Automatisiertes Zertifikatsmanagement erhöht Schutz und Verfügbarkeit

Schwachstelle „Zertifikate“ endlich schließen

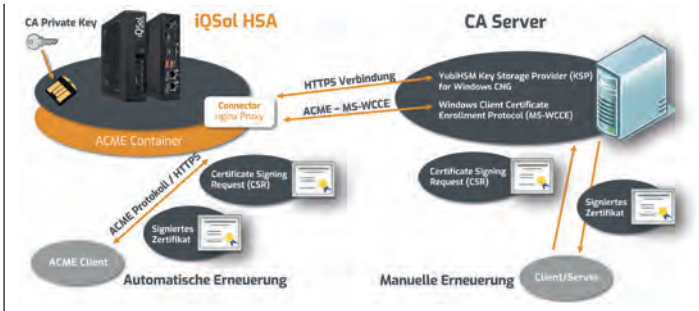
Greifen Cyberkriminelle IT-Infrastrukturen an, haben sie es immer auf den „heiligen Gral“ abgesehen: die PKI, Zertifikate und die wichtigsten „Schlüssel“. Die Hardware Security App (HSA) der niederösterreichischen iQSol GmbH verhindert diese Angriffe durch die hochsichere, zentrale Speicherung sowie die automatisierte Erneuerung von Zertifikaten mit dem neuen ACME-Feature. Kunden sollten ein Update ins Auge fassen, um unvermeidliche Überraschungen durch Ausfälle vorzubeugen.

Von Jürgen Kolb, iQSol GmbH

Mit der iQSol HSA, im Einsatz als physischer Mini-Server mit integriertem YubiHSM, können bis zu 16 PKI-Server angebunden werden. Sie benötigen lediglich eine Netzwerkverbindung und den Treiber. Dann wird das YubiHSM in Domänen unterteilt, wobei jeder Server nur Zugriff auf die eigenen Private-Keys hat. Statt einfacher Passwörter kommen hier also Smartcards zum Einsatz, die eine starke Authentifizierung zum Beispiel in Microsoft-Umgebungen oder im Active Directory ermöglichen. Die iQSol HSA erlaubt zudem das einfache, menügeführte Erstellen von Backups und stellt durch zwei Nodes die Hochverfügbarkeit sicher. Hochsichere Technologie und damit einhergehend die sicheren Abläufe erleichtern die Administration ebenso wie die übersichtliche Benutzeroberfläche.

Höchstes Sicherheitslevel sorgt für Einsparungen

Ein geordnetes Zertifikatsmanagement ist Grundstein dafür, dass keine unnötigen Ausfälle auftreten oder sich häufen. Da allerdings mit der manuellen Abarbeitung der Zertifikate-Deadlines oder der Beseitigung der Stillstände immense Arbeitsaufwände einhergehen, sollte diese rein administrative Aufgabe in einem Tool abgebildet und automatisiert sein. Andernfalls besteht neben der Gefahr der Kostenexplosion auch die hohe Wahrscheinlichkeit, dass besonders global tätige Unternehmen mit einer unübersichtlichen Internet-of-Things-Umgebung (Maschinen, Geräte, Anlagen) rasch den Überblick verlieren.



Die Komponenten der Hardware Security App (HSA) von iQSol. (Bild: iQSol GmbH)

Leichter ausrollen und automatisch erneuern

Um Unternehmen das Zertifikatsmanagement weiter zu vereinfachen, verfügt die iQSol HSA daher neuerdings zudem über das „Automatic Certificate Management Environment“-(ACME)-Protokoll. Es ermöglicht das Zusammenspiel der Zertifizierungsstellen sowie der Server und damit die Bereitstellung einer kostengünstigen und sicheren Public-Key-Infrastruktur. Die dazu notwendigen Dienste laufen auf der iQSol HSA. Die ACME-Clients kommunizieren mit der HSA, die dann die Anfragen über den sogenannten Certificate-Authority-(CA)-Server abarbeitet. Zertifikate werden so über die Domänenvalidierung ausgerollt und automatisch erneuert. Das reduziert den Aufwand für die manuelle Verwaltung und gewährleistet jederzeitige Sicherheit.

Das Rundum-PKI-Sorglos-Paket

Natürlich kann man das Management auch ausgelagert und als Managed-Security-Service betreiben. Das macht vor allem dann Sinn, wenn die gesamte PKI erst aufgesetzt werden muss. Als eine der technisch anspruchsvollsten und höchstsensiblen Königsdisziplinen in der IT-Security gilt es auch hierbei, auf eine europäische Lösung und vertrauenswürdige Experten zu setzen. ■

Messestand iQSol
Halle 7, Stand 505
(Mitaussteller bei sysob IT-Distribution GmbH & Co. KG)
www.itsa365.de/de-de/companies/s/sysob-it-distribution-gmbh-co-kg/iqsol