

S/MIME mit Outlook

Unser Kunde setzt bei der Verteilung von Schlüsseln und Zertifikaten zur Signierung und Ende-zu-Ende Verschlüsselung von E-Mails auf die TOPKI Lösung von Secardeo.

Unser Kunde

Das Unternehmen ist ein Dienstleister sowie Hersteller von Groß- und Industrieküchengeräten zur thermischen Speisenzubereitung.



Herausforderung und Zielsetzung

Die Kommunikation mit internen Mitarbeitern als auch mit externen Partnern findet bei unserem Kunden so wie bei vielen mittelständischen und großen Unternehmen in großem Umfang mittels E-Mail auf der Basis von Microsoft Outlook und Exchange und zunehmend auch Mobilgeräten statt. Aus Sicht der IT-Security Verantwortlichen war es nicht akzeptabel, dass interne E-Mails nicht geheim gehalten werden konnten, so dass beispielsweise eine Sekretärin stets Einblick in streng vertrauliche Unterlagen des Managements hatte. Ferner war es ein dringender Wunsch, dass E-Mails nur noch geschützt mit einer digitalen Signatur nach außen versendet werden sollten. Damit kann der externe Partner sicher sein, dass die E-Mail von einem Mitarbeiter unseres Kunden stammt und der Inhalt unverändert ist.

Die Anforderungen

Dem für dieses Projekt zuständige Information Security Manager wurde rasch klar, dass die Sicherheitsanforderungen nicht mit einem Secure E-Mail Gateway erfüllt werden können. Insbesondere kann hiermit keine durchgängige Ende-zu-Ende Verschlüsselung erreicht werden. Zudem sichert eine damit automatisiert erzeugte Signatur nicht zu, dass der in der E-Mail ange-

gebene Absender auch explizit deren Inhalt bestätigt hat. Auf der anderen Seite war sich der zuständige Mitarbeiter bewusst, dass für S/MIME am Client das Problem der Schlüsselverteilung gelöst werden muss. Insbesondere müssen bei der externen Kommunikation öffentlich anerkannte digitale X.509 Zertifikate verwendet werden, damit der Empfänger signierte E-Mails problemlos prüfen kann.

Die Lösung

Der verantwortliche Information Security Manager stieß schnell auf die von Secardeo angebotene TOPKI-Lösung zur vollautomatisierten Verteilung von privaten Schlüsseln und anerkannten Zertifikaten einer öffentlichen Certification Authority (CA). Neben den hervorstechenden funktionalen und sicherheitstechnischen Merkmalen war er vom Preis der Lösung überrascht, der deutlich unter dem gängiger Secure E-Mail Gateways lag – bei einem deutlichen Mehrwert an Funktionalität. Die anfänglichen Bedenken bezüglich der Komplexität der Schlüsselverwaltung konnten in einem Pilotprojekt ausgeräumt werden, das nur wenige Wochen dauerte.

„Das Problem der Schlüsselverwaltung wird mit der TOPKI Lösung von Secardeo super gelöst“

Information Security Manager

Die Produktivsetzung der Lösung erfolgte dann unmittelbar ohne Verzug. Bei unserem Kunden versorgt der in das Active Directory integrierte Secardeo certEP mittlerweile mehrere Tausend Windows Anwender per Autoenrollment mit anerkannten S/MIME Zertifikaten von SwissSign. Die automatisierte Verteilung des privaten Schlüssels auf weitere (mobile) Geräte des Benutzers erfolgt mit Secardeo certPush. Die Secardeo TOPKI Lösung hat sich bei unserem Kunden zur Schlüsselverteilung äußerst bewährt und sie reduziert den Verwaltungsaufwand durch hochgradige, zuverlässige Automatisierung der Abläufe.

