



REFERENZ

Dienste für Menschen gGmbH

Schlüsselfaktor für Integrität: PKI mit HSM

Projektfeld

Dienste für Menschen mit Sitz in Esslingen betreibt als diakonischer Altenhilfeträger Pflegeheime, Wohnheime, ambulante Dienste und Diakoniestationen. In insgesamt 21 Einrichtungen in den Bundesländern Baden-Württemberg, Bayern und Sachsen werden mehr als 1.600 pflegebedürftige Menschen von rund 1.800 Mitarbeitenden gepflegt und betreut. Im betreuten Wohnen gibt es 350 Wohnungen. Acht ambulante Pflegedienste runden das Angebot ab. An den meisten Standorten sind mehrere Angebote zugleich vorhanden, so dass eine umfassende Betreuung angeboten werden kann nach dem Grundsatz: „Dienste für Menschen ist für uns Name und Anspruch zugleich.“

Und zuverlässig im Dienst der Menschen muss hier auch die IT stehen: als effizientes Fundament einer modernen Organisation mit knapp 100 Servern und VMs, rund 550 Clients und einer Public Key Infrastructure (PKI) zum gesicherten Zugriff auf digitale Ressourcen. An diese Erzeugung und Speicherung von Schlüsseln für Zertifikate werden seit Inkrafttreten der DSGVO allerdings besondere Anforderungen gestellt. Dazu kommt die Bedrohung durch neue Angriffsszenarien wie Spectre, Meltdown & Co. Um den Schutz sensibler Informationen zu gewährleisten, sind daher heute entsprechend solide Lösungen gefragt. Nun liegen die Prioritäten der „Dienste für Menschen gGmbH“ weniger im IT-Bereich, statt vielmehr auf dem sozialen Sektor. Somit ist die IT-Abteilung

dieses Kunden auch eher klein dimensioniert. Umso größer zeigen sich da dann die Ansprüche an den IT-Dienstleister – vor allem in Bezug auf Expertise, Flexibilität und Integrität. Alles Punkte, mit denen das Axians-Team in der langjährigen Zusammenarbeit immer wieder aufs Neue überzeugen konnte. Wie auch 2018 beim Projekt zur Etablierung einer neuen PKI mit Hardware Security Modul (HSM).

Projektanforderungen & Projektziele

Eine PKI ist mittlerweile obligatorischer Bestandteil praktisch aller Netzwerke. Als „Certificate Authority“ stellt sie hier digitale Zertifikate für die eindeutige Identifizierung von Personen oder Institutionen zur Verfügung. Zudem bietet die PKI Verzeichnis-Dienste zum Speichern oder zum Widerrufen von Zertifikaten. Bei der ersten Anfrage an Axians plante die „Dienste für Menschen gGmbH“ nun, ihre vorhandene PKI auf ein aktuelles Server-Betriebssystem zu adaptieren. In Zeiten der Virtualisierung lassen sich die gewachsenen Anforderungen an eine PKI jedoch nur mit Einsatz eines HSM wirklich sicher meistern. Die wesentlichen Vorteile dabei: Eine sichere Schlüsselverarbeitung und -speicherung innerhalb des HSM bzw. in Schlüsselcontainern, das umfassende zentrale Schlüsselmanagement mit Rollenmodell, die Immunität der kryptographischen Hardware vor Manipulationen sowie unterschiedliche Methoden der Authentisierung und Optionen zur Mehrfach-Authentisierung.

AUFGABE / ZIEL

- Etablierung einer neuen PKI im Sinne der DSGVO und als Schutz vor neuartigen Angriffsszenarien (Spectre, Meltdown etc.)
- Beibehaltung der eingesetzten 2-stufigen Architektur mit Offline-Root- und untergeordneter Online-Zertifikatsstelle
- Vereinfachung der Administration und Steigerung der Sicherheit durch verstärkten Zertifikats- bzw. Verschlüsselungseinsatz

LÖSUNG

- Implementierung des Thales SafeNet LUNA 7 Hardware Security Modul (vormals Gemalto) inkl. Backup-Device
- Integration in die ebenfalls neu implementierte 2-stufige PKI (Zertifikatsstellen Infrastruktur) auf Basis von Windows Server 2016
- Ablösung und Rückbau der bisherigen PKI

NUTZEN

- Erhöhte Sicherheit im Umfeld von kritischen personenbezogenen Daten
- Einheitliches und einfaches PKI-Management über alle Windows Server 2016 hinweg
- Maximale Absicherung des sicherheitskritischen Zertifikatsschlüssel-Materials in einer nicht manipulierbaren HSM-Hardware
- Ablösung der alten PKI ohne spürbare Änderung oder Unterbrechung für die Endanwender

Dienste für Menschen gGmbH

Konsequenterweise basierte also das neu angepasste PKI-Konzept von Axians auf diesen „gehärteten“, manipulationssicheren Appliances, die als dedizierte Krypto-Prozessoren die Verschlüsselungspraxis beim Kunden deutlich verbessern und gleichzeitig stark vereinfachen sollten.

Umsetzung

Zu Anfang stand für Axians eine detaillierte Evaluation der bisherigen PKI-Infrastruktur, speziell im Hinblick auf die bereits eingesetzten Zertifikatstypen. Anschließend folgte die Erstellung des detaillierten Konzepts zur Implementierung der neuen 2-stufigen PKI mit HSM. Das in Abstimmung mit dem Kunden entwickelte Lösungsdesign beinhaltete die Implementierung einer neuen PKI auf Windows Server 2016 – aber unter Beibehaltung der vorhandenen 2-stufigen Architektur mit einer Offline-Root- und der untergeordneten ausstellenden Online-Zertifikatsstelle. Entscheidend ist dabei das Verlagern der Erzeugung und Speicherung des Schlüsselmaterials. Also weg von der Software des Windows Betriebssystemes in eine manipulationsgeschützte Hardware. Dafür kam das Thales SafeNet LUNA 7 HSM (vormals Gemalto) zum Einsatz. Ein Schritt, mit dem auch gleich der Grundstein für weitere Sicherheitstechniken im Netzwerk der „Dienste für Menschen“ gelegt wurde – zum Beispiel einer Verschlüsselung von Datenbanken oder von virtuellen Maschinen. Denn: SafeNet HSMs lassen sich in bis zu 100 kryptografisch getrennte Partitionen unterteilen. Wobei jede dieser Partitionen wiederum als ein unabhängiges HSM fungiert. Zuvor musste allerdings eine andere Herausforderung gelöst werden. Da die „Dienste für Menschen gGmbH“ vorläufig nur ein einzelnes HSM anschaffen wollte, konnte standardmäßig

keine Hochverfügbarkeit implementiert werden. Stattdessen entwickelte Axians für die Zeit bis zur Beschaffung eines zweiten HSM eigens einen Modus zur Absicherung aus HSM-Backup und schnellem Hardware-Support. Spätestens 2019 soll dann die komplette HSM-Lösung planmäßig hochverfügbar performen – und auch die „Shielded VM“-Technologie implementiert werden.

Projektergebnis

Der Kunde erhielt primär eine hocheffektive PKI auf seinem aktuellen Betriebssystem – und dadurch auch ein vereinheitlichtes und komfortables Management über sämtlichen Windows Server 2016 hinweg. Im Endeffekt schafft die Lösung aber vor allem eine maximale Absicherung des sicherheitskritischen Zertifikatsschlüsselmaterials in einer gehärteten, nicht manipulierbaren HSM-Hardware. Für den reibungslosen Arbeitsablauf schließlich auch wichtig: Die Ablösung der bisherigen PKI erfolgte für die Endanwender beim Kunden ohne erkennbare Veränderung oder Unterbrechung. Und wie sehen es die Praktiker vor Ort in Esslingen? Ron Sliacky zieht als IT-Spezialist und Projektbeteiligter bei der „Dienste für Menschen gGmbH“ sein Resümee wie folgt: „Wir arbeiten für und mit Menschen – und daher besonders viel mit entsprechend sensiblen Daten. Die neue PKI Lösung in Zusammenarbeit mit Axians erhöht hier die Sicherheit jetzt auch durch einen verstärkten Zertifikats- und Verschlüsselungseinsatz. Dazu kommt die Vereinfachung der Administration durch das Anheben des PKI-Betriebssystems auf dieselbe Version, die wir ansonsten sowieso verwenden. Alles in allem also: Wieder einmal Maßarbeit vom bewährten Axians-Team. Vom ersten Konzept-Workshop bis zum Abbau der alten PKI.“

KUNDENINFO



Unternehmen: Dienste für Menschen gGmbH

Branche: Sozialwirtschaft/Altenhilfe

Sitz: Esslingen

Gründung: 1957

Dimension: Diakonischer Altenhilfeträger und Betreiber von Pflege- und Wohnstiften, ambulanten Diensten und Diakoniestationen. 350 Wohnungen und 21 Einrichtungen für über 1.600 pflegebedürftige Menschen. Rund 1.800 Mitarbeiter, 88,4 Mio. € Umsatz (2017)

Internet: www.dienste-fuer-menschen.de

ÜBER AXIANS

Die Unternehmensgruppe Axians in Deutschland ist Teil des globalen Markennetzwerks für ICT-Lösungen von VINCI ENERGIES. Mit einem ganzheitlichen ICT-Portfolio unterstützt die Gruppe Unternehmen, Kommunen und öffentliche Einrichtungen, Netzbetreiber sowie Service Provider bei der Modernisierung ihrer digitalen Infrastrukturen und Lösungen. In den vier Geschäftsbereichen IT Infrastructure, IoT & Analytics, Telekom & Carrier und Public Software sorgen Berater, Entwickler und Techniker dafür, das Leben von Menschen zu verbessern – etwa durch Cloud- und Data-Center-Infrastrukturen, Cybersicherheit, Unternehmens- und Breitbandnetze, IoT-Lösungen, Managed Services sowie führende Software für Abfallwirtschaft, Schüttgutindustrie, technischen Service und die öffentliche Verwaltung. Im Ranking der „besten Systemhäuser 2018“ auf Basis einer IDG-Umfrage zur Kundenzufriedenheit belegte Axians den zweiten Platz in Deutschland.

KONTAKT

E-Mail: referenzen@axians.de

axians.de

Stand 04/19