Szenario 1 - Fileservices

Pilotierung eines IRM-Systems im Rahmen der IT-Konsolidierung zur Sicherung zentral abgelegter Behördendaten

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
- Zentralisierung der in den jeweiligen Behörden vorhandenen, bisher in separaten Netzsegmenten betriebenen Dateiservern zu den IT-Dienstleistern des Bundes auf einer gemeinsamen Plattform
- Bereitstellung des Dienstes „Fileservice“ durch den zentralen IT-Dienstleister des Bundes

3 Problemstellung

- Der Schutz der bisher mittels in separaten Netzsegmenten betriebenen Dateiservern erbracht wurde, wird durch die Konsolidierung aufgehoben
- Die Informationen 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 mit 3 Standorten und 800 Anwendern mit Windows PCs
- Behörden-eigener Windows Fileserver
  - Windows Server 2012R2 Umgebung (incl. Active Directory)
    - 1 Forest
    - 3 Domänen
    - Bi-Direktionale Vertrauensstellungen zwischen den Domänen
    - Domänen und Domänenfunktionsebene: Server 2012R2
  - Berechtigungen über NTFS und File Share
  - 125 freigegebene Ordner mit insgesamt ca. 10 Millionen Dateien und einem Volumen von 1,5 TB
  - Pro Verzeichnis sind zwischen 10.000 und 250.000 Dateien in einer Größe zwischen 5 KB und 225 MB abgelegt (Typen: 60% Office Dateien (Word, Excel, PowerPoint, PDF), 30% Bilddateien, 10% andere Dateiformate)

- Dateiablage enthält nicht eingestufte sowie als VS-NfD eingestufte Dokumente

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 dem Fileserver gespeicherten Dateien mit einem der Behörde zugewiesenem Schlüssel umgesetzt werden. Personen- und gruppenspezifische Berechtigungen sollen mit dieser Pilotierung noch nicht eingesetzt 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