Szenario 2 - Fachverfahren

Pilotierung eines IRM-Systems im Rahmen der IT-Konsolidierung zur Sicherung eines Fachverfahrens einer Behörde

Version: 1.0

Status: Final

Autor: Tom Pasternak
Michael Riedel
Bastian Kammann

Stand: 29.09.2017

1 Ziele

- Zusätzlicher und granularer Ansatz zur logischen Trennung von Daten unterschiedlicher Behörden auf einem System durch Einsatz von Datei-basierter Verschlüsselung
- Vergabe detaillierter Berechtigungen für
  - den Zugriff auf Information auf Basis von Anwenderkreisen
  - Bearbeitung, Ausgabe und Weiterleitung von Informationen
  - Speicherung von Informationen
  - Gültigkeitsdauer von Informationen sowie deren Widerruf
- Auditierbarkeit von Zugriffen
- Einhaltung geforderter Compliance-Richtlinien

2 Ausgangslage

- IT-Konsolidierung des Bundes gemäß des Haushaltsausschuss-Beschlusses 2015
- Behörden betreiben spezifische, nur in der jeweiligen Behörde genutzte Fachverfahren (sog. „Private Services“)
- Zentralisierung der in den jeweiligen Behörden vorhandenen, bisher in Behörden-eigenem Netzsegment betriebenen Fachverfahren zu den IT-Dienstleistern des Bundes auf einer gemeinsamen Plattform
- Bereitstellung des Fachverfahrens durch den zentralen IT-Dienstleister des Bundes, ausschließlich für diese eine Behörde

3 Problemstellung

- Der Schutz, der bisher mittels in separaten Netzsegmenten betriebenen Fachverfahren und ihrer Informationen erbracht wurde, wird durch die Konsolidierung aufgehoben
- Die Informationen verschiedener Fachverfahren einzelner Behörden sind nicht mehr physikalisch voneinander getrennt
- Die durch Virtualisierung zu erreichende Trennung von Behörden genügt nicht den Trennungsvorgaben des BSI
- Ohne spezifische Erweiterungen ist eine Trennung nur mittels Dateisystemberechtigungen möglich
- Eine einzige Fehlkonfiguration kann dazu führen, dass Daten anderer Behörden sichtbar werden
- Der zentrale IT-Dienstleister hat unbeschränkten Zugriff, da die Dateien im Klartext vorhanden sind

4 Annahme des IST-Zustandes

Die nachfolgende Annahme ist lediglich fiktiv und dient im Weiteren einer Abschätzung von Aufwand, Kosten und Vorgehen.

- 1 Behörde nutzt ein eigenes Fachverfahren (Private Service)
- Das Fachverfahren dient der Anlage von Personenakten. Eine Akte enthält beispielsweise Passbild, Fingerabdrücke und weitere, personenbeschreibende Merkmale sowie eine Liste von Straftaten und Gerichtsurteilen. Der Anwender kann über ein Web-Interface in allen, gespeicherten Informationen spezifisch suchen und selektieren
- Der Datenimport erfolgt via API, Microservices und händischer Eingabe
- Das Verfahren wird auf einem Apache Webserver gehostet, der auf einem Server mit Unix Betriebssystem betrieben wird

- Die Daten werden serialisiert in einer relationalen ANSI SQL Datenbank gespeichert
- Das Fachverfahren erzeugt Reports in Form von PDF-, Excel- und Word-Dateien, die dem Anwender lokal am Arbeitsplatz angezeigt und zur Verfügung gestellt werden. Der Anwender kann diese Dateien auf seinem Arbeitsplatz zur weiteren Bearbeitung speichern. Die Informationen dürfen nur von ausgewählten Nutzern gedruckt oder per E-Mail versendet werden
- Die Web Applikation generiert die Report Daten und legt diese auf dem Server ab. Der Download erfolgt vom Client über den Server

5 Lösungsansatz

- Einführung eines IRM Systems im Rahmen der IT-Konsolidierung als Pilotierung für eine Behörde
- Die Architektur des IRM Systems darf keine Internet-Konnektivität haben. Alle Funktionen müssen On-Premise bereitgestellt werden
- Im ersten Schritt der Pilotierung soll ausschließlich die bisher vorhandene Trennung der Behörde durch Einführung einer Verschlüsselung aller auf den Servern oder lokal gespeicherten Dateien mit einem der Behörde zugewiesenem Schlüssel umgesetzt werden

6 Kontaktdaten

Tom Pasternak

Mobil: 0177 / 24 24 778

E-Mail: tom.pasternak@cassini.de

Michael Riedel

Mobil: 0151 / 11 44 38 63

E-Mail: michael.riedel@cassini.de

Bastian Kammann

Mobil: 0151 / 11 44 68 87

E-Mail: bastian.kammann@cassini.de