Thesenpapier
Verschlüsselte Dokumente in der vorarchivischen Phase

1 Ausgangslage

- Das GEVER-System (Axioma) erzeugt für jedes neue Dokument und bei jeder Dokumentänderung automatisch im Hintergrund ein PDF (Rendering). Der Inhalt des PDF-Dokuments wird über die Volltextsuche zugänglich gemacht.
- Das System unterscheidet eine aktive und eine passive Phase der Dossiers und Unterlagen.
- Die Passivierung erfolgt nach Abschluss eines Dossiers und ist Überführung in die passive Phase für die Aufbewahrung. Die Passivierung kann i.A. nur nach der erfolgreichen Umwandlung aller Dokumente in PDF (Rendering) erfolgen.
- Nach Ablauf der Aufbewahrungsfrist werden die ausgesonderten Dossiers dem Archiv abgeliefert
- Das Rendering erfolgt auf einem speziellen Server über einer Microsoft Office Client Installation mit PDF-Tools

2 Probleme

Der Rendering Service kann nicht alle Dokumente in PDF konvertieren; mögliche Gründe dafür sind:

a) Office-Dokumente sind passwortgeschützt
b) Outlook-Mails sind verschlüsselt
c) ZIP-Dateien sind verschlüsselt, so dass ihr Inhalt nicht gelesen werden kann
d) Office-Dokumente sind durch bedingte Obsoleszenz gesperrt
e) Office-Dokumente enthalten „untrusted macros“
f) Dokumente sind mit speziellen Verschlüsselungsprogrammen verschlüsselt
g) Technische Probleme

Das Fehlschlagen beim Rendern verhindert, dass das Dossier passiviert wird und die Aufbewahrungsfrist zu laufen beginnt, also in letzter Hinsicht wird auch die spätere Archivierung verhindert.

3 Möglicher Lösungsweg

1) Über die Windows Policy Einstellungen (Benutzerprofile) soll festgelegt werden, dass Office-Dokumente nur in aktuellen Formaten gespeichert werden können und dass die Office-Passwort-Option ausgeschaltet ist. (Argumentation: Office-interne Verschlüsselung gilt nicht als sicher). Damit wird die Verschlüsselung von Office-Dokumenten verhindert.
2) Auf dem Rendering Client sollen die Windows Policy Einstellungen sowohl alle Formate wie auch „untrusted macros“ erlauben. Damit können alle irgendwie konvertierbaren Dokumente (auch Altlasten) in PDF überführt und passiviert werden. Damit kein Sicherheitsrisiko mit diesem Vorgehen verbunden ist, muss der Rendering Client durch eine Firewall speziell abgeschottet werden, so dass nur Office-Dokumente in eine Richtung und PDF-Dokumente in die andere Richtung gelangen können (ähnlich wie bei einem Webserver in einer DMZ).

3) Verschlüsselte (Outlook-)Mails und mit einem ausgewählten Verschlüsselungsprogramm verschlüsselte Dokumente werden ohne Rendering passiviert. Das heisst, hier wird keine Umwandlung von Office- zu PDF-Dokumenten unternommen, Dossiers mit solchen Dokumenten können abgeschlossen werden und diese Dokumente gelangen verschlüsselt in die Phase der Aufbewahrung. Der Grund dafür ist, dass diese Dokumente auch während der Aufbewahrungsfrist verschlüsselt bleiben müssen und nicht durch die Volltextsuche erschlossen werden dürfen.
4) Dokumente, die weiterhin nicht gerendert und damit nicht passiviert werden können, werden mit Dokument/letztem Benutzer der Abteilung zur Entschlüsselung gemeldet. Ist ein Entschlüsseln/Rendern durch die Mitarbeiter nicht möglich (ältere Dokumente/fehlerhafte Dokumente/fehlende Passwörter) müssen diese Dokumente manuell für die Passivierung freigegeben werden können, weil sonst ein Dossierabschluss nicht möglich ist. Der Erfolg des Rendering kann im GUI erkannt werden.

Die vorgeschlagen Lösung führt unweigerlich dazu, dass verschlüsselte Objekte (Mails und Dokumente) in der Aufbewahrungsphase landen und dass diese am Ende der Aufbewahrungsphase für die Archivierung entschlüsselt werden müssen. Wie kann das gelöst werden, da möglicherweise weder das Passwort bekannt noch der Mitarbeiter, der mit diesen Dateien gearbeitet hat verfügbar ist?

- Bei der (Outlook-)Mail-Verschlüsselung gibt es offenbar einen Generalschlüssel, der dem IT-Betreiber zur Verfügung steht (ein Beispiel im Staatsarchiv belegt das). Grund dafür ist, dass E-Mail-Betreiber in der Lage sein müssen, die Mails in einem allfälligen Gerichtsverfahren unverschlüsselt zu präsentieren. Das Archiv muss also in Vereinbarungen mit dem E-Mail-Betreiber bzw. der IT Security sicherstellen, dass dieser Generalschlüssel bis zum Ende der Aufbewahrungsperiode zusammen mit der technischen Infrastruktur sicher aufbewahrt wird, so dass dann die Mails entschlüsselt werden können.
- Schwieriger ist das Problem der dokumenttypunabhängigen Verschlüsselung. Der beste Weg, der auch schon von gewissen Plattformbetreibern beschritten wird, ist der, dem Benutzer für die Verschlüsselung ein geeignetes, sicheres Verschlüsselungsprogramm zur Verfügung zu stellen, für das aber ein Generalschlüssel beim Kanton hinterlegt ist. Das Hinterlegen eines Generalschlüssels kann und soll durchaus kommuniziert werden. Nach Ablauf der Aufbewahrungsfrist haben wir das gleiche Vorgehen wie bei der verschlüsselten E-Mail.