deshalb begann die IT-Abteilung von PLUSCARD sich mit modernen SIEM-Lösungen (Security and Information Event Management) zu beschäftigen.

PLUSCARD
Menschen. Karten. Strategien.

SVA unterstützte PLUSCARD in allen Phasen der Migration hin zum revisionssicheren Logmanagement mit IBM QRadar SIEM. Die ursprünglich gesteckten Ziele waren damit erreicht, das Potenzial jedoch längst nicht ausgeschöpft.

IBM QRADAR SIEM ERSETZT MEHRERE PARALLELE LOGSERVER

Nach eingehender Analyse gemeinsam mit den Experten von SVA ist die Wahl auf die SIEM-Lösung aus dem Hause IBM gefallen: QRadar. Denn IBM QRadar SIEM konnte wesentliche Anforderungen erfüllen. Wichtig war vor allem, dass die Kombination aus schlanker Implementierung mit zunächst einem physischen Server schnell das dringend benötigte stabile und auditsichere Logdatenmanagement gewährleistet. Darüber hinaus war die Integration der meisten Logdatenquellen dank der umfangreich vorhandenen Device Service Modules (DSM) unkompliziert möglich. Die Bedienung erfolgt weitgehend über eine nutzerfreundliche Oberfläche. Das spart wertvolle Zeit beim Security-Logmanagement. Alarmierungen und deren Korrelation erfolgen in Echtzeit und gestaltet die Analyse von Events auch über mehrere Loginstanzen effizient. Gerade vor dem Hintergrund des wachsenden Logdatenaufkommens hat sich das bezahlt gemacht. Es muss keine manuelle Auswertung der Logs, sondern lediglich eine separate Prüfung und Bewertung der durch IBM QRadar SIEM erstellten Berichte erfolgen. So kann PLUSCARD allen Compliance-Anforderungen Rechnung getragen.

SVA PUNKTET MIT SEINER IBM-KOMPETENZ

Die IT-Security-Experten von SVA führten mit PLUSCARD einen erfolgreichen Proof-of-Concept (PoC) durch. Dieser belegte, dass IBM QRadar SIEM die gestellten Anforderungen erfüllt und darüber hinaus viel Spielraum für weitere Anwendungsbereiche bietet. Im Folgenden unterstützte SVA PLUSCARD in allen Phasen der Migration weg von der bestehenden Lösung hin zum revisionssicheren Logmanagement mit IBM QRadar SIEM.
Die ursprünglich gesteckte Zielsetzung war damit erreicht, das Potenzial jedoch längst nicht ausgeschöpft. In zahlreichen Workshops haben die Teams von SVA und PLUSCARD gemeinsam neue Ziele definiert und in Angriff genommen. So wurde die Lösung kontinuierlich zu einem vollwertigen SIEM-System ausgebaut. Dank der Weiterentwicklung durch IBM ist es zudem möglich ein Mapping von vorhanden Anwendungsfällen direkt in QRadar auf MITRE ATT&CK Framework vorzunehmen. Mit diesem Schritt kann PLUSCARD die Sicherheit im internen Netzwerk gezielt und über alle Bereiche auf ein gleiches, hohes Niveau heben.
Dabei soll es nicht bleiben. Die IT Security Consultants von SVA unterstützen im engen Dialog mit PLUSCARD bei der Optimierung bestehender Use Cases sowie der Entwicklung von neuen Themenfeldern.

KONTAKT
SVA System Vertrieb
Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel: +49 6122 536-0
Fax:+49 6122 536-399
mail@sva.de
www.sva.de

PLUSCARD
Menschen. Karten. Strategien.