Zertifikatsverwaltung in einer EU-Einrichtung

Eine Einrichtung der EU setzt auf die TOPKI Lösung von SECARDEO bei der Automatisierung des X.509 Zertifikatsmanagements.

Einrichtung der Europäischen Union

Unser Kunde ist eine der Einrichtungen, die im Dienste der Verwaltung der Europäischen Union stehen.

Herausforderung und Zielsetzung

Der Kunde betrieb eine interne PKI auf der Basis einer Microsoft CA. Damit wurden mehrere hundert SSL Zertifikate sowie über 1.000 S/MIME Zertifikate verwaltet. Der primäre Bedarf bestand darin, die Abläufe im Zusammenhang mit der internen PKI zu rationalisieren. Das bedeutet, die Verwaltung des Lebenszyklus der Zertifikate zu optimieren und die Ausstellung und Bereitstellung von Zertifikaten sowohl auf Windows-Endpunkten als auch auf mobilen Geräten zu automatisieren. Zuvor stützten sich all diese Vorgänge zu einem großen Teil auf manuelle Verfahren und hausgemachte Skripte. Deshalb hätte der Kunde gerne ein professionelles Tool, das dabei helfen könnte, all diese Aktivitäten effizienter und zuverlässiger durchzuführen.

Zudem wurde darüber nachgedacht, die internen S/MIME-Zertifikate durch Zertifikate einer öffentlichen CA zu ersetzen.

Anforderungen

Die wesentliche Anforderung an die Lösung zur Zertifikatsverwaltung ist die Automatisierung des gesamten Zertifikatslebenszyklus für verschiedene Zertifikatstypen für SSL, S/MIME sowie Geräteauthentifizierung.

Ferner wäre in diesem Sinne die Fähigkeit einer solchen Lösung, mit der internen Microsoft-CA sowie mit einer externen CA zusammenzuarbeiten, ein zusätzlicher Mehrwert.

Um zu prüfen, ob all diese Anforderungen von der TOPKI-Lösung von SECARDEO grundsätzlich erfüllt werden, wollte der Kunde möglichst zeitnah ein Proof-of-Concept realisieren.

Die Lösung

Für das Proof-of-Concept wurden die benötigten Software-Komponenten durch die Experten von SECARDEO beim Kunden installiert. Gleichzeitig wurde mit Unterstützung von SECARDEO eine MKPI-Vereinbarung mit einer der öffentlichen CA abgeschlossen, die mit TOPKI interoperabel sind, und es wurde ein MPKI-Konto für diese öffentliche CA eingerichtet.

> *„TOPKI hat die Art und Weise, wie wir unsere PKI- und S/MIME-Zertifikate verwalten, grundlegend verändert. Es hat uns ermöglicht, die Abläufe im Zusammenhang mit der Verwaltung von Zertifikaten zu rationalisieren, indem wir Aufgaben automatisiert haben, die früher menschliches Eingreifen erforderten."*
>
> *IT Security Officer*

Die Lösung besteht aus den Komponenten certEP für das Autoenrollment von Zertifikaten für Benutzer und Computer in der Active Directory Domäne, certLife für die zentrale Verwaltung aller Zertifikate mittels Web-Browser, certRevoke für die Auto-Revokation von verwaisten Zertifikaten sowie certPush MDM für die Verteilung von S/MIME Zertifikaten auf Mobilgeräte. Die Zertifikatsdatenbank wurde auf einem Microsoft SQL Server installiert.

Der PoC konnte mit einigen Anpassungen und Software-Updates nach wenigen Wochen erfolgreich abgeschlossen werden. Nun erfolgte das Setup des Produktivsystems. Hier wurden die TOPKI-Komponenten an zwei CA-Backends angeschlossen, die Public CA sowie die interne Microsoft CA. Die Konfiguration der Lösung und der AD Certificate

Templates, Group Policies sowie die Anbindung an das Mobile Device Management System MobileIron Core erfolgte mit kompetenter Unterstützung durch das SECARDEO Team.

Kundenvorteile

Die SECARDEO TOPKI Lösung brachte für den Kunden zum einen eine durchgängige Automatisierung der Prozesse innerhalb des Zertifikatslebenszyklus.

Zum anderen wurde die Verwaltung der Zertifikate sowohl von der öffentlichen CA als auch der internen CA durch ein Web-basiertes Tool wesentlich vereinfacht. Viele weitere Features wie automatische Benachrichtigungen halfen, die Zuverlässigkeit des PKI-Betriebs deutlich zu steigern.

Für den einzelnen Nutzer ist die Nutzung sicherer E-Mails dank der automatischen Verteilung von Zertifikaten und privaten Schlüsseln an alle Geräte äußerst bequem geworden und gehört daher zum Standard.

Insgesamt führte die Einführung der SECARDEO TOPKI-Lösung beim Kunden zu einer erheblichen Vereinfachung der PKI-Prozesse durch Automatisierung und der damit verbundenen Zeit- und Kosteneinsparung.