Durchbruch der Corporate PKI

Immer mehr Unternehmen entschliessen sich dazu, eine eigene Public Key-Infrastruktur für die Ausgabe und Verwaltung von X.509-Zertifikaten aufzubauen. Die Gründe hierfür sind nahezu immer die gleichen. Die Unternehmen möchten den Zugriff auf ihre Daten bestmöglichst, effizient und kostengünstig schützen. Moderne Applikationen und Netzwerkkomponenten unterstützen standardmässig den Einsatz von X.509-Zertifikaten und ermöglichen so eine definierte und einheitliche Authentifizierung als Basis für eine Autorisierung von Benutzern und Systemen.

Dieser Erfahrungsbericht im Bereich unternehmensspezifischer Public Key-Infrastrukturen klärt auf.

Huhn-Ei-Problem überwunden

Noch vor wenigen Jahren fand der Aufbau einer PKI primär auf konzeptioneller Basis, sprich auf Papier, statt. Der Fokus lag auf den organisatorischen Prozessen, die mangels ausgereifter technischer Komponenten viel zu theoretisch betrachtet wurden. Die praktische Umsetzung wurde oft zurückgestellt, da die eingesetzten Applikationen nicht mit X.509-Zertifikaten umgehen konnten. Der Entscheid war aus damaliger Sicht richtig, denn eine PKI ohne Applikationen, die mit X.509-Zertifikaten umgehen kann, macht keinen Sinn.
Dies hat sich in den letzten Jahren stark geändert. Moderne Applikationen und Netzwerkkomponenten unterstützen standardmässig X.509-Zertifikate und sind so der Treiber für den Aufbau einer PKI.

PKI Enabler

Als Treiber für den Aufbau einer PKI können heute die folgenden Anwendungen bezeichnet werden:

- 802.1X Port Security (EAP TLS)
- Zertifikatsbasierter VPN-Zugriff
- Zertifikatsbasierte Authentifizierung von Webapplikationen und Webservices
- Zertifikatsbasierter Windows-Logon mittels Smartcard
- Secure E-Mail
- Festplatten und Fileverschlüsselung

Sie stellen aus Sicht einer PKI unterschiedliche Anforderungen an die Ausgabe und Verwaltung von Zertifikaten. Während Zertifikate für die Authentifizierung einfach an Benutzer und Systeme ausgegeben werden können, müssen bei Zertifikaten für Verschlüsselung die jeweiligen privaten Schlüssel hinterlegt werden, sodass im Falle eines Verlustes des privaten Schlüssels die Daten wieder lesbar gemacht werden können. Diese Basisfunktionalität wird heute standardmässig in den entsprechenden Produkten unterstützt.

Teile und herrsche

In einer engen Beziehung zu einer PKI steht das Identity und Access Management (IAM). Eine PKI stellt Zertifikate (Identitätsnachweise) an Benutzer oder Systeme (Entitäten) aus, welche über diese Zugriff auf Daten oder Systeme erhalten (Access Management). Die Erfahrung zeigt, dass PKI- und IAM-Projekte oft zu umfassend betrachtet werden und daher nicht wie gewünscht umgesetzt werden können. Viele bestehende technische und organisatorische Prozesse sind wenig harmonisiert und basieren auf voneinander unabhängigen Applikationen. Beispielsweise ist die organisatorische Verwaltung von Mitarbeitern (Eintritt, Dossier, Ferien, Lohn, Austritt usw.) oft unabhängig von der technischen Verwaltung der Mitarbeiter (Active Directory, LDAP usw.). Zudem sind die diesbezüglichen Prozesse abhängig von politischen und ökonomischen Entscheiden und daher oft im Wandel.
Ein PKI- und IAM-Projekt sollte in einer ersten Phase auf eine einzige oder wenige Applikationen ausgerichtet sein. Die modulare Umsetzung erlaubt den Ausbau der Lösung in weiteren Phasen, indem zusätzliche Komponenten und Applikationen in die Lösung integriert werden.

Ausgereifte Produkte und Prozesse

Nahezu alle Corporate PKI-Projekte werden heute auf der Basis der Certificate Services des Microsoft Server 2003/2008 umgesetzt. Der Grund hierfür ist die kostengünstige Lizenz sowie die nahtlose Integration der Lösung in die von Microsoft dominierten Client-Umgebungen (AD, Windows-Betriebssysteme).
Die Lösung von Microsoft ist ausgereift und bietet vor allem im Zusammenhang mit Authentifizierungszertifikaten im Bereich 802.1X oder VPN-Zugriff effiziente Mechanismen für deren Verteilung und Verwaltung. Die diesbezüglich technischen und organisatorischen Voraussetzungen und Prozesse sind einfach zu definieren und umzusetzen.
Token Management-Systeme von Microsoft oder Drittanbietern können einfach integriert werden und ermöglichen die Ausgabe und Verwaltung von Zertifikaten auf Hardwaretokens (Smartcard, USB-Token). Die Certificate Services von Microsoft können modular erweitert und auch nahtlos in heterogene Umgebungen (Unix, Host-Systeme) integriert werden.

Public Corporate PKI

Eine eigene Corporate PKI sichert einem Unternehmen die Flexibilität, die es braucht, um Applikationen und Prozesse rasch integrieren zu können. Ein Outsourcing einer Corporate PKI ist wenig sinnvoll, da die zentralen Prozesse wie die Registrierung von Benutzern und Systemen oder die Integration von PKI-basierten Applikationen nur durch das Unternehmen selbst durchgeführt werden können. Im Weiteren können durch das Outsourcing einer Corporate PKI automatisierte Prozesse wie beispielsweise das AD-basierte Auto-Enrollment von Zertifikaten nicht genutzt werden.

Der «Nachteil» einer eigenen Corporate PKI ist, dass diese nicht global bekannt ist. Das CA-Zertifikat der Corporate PKI ist beispielsweise nicht global auf Betriebssystemen oder Browsern vorinstalliert und muss daher organisatorisch zwischen den Parteien ausgetauscht werden.

Um eine Corporate PKI global bekannt zu machen, kann diese von einer öffentlichen CA subordiniert werden. Das CA-Zertifikat der Corporate PKI kann über das vorinstallierte Zertifikat der öffentlichen CA überprüft werden und ist somit global vertrauenswürdig. Unternehmen können so Zertifikate austauschen, ohne sich vorgängig abgesprochen zu haben. Der Betrieb einer solchen «Public Corporate PKI» unterliegt den jeweiligen Richtlinien der öffentlichen CA und kann auch als Gütesiegel einer Corporate PKI betrachtet werden.

Fazit

Alle modernen Applikationen und Netzwerkkomponenten unterstützen heute X.509-Zertifikate. Die IT-Verantwortlichen müssen sich immer öfter zwischen Username/Passwort oder Zertifikaten als Identitätsnachweis entscheiden. Aus sicherheitstechnischer, organisatorischer und betriebswirtschaftlicher Sicht ist der Aufbau einer Corporate PKI zukunftssicher und gewinnbringend. ■

keyon AG, 8645 Jona
René G. Eberhard, CEO
Telefon 055 220 64 03, Telefax 055 220 64 01
eberhard@keyon.ch, www.keyon.ch