Kundeninformation aus der Serie "electronic workflow in Unternehmen"

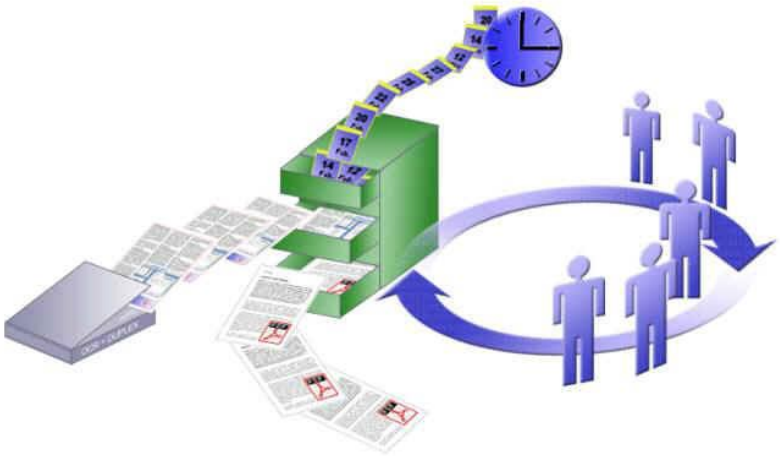
id newmedia KnowHow - für *Sie ...*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

electronic workflow
Teil 1



Technische Aspekte der rechtskonformen Archivierung elektronischer Vorgänge

Copyright © 2018-2025 id newmedia im Januar 2025

Über dieses Dokument

Dieses Dokument ist Teil 1 einer „White Paper“ Ausarbeitung von Ralf Kimmelmann, id-newmedia

Angesprochen sind Geschäftsleitungen von Verwaltungen des öffentlichen Dienstes und von kleinen bis mittelständischen Unternehmen der freien Wirtschaft.

Die Kaufmännischen Aspekte sind im White Paper, Teil 2

Positionspapier zur Einführung von Dokumenten Management Systemen
Kaufmännische Aspekte der Archivierung elektronischer Akten und Vorgänge

sowie im Folgepapier, Teil 3

Positionspapier zur Einführung von Dokumenten Management Systemen
Infrastruktur & Technologien
für die Archivierung elektronischer Akten
und Vorgänge

festgehalten, welche als Ergänzung für diese Ausarbeitung beizuziehen sind.

Im Folgenden werden spezifische Fachtermini in erheblichem Umfang verwendet. Dies ist zum Verständnis bei zukünftigen Diskussionen mit Planern und Lieferanten unumgänglich. Soweit möglich wurden deutsche Begriffserklärungen beigefügt.

Die 10 Grundsätze der Archivierung

Diverse gesetzliche Vorschriften (u.a. gdpdu, GOB, GOBS, …) zur elektronischen Archivierung lassen sich in 10 Grundsätzen zusammenfassen:

01. Jedes Dokument muss gemäß seiner gesetzlichen und betrieblichen Anforderungen aufbewahrt werden.
02. Es darf kein Dokument auf dem Weg ins oder im Archiv selbst verloren gehen.
03. Jedes Dokument muss unveränderbar archiviert werden.
04. Alle ändernden Aktionen im elektronischen Archivsystem müssen nachvollziehbar protokolliert werden.
05. Jedes Dokument muss eindeutig gefunden und reproduziert werden können.
06. Jedes Dokument muss zeitnah wiedergefunden werden können.
07. Jedes Dokument darf nur von berechtigten Benutzern eingesehen werden.
08. Jedes Dokument darf erst nach seiner Aufbewahrungsfrist vernichtet werden.
09. Die Anforderungen dieser Grundsätze müssen über technische Änderungen und Migrationen hinweg sichergestellt werden.
10. Die Erfüllung dieser Merksätze muss Dritten dargestellt werden können.

(Quelle: VOI [VOI Verband Organisations- und Informationssysteme])

Präambel

Gesetzliche Grundlagen zur Archivierung von Dokumenten

Ein Mindestmaß an Archivierung muss jedes – auch noch so kleines - Unternehmen betreiben. Im Handelsgesetzbuch (HGB, § 257) ist die Aufbewahrung von Unterlagen sowie die Aufbewahrungsfristen festgelegt, welche kaufmännischen Unterlagen für wie lange aufbewahrt werden müssen. Laut Gesetz müssen demnach folgende Dokumente aufbewahrt werden:

- Handelsbücher,
- Inventare,
- Jahresabschlüsse,
- Konzernabschlüsse und Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, empfangene und abgesandte Handelsbriefe und Buchungsbelege.

Diese Dokumente können mit Ausnahme der Eröffnungsbilanzen und der Abschlüsse, auch elektronisch archiviert werden. Diese elektronische Archivierung muss allerdings den Grundsätzen der ordnungsmäßigen Buchführung (GOB) entsprechen.

Wichtig: Diese Regelungen gelten auch für emails !

Gesetzliche Aufbewahrungsfrist

Die gesetzliche Aufbewahrungsfrist beläuft sich dabei auf sechs (6) Jahre für die Handelsbriefe und zehn (10) Jahre auf die übrigen Dokumente. Diese Aufbewahrungsfrist beginnt mit Abschluß des Kalenderjahres. In dieser Zeitspanne ist das Unternehmen verpflichtet auf seine Kosten den Erhalt und die Lesbarmachung sicher zu stellen (HGB §261). Auf Grund dieser Verpflichtung müssen auch Rückstellungen für die Archivierung dieser Dokumente gebildet werden.

Ähnliche gesetzliche Forderungen werden auch in der Abgabenordnung (AO, § 146) Ordnungsvorschriften für die Buchführung und für Aufzeichnungen und in § 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen gemacht.

Gesetzliche Anforderungen nach Branche

Zusätzlich zu diesen allgemeinen gesetzlichen Forderungen gibt es aber auch branchenspezifische Anforderungen an Dokumentation und Archivierung.

Gesetzliche Grundlagen zur Archivierung von emails

emails zum Beispiel, die für die Besteuerung von Bedeutung sind, sind nach den allgemeinen Vorschriften des § 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen der Abgabenordnung (AO) zu archivieren.

Aber auch emails, die Dokumente nach dem Handelsgesetzbuch (HGB) darstellen. Eine (elektronisch übersandte) email stellt ein originär digitales Dokument dar, das für den Datenzugriff im Originalformat maschinell auswertbar vorgehalten werden muss. Zum Beispiel eine Abrechnung der Reisekosten in einer Excel Datei.

Nach den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS, Abschnitt VIII. "Wiedergabe der auf Datenträgern geführten Unterlagen") sind auch emails als originär digitale Dokumente mit einem unveränderbaren Index zu versehen, unter dem das archivierte digitale Dokument eingesehen und verwaltet werden kann.

Entsprechende Paragraphen, u. A. :
§ 147 AO Ordnungsvorschriften für die Aufbewahrung von Unterlagen
§ 257 HGB Aufbewahrung von Unterlagen, Aufbewahrungsfristen

emails, die archiviert werden müssen, sind emails, die Dokumente im Sinne von Handelsgesetzbuch (HGB, § 257) "Aufbewahrung von Unterlagen, Aufbewahrungsfristen" darstellen. Das sind:

- Handelsbücher,
- Inventare,
- Jahresabschlüsse,
- Konzernabschlüsse und Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
- empfangene und abgesandte Handelsbriefe[1] oder
- Buchungsbelege.

[1]Ein Handelsbrief ist ein Schriftstück, das der Vorbereitung, Durchführung und dem Abschluß oder der Rückgängigmachung eines Geschäfts dient.

Aufbewahrungsfrist

Die Aufbewahrungsfrist für archivierte emails beträgt sechs Jahre für die Handelsbriefe und zehn Jahre für alle anderen oben genannten Mails. Die Frist beginnt mit dem Ende des Kalenderjahres. Diese Fristen sind im Handelsgesetzbuch (HGB) festgelegt.

Datenschutz

Wenn das Unternehmen dem Mitarbeiter die Nutzung des email-Postfachs auch zu privaten Zwecken gestattet, so wird dieses gegenüber dem Mitarbeiter als Telekommunikationsdienstleister im Sinne des Telekommunikationsgesetzes angesehen.

Das bedeutet für das Unternehmen, dass es den Pflichten des Fernmeldegeheimnisses unterliegt. Das Unternehmen darf dann nur noch im Rahmen der Sicherung der technischen Bereitstellung auf die Mail-Postfächer zugreifen. Ein automatisches Archivieren der emails ist also nicht erlaubt. Das Fernmeldegeheimnis greift allerdings nicht, wenn der Arbeitgeber es seinen Mitarbeitern untersagt, die email-Adresse auch privat zu nutzen.

Muss eine email elektronisch archiviert werden wenn man sie ausdruckt und in Papierform archiviert ?

Ja, da laut den Vorgaben in "Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme" (GoBS, VIII. "Wiedergabe der auf Datenträgern geführten Unterlagen") die Originalform archiviert werden muss. Die Archivierung der Originalform wird auch von § 147 Abgabenordnung (AO) gefordert. Man kann die email Archivierung also nicht umgehen, indem man alles ausdruckt und als Papierdokument ablegt.

Kosten und Aufwand

Die Aufwendungen und Investitionen – gerade für kleine Unternehmen – hängen maßgeblich von folgenden Faktoren ab :

- Größe des Unternehmens und des email-Verkehrs,
- Inhalt der emails, (Anhänge etc.),
- vorhandene IT-Systeme (Client, Server, eingesetztes email Programm etc.)
- Recherche und Zugriff auf die Emails,
- Komprimierung und Verschlüsselung,
- rechtliche Anforderungen und Datenschutz.

Quelle :
- Andreas Pfund
- AO
- GOB
- GoBS
- HGB

Inhaltsverzeichnis

1 Kurzfassung für Geschäftsleitungen
2 Aufbau und Zweck des Dokumentes
3 Grundlagen
3.1 Strategien der elektronischen Archivierung
3.1.1 Ausdruck
3.1.2 Technikmuseum
3.1.3 Emulation
3.1.4 Migration
3.2 Komponenten eines Archivsystems
3.2.1 Medienverwaltung
3.2.2 Indexdatenbank
3.2.3 Volltextdatenbank
3.2.4 Benutzerverwaltung
3.2.5 Cache
3.2.6 Clients
3.2.7 Server
3.3 Zusammenhang von organisatorischen und technischen Aspekten der elektronischen Archivierung
3.3.1 Auslagerungswürdige Datenbestände eines Vorgangsbearbeitungssystems
3.3.2 Aktiver und passiver Datenbestand
3.3.3 Sinnvolle Auslagerungszeitpunkte
3.3.4 Abgrenzung der (elektronischen) Langzeitarchivierung im Hinblick auf die Begriffe Archivierung und Aussonderung der Behördenwelt
4 SPEICHERMEDIEN UND –FORMATE
4.1 Speichermedien
4.1.1 Magnetische Speicher
4.1.2 Optische Speicher
4.1.3 Optomagnetische Speicherung
4.1.4 Weitere Systeme (Cloud & Co.)
4.2 Speicherformate
4.2.1 Formatkonvertierung
4.2.2 Formate zur Archivierung
5 GEWÄHRLEISTUNG DER KONSISTENZ ELEKTRONISCHER DATEN
5.1 Revisionssicherheit
5.1.1 Rekonstruktion von Indexinformationen
5.1.2 Zugriffsberechtigungen auf archivierte Objekte und Metadaten
5.1.3 Elektronische Signatur
5.2 Ausfallsicherheit von Archivsystemen
5.2.1 Hot-Standby
5.2.2 Backup
5.2.3 Caching
5.2.4 Medienkopien
5.3 Medienüberprüfung und Qualitätssicherung
5.3.1 Medienchecks auf physikalischer Ebene
5.4 Echtes Löschen archivierter Objekte
6 Berechtigungskonzepte
7 Migration
7.1 Vollständige Migration inkl. Medienwechsel, Benutzerverwaltung, Index
7.2 Migration ohne Wechsel der Medienverwaltung
8 Anhang
8.1 Die 10 Merksätze des VOI zur elektronischen Archivierung 50
8.2 Interpretation zu § 17 Signaturverordnung (SigV) durch ArchiSig (Zitat)
9 Quellenverzeichnis

1 Kurzfassung für Geschäftsleitungen

Der Begriff „Archivierung“ wird in diesem Dokument im technischen Sinne der Langzeitarchivierung auf Basis anderer Medien verwendet und ist damit nicht zu verwechseln mit der Aussonderung und Altaktenarchivierung im Sinne anderer Konzepte (z.B. Bayerisches Archivgesetz, BayArchivG).

Da elektronische Akten bis zum Ablauf der Aufbewahrungsfrist im Unternehmen / der Behörde verbleiben, sind die Anforderungen an die Verwahrung innerhalb des Unternehmens bzw. der Behörde zukünftig nicht nur unter dem Blickwinkel **des schnellen und zuverlässigen Zugriffs zum Zwecke der Bearbeitung** zu sehen, sondern auch unter den Aspekten **der langfristigen Sicherstellung der Lesbarkeit** und **der verlustfreien Reproduzierbarkeit** des elektronischen Schriftguts.

Bei einer Aufbewahrungsfrist von heute fünf, zehn und bis zu 30 Jahren sind die in diesem Organisationskonzept aufgestellten Forderungen daher grundsätzlich auch innerhalb des Unternehmens / der schriftgutverwahrenden Behörde von Bedeutung.

Mit dem Einsatz technischer Archivierungssysteme werden grundsätzlich folgende Ziele angestrebt :

- Revisionssichere Speicherung von Daten und Dokumenten
- Reduzierung der Kosten für Speichermedien
- Erhöhung der Performanz eines Vorgangsbearbeitungssystems.

Die Langzeitarchivierung von Dokumenten ist unter den o. g. Aspekten als ein wichtiger Bestandteil eines Vorgangsbearbeitungssystems (VBS[1]) anzusehen und muß im Rahmen der Weiterentwicklung unseres VBS die notwendige Beachtung finden.

[1]VBS Unter Vorgangsbearbeitungssystem wird unter anderem das von id-newmedia / moreOffice für die Gemeinde Gauting entwickelte und seit 18 Jahren betriebene

- von der Bayerischen Staatsregierung und der Bundesregierung ausgezeichnete –

eDOC electronic DOCument System verstanden.

Neben der heute noch vorherrschenden Technik der optischen Archivierung treten Systeme neu auf den Markt, welche für die Datenspeicherung nicht mehr die Verwendung von Wechseldatenträgern vorsehen, sondern eigene proprietäre Speichersysteme zur Verfügung stellen, die den Vorteil bieten, dass sie Daten unabhängig von zusätzlicher Hard- und Software sehr flexibel speichern können.

Dieser völlig neue Ansatz wird grundsätzliche Auswirkungen auf die notwendige Langzeitarchivierung elektronischer Daten haben, die heute jedoch noch nicht abzusehen sind.

2 AUFBAU UND ZWECK DES DOKUMENTS

Dieses Dokument wendet sich an alle Institutionen (Firmen jeder Größe, Öffentlicher Dienst), die sich im Rahmen der Einführung eines Vorgangsbearbeitungssystems mit der revisionssicheren und kostengünstigen Speicherung von Daten und Dokumenten und der Auswahl geeigneter Archivierungssysteme aktuell auseinandersetzen müssen.

Auch besondere organisatorische Aspekte der elektronischen Archivierung in der öffentlichen Verwaltung sollen dabei von Beginn an Berücksichtigung finden.

Nach einem kurzem Überblick über grundsätzliche Strategien der elektronischen Archivierung folgt eine Beschreibung der allgemeinen Komponenten eines technischen Archivsystems, welches die Basis für das weitere Verständnis der fachlichen Betrachtungen darstellt. Darüber hinaus zeigt **Kapitel 3** organisatorische Grundsätze der Langzeitarchivierung auf: So wird z. B. erläutert, welche Datenbestände eines Vorgangsbearbeitungssystems sinnvoll ausgelagert werden können und welche Zusammenhänge zwischen Langzeitarchivierung und der Aussonderung von Unterlagen bestehen.

Im **Kapitel 4** werden die bei der Langzeitarchivierung verwendeten Speichermedien und -formate mit ihren jeweiligen Charakteristika vorgestellt. Dieses Kapitel gibt auch Hinweise im Hinblick auf die Konvertierung bestehender Dateien in archivierungsfähige Formate. Dabei wird insbesondere darauf hingewiesen, welche Speicherformate für die jeweiligen Informationsarten eines VBS (Primärinformationen, Metainformationen, Bearbeitungs- und Protokollinformationen) geeignet sind.

Kapitel 5 beschreibt, wie über die Aspekte Revisionssicherheit und Ausfallsicherheit von Archivsystemen die Gewährleistung der Konsistenz elektronischer Daten und Dokumente ermöglicht wird. Um im Falle eines Ausfalls von optischen oder anderen Langzeitspeichermedien einen Informationsverlust zu verhindern oder zumindest zu reduzieren, werden in diesem Kapitel entsprechende Vorgehensweisen und technische Mechanismen erläutert. Die Speicherung von und der Zugriff auf archivierte Daten und Dokumente wird über Berechtigungen geregelt.

In **Kapitel 6** wird auf die in einem entsprechenden Berechtigungskonzept zu berücksichtigenden Aspekte eingegangen, die zur Umsetzung optimaler Archivierungsszenarien beitragen. Die Lebenszeit von elektronischen Archivsystemen ist i. d. R. viel kürzer als die Aufbewahrungsfrist der in ihnen gespeicherten Daten. Ein Wechsel zu einem Archivsystem eines anderen Anbieters bzw. ein Wechsel der Archivsystemtechnologie ist im Rahmen der vorgegebenen Aufbewahrungsfrist einzelner Behörden (z. B. 30 Jahre) unumgänglich.

Man kann nach Erfahrungswerten davon ausgehen, dass eine solche Migration alle fünf bis sieben Jahre ansteht. Damit ist es wichtig, bereits bei der Planung eines Archivsystems eine spätere Migration zu berücksichtigen.

Mögliche Migrationsszenarien weisen diesbezüglich den Weg und werden in **Kapitel 7** vorgestellt.

3 GRUNDLAGEN

Eine dauerhafte Verwahrung von Unterlagen von bleibendem Wert beim Schriftgut erzeugenden Unternehmen / bei der schriftguterzeugenden Behörde ist nicht mit dem Archivgesetz zu vereinbaren.

Allerdings verbleiben die Unterlagen bis zum Ablauf der Aufbewahrungsfrist innerhalb der entsprechenden Behörde. Da diese Frist bis zu 30 Jahre und mehr betragen kann, muß dem Schutz und der Sicherung der Unterlagen – auch aus Sicht der Archivbehörden (zuständiges Archiv) – eine hohe Priorität zukommen.

Aus diesen Anforderungen der Archive zur Langzeitarchivierung lassen sich folgende Schlußfolgerungen ableiten :

- Die Schriftgutablage innerhalb von Unternehmen, Behörden und Einrichtungen der öffentlichen Verwaltung ist unter keinen Umständen als Langzeitarchivierung von Dokumenten im Sinne einer zeitlich unbefristeten Endablage zu verstehen.

- Die schriftgutführenden und -verwahrenden Unternehmen und Behörden sind gleichwohl verpflichtet das anfallende Schriftgut für die Dauer einer ggf. mehrere jahrzehntelangen Aufbewahrungsfrist derart zu verwahren, dass eine vollständige und verlustfreie Reproduzierbarkeit des Schriftguts dauerhaft gesichert ist (z.B. Finanzsystem – Daten oder Warenwirtschaftssystem - Daten).

- Eine nachträgliche Verfälschung, Manipulation oder Löschung des zu verwahrenden Schriftguts ist durch geeignete Maßnahmen durch das Unternehmen / die zuständige Behörde bis zum Zeitpunkt der Übergabe/Übernahme an das ggf. zuständige Archiv zu verhindern.

- Die Festlegung der Aufbewahrungsfrist für Schriftgut erfolgt in Zusammenarbeit mit dem zuständigen Archiv.

- Um eine vollständige und verlustfreie Übergabe des Schriftguts an das zuständige Archiv zu gewährleisten, sind elektronische Daten in einem mit dem zuständigen Archiv abzustimmenden Format und unter Einhaltung eines abgestimmten Übergabe- bzw. Übernahmeverfahrens zu übermitteln.

Bei der Einführung von technischen Archivierungssystemen im Unternehmen / in der schriftgutverwahrenden Behörde sollte von Anfang an darauf geachtet werden, dass die genannten Anforderungen durch entsprechende Komponenten und Systeme der technischen Archivierung sichergestellt werden können.

3.1 Strategien der elektronischen Archivierung

Die mit der elektronischen Archivierung verbundenen Probleme werden durch die spezifischen Eigenschaften der digitalen Daten bestimmt.

Analoge Trägermaterialien können mit dem bloßen Auge oder unter Zuhilfenahme eines Lesegeräts gelesen werden. Computergenerierte Daten müssen dagegen zunächst vom Computer entziffert und mehrfach verarbeitet werden, bevor eine für das menschliche Auge lesbare Schrift dargestellt werden kann.

Um ein archiviertes digitales Dokument originalgetreu reproduzieren zu können, müssen u.a. folgende Bedingungen erfüllt sein:

- das Dokument muß in einem zur Archivierung geeigneten Datenformat gespeichert sein ...
- die Unversehrtheit des Datenträgers muß gegeben sein ...
- das passende Lesegerät muß zur Verfügung stehen ...
- die zugehörige IT-Infrastruktur muß vorhanden und einsatzbereit sein ...
- die verwendeten Daten-, Datei- und Speicherformate müssen bekannt ein und es müssen entsprechende Softwareanwendungen zur Visualisierung/Reproduktion zur Verfügung stehen.

Die Lesbarkeit der heute verwendeten Datenträger ist nur für einen beschränkten Zeitraum gewährleistet. Lesegeräte, Betriebssysteme und Anwendungsprogramme unterliegen Innovationszyklen, die sich nur auf wenige Jahre belaufen. Die nachfolgenden Programme und Geräte sind aber zumeist nicht vollständig abwärtskompatibel, d. h. die zuvor erstellten Dateien können nicht vollständig und unverändert dargestellt werden.

Ältere Formen maschinenlesbarer Datenträger wie z. B. Lochkarten können heute schon nicht mehr erfaßt und bearbeitet werden. Um daher elektronische Unterlagen langfristig verfügbar zu halten, müssen bereits wenige Jahre nach ihrer Entstehung geeignete Archivierungsmaßnahmen vorgenommen werden, welche - anders als bei analogen Materialien (z. B. Papier) - nicht hinausgeschoben werden können.

Zur Lösung des Archivierungsproblems wurden in den letzten Jahren verschiedene Strategien entwickelt, die sich grundlegend voneinander unterscheiden.

3.1.1 Ausdruck

Analoge Materialien sind wesentlich einfacher zu archivieren als elektronische Datenträger. Andererseits gehen bei dem Ausdruck einer elektronischen Datei sämtliche spezifischen Eigenschaften und Funktionalitäten verloren. Der Ausdruck eines elektronischen Datenträgers bietet sich daher nur in bestimmten Sonderfällen an.

3.1.2 Technikmuseum

Das zuständige Archiv kauft die notwendige Hard- und Software und hält diese vor. Diese Variante eignet sich ausschließlich für kurz- und mittelfristige Archivierungsvorhaben. Da behördliches Schriftgut nach Ablauf der Aufbewahrungsfrist ggf. dauerhaft in dem zuständigen Archiv gelagert wird, scheidet diese Option grundsätzlich aus.

3.1.3 Emulation

Die Originalhardware wird durch eine eigens zu erstellende Software imitiert. Künftige Computer verhalten sich dann wie die ursprünglich verwendeten und sind in der Lage, die gleichfalls archivierte Software zu lesen. Eine Emulation kann jedoch nur dann erfolgreich sein, wenn sämtliche Bestandteile problemlos funktionieren.
Der Ausfall einer einzelnen Komponente führt anders als bei der Migration zu dem Ergebnis, daß die Daten innerhalb des Systems nicht mehr gelesen werden können.

Dabei ist auch zu bedenken, dass bei einer Archivierung der Software auch deren Fehler (Bugs) archiviert werden. Bis heute liegen keine konkreten praktischen Erfahrungen mit dem Einsatz der Emulation zum Zwecke der Langzeitarchivierung vor.

3.1.4 Migration

Die Daten werden aus ihren bestehenden Formaten in kontinuierlichen Abständen in neuere Formate migriert (konvertiert). Zumeist werden dabei die auszulagernden Daten in ein Format migriert, das aufgrund seiner relativen Langlebigkeit nicht so häufig gewechselt werden muß, wie das zuvor benutzte proprietäre Ausgangsformat. Das neu überarbeitete Konzept zur Aussonderung elektronischer Akten empfiehlt bei der Festlegung eines solchen Formats die Beachtung der SAGA-Standards. Auf diese Standards beziehen sich auch die Formatempfehlungen in Kapitel 4.2.

Auch die Inhalte der Datenträger selbst müssen in kontinuierlichen Abständen auf neue Träger kopiert werden (Refreshing), damit ein Datenverlust aufgrund Materialfehler oder Alterung verhindert werden kann. Die Migration wird bislang von nahezu allen zuständigen Archiven, die bereits elektronische Dokumente übernommen haben, angewandt. Auch das Bundesarchiv sichert die langfristige Lesbarkeit elektronisch übergebener Daten durch ein Migrationskonzept.

Für die bis zu 30 Jahre und länger währende Aufbewahrungsfrist innerhalb von Behörden wird daher ebenfalls die Anwendung eines Migrationskonzeptes empfohlen, welches die sichere Aufbewahrung und die Reproduzierbarkeit der elektronischen Daten langfristig sicherstellt. Da die Daten nach Ablauf der Frist ggf. an das zuständige Archiv zu übergeben sind, sollten das Übergabeverfahren sowie die zu übergebenden Formate und Datenstrukturen möglichst frühzeitig mit dem zuständigen Archiv abgestimmt werden, damit Mehrfachmigrationen nach Möglichkeit vermieden werden.

Eine detaillierte Beschreibung zum Verfahren des Anbietens und der Übergabe an das zuständige Archiv findet sich in einem getrennt verfügbaren Konzept zur Aussonderung elektronischer Akten.

3.2 Komponenten eines Archivsystems

Die folgenden Komponenten sind - in der Regel - Bestandteile eines elektronischen Archivsystems.

3.2.1 Medienverwaltung

Damit eine Suchanfrage tatsächlich zum Erfolg führt, muß das System ermitteln können, an welchem Speicherort die angefragten Informationen abgelegt sind.

Die Information kann sich beispielsweise an einer genau festgelegten Stelle (ReadOffset) auf einer bestimmten WORM in einer bestimmten Jukebox befinden. Diese Information benötigt das System zwingend, um die angefragten Daten zur Verfügung stellen zu können.

Wird an diese Datenbank eine Anfrage in Form einer übergebenden Objekt-ID gestellt, so antwortet das System mit der genauen Angabe der physikalischen Speicheradresse.

Zusätzlich können in dieser Datenbank beschreibende Informationen über die Inhalte der verwalteten Medien strukturiert abgelegt werden (z. B. Mediennummer, Medientyp, Speicherkapazität und allgemeiner Inhaltsinformation, wie z. B. „Dokumente des Jahrgangs 2009“, etc.).

3.2.2 Indexdatenbank

Diese Datenbank enthält die gespeicherten Metainformationen zu den abgelegten oder archivierten Dokumenten.

Erst der Aufbau dieser Datenbank ermöglicht es den Nutzern eines Archivsystems, gezielt auf die gespeicherten Informationen zuzugreifen. Die Indexdatenbank enthält Grundinformationen (Grundindex und 'Unique Identifier') für einen eindeutigen Zugriff und die Verwaltung der Dokumente. Die Definition der zu erfassenden Metainformationen einzelner Objektarten stellt einen entscheidenden Arbeitsschritt bereits in der Konzeptionsphase eines elektronischen Archivsystems dar.

Die zu diesem frühen Zeitpunkt festgelegte Metadatenstruktur bestimmt wesentlich die zukünftigen Recherchemöglichkeiten innerhalb des Systems.

Sollte es im Laufe des Archivbetriebs zu einem Verlust oder einer Beschädigung der Indexdatenbank kommen, so hat dies zur Folge, daß der archivierte Datenbestand nicht mehr zugänglich ist. Die Dokumente auf den Speichermedien müssen daher so archiviert werden, dass die Indexdatenbank bei Datenverlust wiederhergestellt werden kann. Um ein hohes Maß an Sicherheit zu erzielen, wird vorausgesetzt, dass die Datenbank alle Aktionen vollständig protokolliert (Logging).

3.2.3 Volltextdatenbank

Die Volltextdatenbank beinhaltet komplette Volltextinformation der archivierten Objekte. Dies umfasst in der Regel sowohl die Metainformation als auch die Primärinformation von Dokumenten, sofern diese in einem gängigen Textverarbeitungsformat erstellt wurden (MS-Word, Excel, csv, etc.).

Handelt es sich bei den archivierten Dokumenten um ein NCI-Datenformat, so kann ein Volltextindex ggf. über den Einsatz von OCR-Software erstellt werden. Durch den (automatisierten) Aufbau einer Volltextdatenbank kann mit relativ geringem Aufwand ein mächtiges Recherchewerkzeug geschaffen werden, wenn die kostenintensive Erfassung differenzierter Metadaten zu Objekten nicht möglich ist.

Als Ergebnis einer Suche in der Volltextdatenbank liefert die Anwendung eine Liste derjenigen Objekte zurück, in denen die gesuchte Zeichenkette gefunden wurde.

3.2.4 Benutzerverwaltung

Das Archivierungssystem muß über eine eigene Benutzerverwaltung verfügen, die es erlaubt, eine möglichst feingliedrige Zuweisung von Nutzungsrechten auf einzelne Benutzer bzw. Benutzergruppen vorzunehmen. Die Benutzerverwaltung umfasst damit neben der Speicherung von Benutzerinformationen und Passwörtern auch die Verwaltung von Zugriffsrechten auf die archivierten Objekte und die Definition frei konfigurierbarer Nutzerprofile, die beispielsweise nur die Ausübung ganz bestimmter Funktionen des Archivsystems ermöglichen (z.B. Datenerfassung, Recherche, Administration).

3.2.5 Cache

Um einen schnellen Zugriff auf archivierte Objekte zu ermöglichen, die bereits einmal angefordert wurden, bzw. die einer definierten Gruppe häufig genutzter Objekte angehören, können diese Objekte in Kopie in einem Direktzugriffscache vorgehalten werden. Bei einer entsprechenden Suchanfrage muß das archivierte Objekt dann nicht zeitaufwendig z. B. über eine Jukebox bereitgestellt werden, sondern kann direkt aus dem Zwischenspeicher aufgerufen und am Client angezeigt werden. Unter dem Begriff „Cache“ wird somit die duplizierte Speicherung archivierter Objekte auf schnell zugreifbaren, temporären Medien (bspw. Festplattenpool) verstanden, die einen beschleunigter Zugriff auf archivierte Objekte unabhängig vom tatsächlichen Speicherort erlauben.

3.2.6 Clients

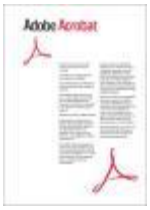
Ein Archivierungssystem verfügt über unterschiedliche Zusatzmodule, welche die zentralen Funktionalitäten (anbieterabhängig) an entsprechenden Client-Arbeitsplätzen zur Verfügung stellen.

3.2.6.1 Scan-Client

Am Scan-Client-Arbeitsplatz wird entsprechend vorbereitetes analoges Schriftgut über einen Scanner digitalisiert und in einem entsprechenden Format gespeichert. Je nach Ausstattung des Scan-Clients bestehen unterschiedliche Optionen zur Aufbereitung und Weiterverarbeitung der gescannten Images.

Hauptaufgabe des Scan-Clients ist jedoch die Umwandlung und Speicherung von analogem Papierschriftgut in ein digitales Datenformat. Dieser Prozeß kann üblicherweise in unterschiedlichen Automatisierungsstufen erfolgen.

3.2.6.2 Index-Client



Die in einem digitalen Datenformat vorliegenden Informationen werden an einem Indizier-Client um entsprechende Metadaten ergänzt, so daß die Informationen über Recherchefunktionalitäten wiederauffindbar sind (z.B. Adobe Acrobat ™).

Der Indexierung des zu archivierenden Schriftguts kommt im Zusammenhang mit der Erschließung des Datenbestands eine herausragende Bedeutung zu.

Auch die Indexierung des Datenbestandes kann in Abhängigkeit der Systemausstattung in verschiedenen Ausbaustufen automatisiert erfolgen, so können z. B. in anderen Anwendungen vorliegende Metadatensätze zur automatischen Indexierung Verwendung finden oder mittels Barcodetechnologie eine automatische Zuordnung und Verschlagwortung stattfinden.

3.2.6.3 Web-Client

Ein Web-Client ermöglicht die Nutzung des Archivierungssystems von einem mobilen Arbeitsplatz mit Internetanbindung.

Die Funktionalitäten des Web-Clients können in Abhängigkeit von der Systemauswahl einfache Recherchefunktionalitäten (Nutzung als mobiles Auskunftssystem) umfassen oder sogar eine mobile Datenerfassung und Archivierung ermöglichen.

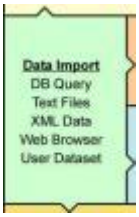
Die Hardwareanforderungen an einen Web-Client, wie auch die Lizenzkosten sind in der Regel deutlich geringer, als die eines Vollclients (→siehe auch Cloud-Dienste).

3.2.6.4 Viewer

Elektronische Archivierungssysteme sind heute in der Lage unterschiedlichste Dateiformate und Datenströme zu speichern.

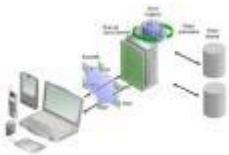
Bei einer sehr langen Aufbewahrungsfrist kann jedoch nicht davon ausgegangen werden, dass die Anwendungen, in denen die Datenformate erzeugt wurden, nach Jahren noch existieren. Trotzdem muß es eine Möglichkeit geben, die ggf. vor langer Zeit in einem proprietären Datenformat archivierten Daten mit ihrem ursprünglichen Erscheinungsbild zu reproduzieren. Der Viewer unterstützt eine Vielzahl von Datenformaten und ermöglicht so die Abbildung und Druckausgabe vieler gängiger Speicherformate, ohne dass die ursprünglichen DV-Anwendungen am Arbeitsplatz vorgehalten werden müssen.

3.2.6.5 Datei-Import-Client



Neben der Archivierung von Standard-Datenformaten, die heute vielfach über einfaches Drag&Drop den zu archivierenden Objekten hinzugefügt werden können, ist es auch möglich beliebige strukturierte Datenströme, die beispielsweise von Fachverfahren über eine Druckerschnittstelle erzeugt werden, automatisch zu erfassen, zu indexieren und in einem Format zu speichern, das die originalgetreue bildhafte Wiedergabe des ursprünglichen Ausgabeformats ermöglicht. Die Übernahme solcher Datenströme erfolgt in der Regel skriptgesteuert und erfordert eine individuelle Anpassung der Übernahmeskripte durch den Systembetreuer.

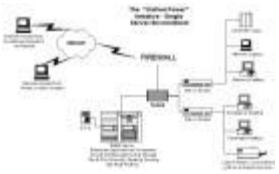
3.2.7 Server



Die Verwaltung, Ablage und Zwischenspeicherung der Daten eines Archivsystems erfolgt in einer Serverarchitektur, die die folgend beschriebenen Komponenten umfasst.

Je nach Umfang und Datenmenge der archivierten Daten, sowie in Abhängigkeit von der angeschafften Hard- und Software können verschiedene Dienste auf einem gemeinsamen Server installiert werden, wodurch die Zahl der einzusetzenden Server-Hardware verringert werden kann.

3.2.7.1 Cache-Server



Auf dem Cache-Server werden bereits einmal angeforderte Daten bzw. häufig benötigte Daten temporär für einen Direktzugriff vorgehalten. Der Zugriff auf gecachte Daten führt zu einer signifikanten Verkürzung der Zugriffszeiten auf archivierte Daten.

3.2.7.2 Dokumenten-Server

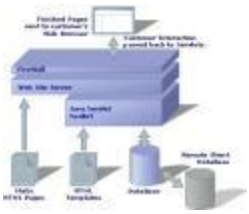
Auf dem Dokumentenserver werden elektronische Dokumente auf Magnetspeichermedien (NAS / SAN) für den Zugriff vorgehalten.

Auf dem Dokumentenserver können bei einer kontinuierlich anwachsenden Datenmenge jedoch nicht alle archivierten Dokumente auf Dauer vorgehalten werden. Auch in Zusammenhang mit Anforderungen an die Revisionssicherheit von Dokumenten, sollten diese nach einem bestimmten Zeitraum auf optische Speichermedien bzw. auf andere geeignete Speichersysteme ausgelagert werden.

3.2.7.3 Medien-Server

Ein Medienserver stellt sicher, dass die an verteilten Standorten und auf verschiedenen Speichermedien abgelegten Daten zuverlässig adressiert und zur Verfügung gestellt werden können. Zusätzliche Tools ermöglichen die Verwaltung und Strukturierung des Medienbestandes.

3.2.7.4 Datenbank-Server



Objektmetadaten und Volltextauszüge der archivierten Dokumente werden auf einem Datenbankserver vorgehalten.

Rechercheanfragen von Auskunftsarbeitsplätzen werden immer über den Datenbankserver bearbeitet. Die Aufgabe dieses Servers besteht in der Lieferung einer Trefferliste, in der alle Objekte referenziert werden, die der Suchanfrage entsprechen. Über die Objekt-ID referenziert der Medienserver anschließend den Speicherort der archivierten Objekte, die daraufhin geladen und an den Recherchearbeitsplatz übermittelt werden können.

3.2.7.5 Jukebox und Speichermedien

Ein Großteil der archivierten Daten kann auf optischen Speichermedien in so genannten Jukeboxen vorgehalten werden.

In einer Jukebox werden mehrere Speichermedien permanent für den Zugriff vorgehalten. Erfolgt eine Zugriffsanfrage an die Jukebox, so wird das entsprechende Medium ausgewählt und automatisch in das Leselaufwerk eingelegt.

Aufgrund des mechanischen Prozesses der Medienbereitstellung erfolgt die Auskunft am Recherchearbeitsplatz mit einer entsprechenden Zeitverzögerung.

3.3 Zusammenhang von organisatorischen und technischen Aspekten der elektronischen Archivierung

3.3.1 Auslagerungswürdige Datenbestände eines Vorgangsbearbeitungssystems

Die Bewertung der Auslagerungswürdigkeit von Datenbeständen eines VBS und damit die Entscheidung, ob Daten aus dem aktiven Datenbestand in ein technisches Archiv verlagert werden, kann nur durch die Etablierung **frühzeitig** einsetzender organisatorischer Festlegungen und Verfahren systematisch geregelt werden.

Innerhalb der öffentlichen Verwaltung empfiehlt z.B. das *DOMEA®-Konzept* die Definition der Aufbewahrungsfrist für Schriftgut bereits auf Aktenplanebene durch die aktenführende Stelle. Sie selbst ist dabei gehalten, die Fristen in enger Abstimmung mit dem zuständigen Archiv (z. B. Bundesarchiv) festzulegen. Innerhalb dieser Fristen ist das Schriftgut in der Behörde, also der Gemeinde Gauting, selbst für einen Zugriff aufzubewahren.

Das zuständige Archiv behält sich vor, nach Ablauf der Aufbewahrungsfrist in einem festgeschriebenen Verfahren über die endgültige Übernahme der Daten zu entscheiden.

Erst nach dieser endgültigen Verzichts- bzw. Übernahme-Entscheidung des zuständigen Archivs und ggf. der erfolgten Datenübergabe dürfen die Daten in der Behörde endgültig vernichtet werden.

Sofern für Teile des entstehenden elektronischen Datenbestandes keine Aufbewahrungsfrist definiert ist, so kann diese z. B. durch den zuständigen Bearbeiter selbst festgelegt werden.

3.3.2 Aktiver und passiver Datenbestand

Innerhalb des Datenbestandes wird unterschieden zwischen Daten, die für einen Direktzugriff vorgehalten werden (Aktiver Datenbestand) und Daten, die zwar noch in der Behörde aufbewahrt werden, die aber aufgrund ihrer selteneren Zugriffshäufigkeit bzw. aufgrund ihres Entstehungsdatums oder eines anderen definierten Kriteriums nicht für einen unmittelbaren Zugriff vorgehalten werden müssen (Passiver Datenbestand).

Auch die Daten des passiven Datenbestandes werden so verwaltet, daß sie jederzeit recherchierbar sind und auf Anforderung hin durch das System vollständig zur Verfügung gestellt werden können.

Ein Zugriff auf bzw. eine Recherche innerhalb dieses passiven Datenbestands ist also jederzeit möglich, die Bereitstellung der vollständigen angeforderten Information dauert ggf. jedoch länger, als dies bei einem Zugriff auf den aktiven Datenbestand der Fall ist. Zu beachten ist in diesem Zusammenhang, dass der Übergang von Objekten aus dem aktiven in den passiven Datenbestand nicht gleichbedeutend mit der Verlagerung von Daten aus dem VBS in ein technisches Archiv sein muß.

Die nachfolgende Abbildung verdeutlicht dies anhand der Unterteilung des aktiven Datenbestands, der in einen VBS-Bereich und den Bereich des VBS-Archivs gegliedert ist.

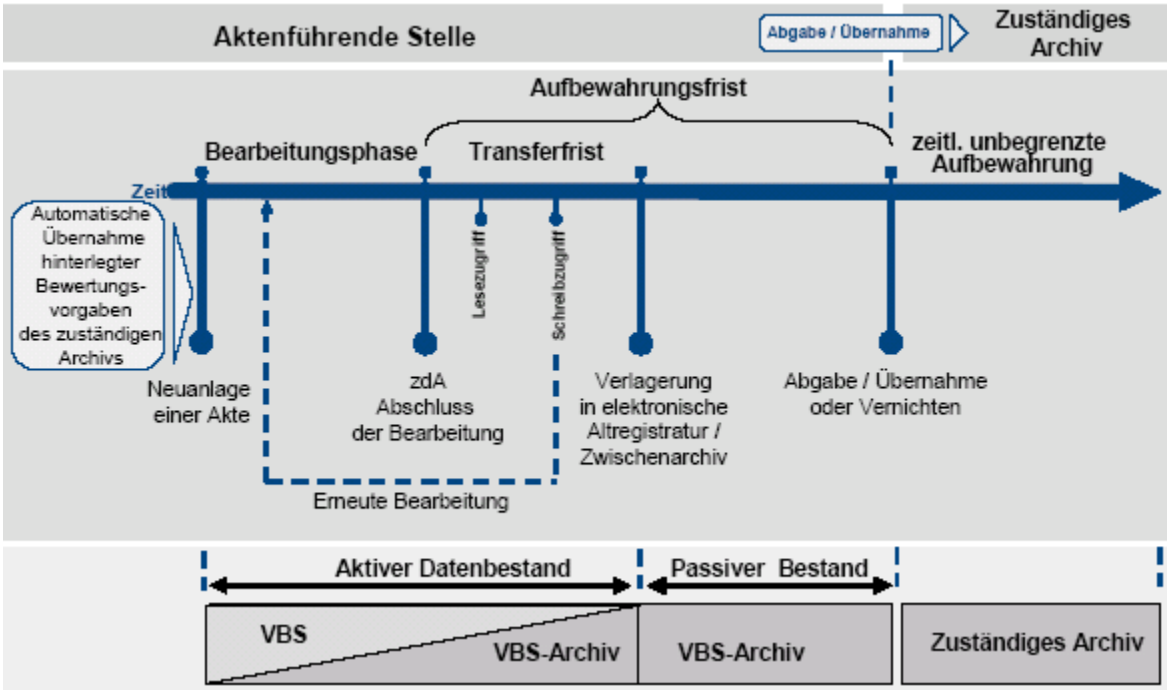


Abbildung 1: Lebenszyklus einer elektronischen Akte

Die Nutzbarkeit des aktiven Datenbestandes kann aus systemtechnischer Sicht begrenzt sein.

Mit dem Anstieg der Datenmenge im aktiven Bestand nimmt immer die Performance des Systems ab.

Dies kann zur Folge haben, dass das System im Extremfall nicht mehr sinnvoll genutzt werden kann.

Zur Lösung dieser Problematik kann es sinnvoll sein, den Zeitpunkt einer physischen Datenverlagerung an den Systemzustand zu koppeln.

Daten werden dann beispielsweise bei Überschreiten einer kritischen Datenmenge aus dem aktiven Bestand des VBS in den Bereich des VBS-Archivs verlagert. Trotz dieser Datenverlagerung verbleiben die Daten jedoch aus logischer Sicht weiterhin im aktiven Bestand.

Der aktive Datenbestand kann also sowohl im unmittelbaren Zugriff des VBS liegen, als auch bereits in das VBS-Archiv ausgelagert sein. Für beide Fälle gilt gleichbedeutend, dass die Daten noch in ihrem ursprünglichen Dateiformat vorliegen und jederzeit wieder in Bearbeitung genommen werden können.

Die Festlegung des Verlagerungszeitpunktes erfolgt in diesen Fällen nicht aus einer fachlichen Datensicht heraus, sondern aus einer rein technisch begründeten Sicht, die trotz großer unmittelbar vorzuhaltender Datenmengen im aktiven Bestand eine weitere Nutzung des Systems ermöglicht. Bei dieser Form der Verlagerung findet kein Übergang vom aktiven in den passiven Bestand statt.

3.3.3 Sinnvolle Auslagerungszeitpunkte

Mithilfe eines Metadatums kann der Zeitpunkt des Übergangs von Daten vom aktiven in den passiven Datenbestand bestimmt werden. Das Aussonderungskonzept z.B. der KBSt sieht hierfür das Metadatum „Transferfrist“ vor.

Die Dauer der Transferfrist kann aufgrund mehrerer Kriterien festgelegt werden. Welches Kriterium zur Verlagerung eines bestimmten Teildatenbestandes zugrunde gelegt wird, kann aus verschiedenen Sichten begründet sein.

3.3.3.1 Festlegung aus Nutzersicht

Der Nutzer entscheidet interaktiv, zu welchem Zeitpunkt Daten transferiert werden sollen.

Dieses kann sinnvoll sein, wenn Daten ausschließlich aus rechtlichen Gründen weiterhin im Unternehmen / in der Behörde verbleiben müssen und die (Nutzer-)Erfahrung gezeigt hat, dass auf diese Art von Daten zukünftig in der Regel nicht mehr zugegriffen werden muß.

In einem solchen Fall können die Daten bereits unmittelbar nach Abschluß der Bearbeitung in den passiven Datenbestand verlagert werden. Die Festlegung des Verlagerungszeitpunkts durch den Nutzer kann andererseits auch dazu führen, dass bestimmte Daten bis zum Ablauf der Aufbewahrungsfrist im aktiven Bestand des Systems verbleiben.

3.3.3.2 Festlegung auf Grundlage vordefinierter Kriterien

Ist der Verlagerungszeitpunkt von Daten durch festgelegte Regeln definiert, so kann das System durch Anwendung dieser Regeln einen Automatismus in Gang setzen, der die Verlagerung der betreffenden Daten ohne weiteren Benutzereingriff durchführen kann.

Vorgänge können beispielsweise in Abhängigkeit vom Vorgangstyp und dem Datum der zdAVerfügung nach einem festdefinierten Zeitraum (Transferfrist) aus dem aktiven Bestand in den passiven Bestand verlagert werden.

Der Zeitraum der Aufbewahrung im aktiven Bestand muß dabei nicht zwingend einer statischen Vorgabe entsprechen. Die Definition des Verlagerungszeitpunkts kann z. B. auch in Abhängigkeit vom letzten Zugriff durchgeführt werden.

Wird auf bestimmte Daten regelmäßig zugegriffen, so ist es durchaus möglich und auch gewünscht, dass diese Daten ggf. bis zum Ablauf der Aufbewahrungsfrist im aktiven Bestand des Systems verbleiben.

3.3.4 Abgrenzung der (elektronischen) Langzeitarchivierung im Hinblick auf die Begriffe Archivierung und Aussonderung der Behördenwelt

Der Begriff der (elektronischen) Archivierung ist nicht zu verwechseln mit den Begriffen der Archivierung und Aussonderung gemäß des DOMEA® - Konzepts in der Behördenwelt.

Grundsätzlich dient die elektronische Archivierung zur langfristigen, sicheren, authentischen und unverfälschbaren elektronischen Speicherung von Daten.

Unter dem Begriff der „Elektronischen Archivierung“ versteht man die Bereitstellung von beliebigen Informationen über einen Zeitraum von mindestens 10 Jahren.

Unter „revisionssicherer elektronischer Archivierung“ versteht man Archivsysteme, die nach den Vorgaben von §§ 239, 257 HGB, §§ 146,147 AO und GoBS beliebige Informationen sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar verwalten.

Die Anforderungen an ein System, das in Behörden zur elektronischen Archivierung genutzt wird, müssen zum einen der Definition einer revisionssicheren elektronischen Archivierung entsprechen (Urkundencharakter behördlichen Schriftguts) und zum anderen dem Begriff der „Elektronischen Langzeitarchivierung“ im Sinne der maximalen Aufbewahrungsfrist eines Schriftstücks im Unternehmen (10 Jahre + 12 Monate) bzw. in einer Behörde mit im Einzelfall bis zu 30 Jahren und länger genügen.

Nach Ablauf der (finanz-) behördlichen Aufbewahrungsfrist wird das verwahrte Schriftgut dem zuständigen Archiv angeboten und anschließend entweder der Behörde übergeben oder aber endgültig vernichtet (Firmen).

Das Verfahren der Aussonderung nach dem DOMEA – Konzept beschreibt detailliert die Vorgehensweisen im Aussonderungsverfahren, verzichtet aber bewußt auf die Vorgabe technischer Verfahrensweisen zur Sicherstellung einer revisionssicheren elektronischen Archivierung von Behördendaten im bisher genannten Sinne.

4 SPEICHERMEDIEN UND – FORMATE

Die Lesbarkeit der bisher verwendeten Datenträger ist nach den vorliegenden künstlichen Alterungsversuchen nur für **2** (Disketten) bis **15** (CD-R) **Jahre** gewährleistet.

Lesegeräte, Betriebssysteme und Anwendungsprogramme unterliegen Innovationszyklen, die sich ebenfalls nur auf einige Jahre belaufen. Die nachfolgenden Programme und Geräte sind aber zumeist nicht vollständig abwärtskompatibel, d.h. die zuvor erstellten Dateien können nicht vollständig und unverändert dargestellt werden. Ältere Formen maschinenlesbarer Datenträger wie z. B. Lochkarten können heute schon **nicht mehr erfaßt und bearbeitet** werden.

Um daher elektronische Unterlagen langfristig verfügbar zu halten, müssen bereits wenige Jahre nach ihrer Entstehung geeignete Archivierungsmaßnahmen vorgenommen werden, die anders als bei analogen Materialien (Papier) nicht hinausgeschoben werden können.

4.1 Speichermedien

Die im Folgenden beschriebenen Medien speichern Daten in digitaler Form.

Es sollten dabei Formatstandards gewählt werden, die aus heutiger Sicht auch für eine lange Archivierungsdauer Bestand haben.

Die elektronische Speicherung erfordert Hard- und Softwarekomponenten, die aufeinander abgestimmt sein müssen. Insbesondere bei sehr langen Speicherzeiträumen muß sichergestellt sein, dass die zum Lesen der Daten erforderliche Hardware noch langfristig verfügbar ist.

Heute finden drei grundsätzlich verschiedene Typen von Speichermedien Verwendung: Magnetische, Optische und Optomagnetische Speichermedien.

4.1.1 Magnetische Speicher (HDD, NAS, SAN)

Magnetische Speicher benützen remanente Magnetisierung für die Darstellung von Daten. Sie sind heute die am häufigsten verwendeten Speichermedien.

Sie können beliebig oft überschrieben werden und zeichnen sich durch schnellen Zugriff und große Speicherkapazität aus.

Sie weisen jedoch eine begrenzte Lebensdauer auf.

4.1.1.1 Magnetband

Das Magnetband wurde bereits um 1930 zur analogen Ton- und später auch zur Bildaufzeichnung entwickelt.

Speziell für die Datenspeicherung entwickelte Geräte bieten sehr hohe Speicherkapazitäten.

Nachteilig sind jedoch die hohen Initialkosten für die Bandgeräte, der geringe Standardisierungsgrad der Hard- und Software sowie die Empfindlichkeit des Bandes gegenüber mechanischen und elektromagnetischen Einflüssen.

Zur Vermeidung von Datenverlusten sind daher gelagerte Magnetbänder in regelmäßigen Abständen auf neues Material zu kopieren.

4.1.1.2 Festplatte / Serversysteme

Die Festplatte arbeitet wie das Magnetband mit elektromagnetischer Speicherung und ist fester Bestandteil jedes PCs sowie von Datenverarbeitungsanlagen. Vorteilhaft sind die gute Verfügbarkeit, der geringe Platzbedarf und die im Vergleich zum Magnetband geringen Initialkosten.

Die Festplatte eignet sich jedoch nur bedingt zur langfristigen Speicherung, da sie in der Regel fest mit dem PC verbunden bleibt und die gespeicherten Daten nach dem Lebensende des PCs auf andere Datenträger überspielt werden müssen. Die Sicherheit gegen Datenverlust ist relativ hoch, gegen Manipulationen hingegen ähnlich gering wie beim Magnetband.

Eine Festplatte besteht aus einer oder mehreren rotierenden Platten, einem Antrieb, einem beweglichen Schreib-Lesekopf, einer Steuerelektronik sowie einer Schnittstelle zur Verbindung mit dem Computer. Festplatten in Arbeitsplatzrechnern - zum größten Teil SATA-Platten – rotieren typischerweise mit Umdrehungsgeschwindigkeiten zwischen 5.400 und 7.200 Umdrehungen pro Minute. Bei solchen, die in Servern zum Einsatz kommen - oft SCSI- bzw. SAS-Platten - sind es in der Regel 10.000 oder 15.000 Umdrehungen pro Minute.

Die Kapazität einer Festplatte wird normalerweise in Gigabyte (GB) angegeben. Eine übliche Festplatte hat heutzutage eine Kapazität von 80 - 250 GB (März 2005).

Als Schnittstelle zum Computer wird heute hauptsächlich SATA verwendet. Immer häufiger werden aber auch universelle Schnittstellen wie Firewire oder USB für den Anschluß verwendet. Festplatten mit Fibre Channel-Interface sind teuer und finden daher hauptsächlich in Rechenzentren Verwendung.

Da auch Festplatten ausfallen können, zum Beispiel durch Aufsetzen des Schreib-Lesekopfes (Head-Crash), durch Fehler in der Steuerelektronik oder allgemein durch Abnutzung, werden in kritischen Anwendungsgebieten oft mehrere Festplatten zur Steigerung der Ausfallsicherheit, oft gleichzeitig auch zur Verbesserung des Datendurchsatzes, als RAID betrieben.

Da sich Festplatten nur bedingt für die langfristige Speicherung von Daten eignen, finden bis heute i.d.R. Wechseldatenträger für die dauerhafte Archivierung elektronischer Daten Verwendung. Aktuell treten am Markt Anbieter mit neuartigen Serversystemen auf, die elektromagnetische Speichertechnologie nutzen und die zur Langzeitarchivierung geeignet sein sollen.

Es handelt sich dabei um Lösungen, die aus mehreren zusammengeschalteten Rechnersystemen bestehen, von denen jedes eine bestimmte Anzahl von Festplatten via RAID5/6 unterstützt. Eine nicht offen gelegte Software fügt dieses System zu einem großen Speicherplatz zusammen und übernimmt auch die Speicherschutzfunktion.

Die Fälschungssicherheit der Daten, die wie bei der WORM über Hardware und Treiber realisiert wird, soll dabei über eine nicht offen gelegte Software gewährleistet werden. Dieser völlig neue Ansatz wird grundsätzliche Auswirkungen auf die Archivierung elektronischer Daten haben, die heute noch nicht absehbar sind. Erst durch eine dauerhafte Beobachtung der neuen Systeme in der Praxis wird sich zeigen, ob sich diese Art der Langzeitarchivierung zukünftig gegen die bisherige gängige Praxis der Verwendung von Wechseldatenträgern zur Datenarchivierung durchsetzen wird.

4.1.2 Optische Speicher

Optische Speicher sind von Laser abgetastete digitale Speicher.

Ein Laserstrahl tastet dabei berührungsfrei eine reflektierende Oberfläche ab, in der 1–2 Mikrometer feine Strukturen Daten speichern. Typische optische Speicher sind CD-ROM, DVD und WORM-Medien. CD-ROM / DVD zeichnen sich gegenüber magnetischen Festplattenspeichern durch eine begrenzte Speicherkapazität und eine langsamere Zugriffszeit aus. Sie können nur einmal beschrieben, aber mehrere Male gelesen werden (Read Only Memory).

Die Norm für CD-ROM ist ISO 9660. Im Vergleich mit Festplattenspeichern weisen sie jedoch eine bedeutend längere Lebenszeit auf. WORM-Speicher (Write Once Read Many) erlauben im Gegensatz zur CD-ROM-Speichertechnologie mehrfache Einlesevorgänge. Einmal beschriebene Plattensektoren sind jedoch nicht mehr überschreibbar.

WORM-Speicher werden vor allem im Zusammenhang mit umfangreichen Datenbeständen eingesetzt.

4.1.2.1 CD-ROM

CD-ROM (auch CDROM) ist die Abkürzung für Compact Disc Read-Only Memory.

Eine CD-ROM speichert digitale Daten (temporär) dauerhaft. Eine CD-ROM besteht aus einem Kunststoffträgermaterial mit Aluminiumbeschichtung. Die digitale Information wird auf einer spiralförmigen Spur aufgebracht. Es werden stellenweise Vertiefungen in die Beschichtung gepreßt, so entstehen nicht-reflektierende Stellen, so genannte Pits. Die unbeschädigten reflektierenden Stellen werden Lands genannt. Beim Lesen tastet ein schwacher Laserstrahl die gespeicherte Information ab.

Eine CD-ROM speichert zwischen 650 MB und 800 MB. Die Frage, wie lange die Daten dann effektiv gelesen werden können, ist offen. Schätzungen schwanken zwischen 10 und 50 Jahren, wobei die Alterung sehr stark von Temperaturschwankungen abhängig ist; auch Sonnenlicht läßt die Medien sehr viel schneller altern (im Idealfall sollten CD-ROMs konstant bei 20 Grad Celsius in absoluter Dunkelheit gelagert werden).

Sicher ist, dass Daten auf CD-ROM bedeutend kürzer als auf Stein, Papier oder Pergament halten.

Fast alle heutigen Computersysteme verfügen über ein CD-ROM-Laufwerk, mit dem die Daten gelesen werden können. Die CD-ROM ist eines der wenigen Speichermedien, die von verschiedenen Computersystemen gelesen werden können, vorausgesetzt die Daten wurden nach der ISO9660-Konvention aufgezeichnet.

Andere verbreitete Dateisysteme für CD-ROM sind z. B. RockRidge (UNIX) und Joliet (Windows). Unterstützt eine CD-ROM die El Torito-Spezifikation, so ist sie ein bootfähiges Medium.

Die CD-ROM ist neben dem Memory-Stick (USB-Stick) das (noch) am weitesten verbreitete Medium zum Verteilen von Software und Daten.

4.1.2.2 DVD

Bei der Digital Versatile Disc, kurz DVD, handelt es sich um einen Datenträger, der wie eine Compact Disc (CD) aussieht und ähnlich wie diese gelesen werden kann.

Die DVD ist die konsequente Weiterentwicklung der optischen Speichermedien, es ist die dritte Generation nach CD und MiniDisc.

Die Kapazität einer DVD liegt um ein Mehrfaches höher als bei einer CD. Ermöglicht wird dies durch eine höhere Datendichte und zwei parallele Datenschichten (Layer).

Bei einer DVD können zudem beide Seiten beschrieben sein, was die CD-Spezifikation nicht zuläßt.

Doppelseitige DVDs sind jedoch (noch) selten. Um diese nutzen zu können, benötigt man entweder Abspielgeräte, die mit zwei Leseeinheiten ausgestattet sind, oder man muß die DVD im Betrieb umdrehen.

Bei einer Kapazität von 4,7 Gigabyte (GB) für den Hauptlayer und 3,8 GB für den semitransparenten Layer ergeben sich folgende DVD-Typen (die Kapazitäten werden für die Benennung auf jeweils volle GB aufgerundet) :

- DVD-5: single side, single layer; 4,7 GB (eine Seite mit einer Schicht)
- DVD-9: single side, dual layer; 8,54 GB (eine Seite mit zwei Schichten)
- DVD-10: double side, single layer; 9,4 GB (zwei Seiten mit jeweils einer Schicht)
- DVD-14: double side, one side one layer, second side dual layer; 13,24 GB (eine Seite mit einer Schicht + eine Seite mit zwei Schichten)
- DVD-18: double side, dual layer; 17,08 GB (zwei Seiten mit jeweils zwei Schichten)

DVD-Brenner beherrschen meist nicht die "dual layer"-Technik.

Zudem verringert sich die Kapazität für den einen beschreibbaren Layer, so daß die Kapazitäten derzeit bei 4,6 GB für einmalig beschreibbare Rohlinge (DVD-R) und bei 4,5 GB für wiederbeschreibbare DVDs (DVD-RW) liegen.
Eine DVD kann Filme (DVD-Video), Musik und Ton (DVD-Audio) und Daten (DVD-ROM) enthalten.

Anders als bei der Compact Disc, bei der Musik anders gespeichert wird als Daten, wird eine DVD immer im Universal Disc Format beschrieben.

Das enorme Mehr an Speicher, gegenüber einer herkömmlichen CD ist die DVD aus zwei Gründen imstande zu speichern : zum einen sind die so genannten "Pits and Lands" sehr viel enger aneinander gereiht, als auf einer CD.

Das bedeutet vor allem, dass auf weniger Raum mehr Daten gespeichert werden können.

Zum anderen ist es möglich, auf einer DVD zwei Schichten an Daten übereinander zu lagern.

Zur Nutzung beider erweiterter Technologien braucht es filigranere und bessere Laser als zum Auslesen einer CD.

Um die zweite Datenschicht lesen zu können, muß der Laser dazu noch leicht anwinkelbar sein. Nur so ist es möglich, die untere ("verdeckte") Schicht lesen zu können.

4.1.3 Optomagnetische Speicherung

Die optomagnetische Speichertechnologie ähnelt der WORM-Technik.

Im Gegensatz zu dieser lassen sich auf optomagnetischen Speicherträgern Daten löschen bzw. wieder überschreiben.

Wie bei der WORM-Technologie sind verschiedene Normen vorhanden, die relativ rasch veralten. Es gibt heute keine wirklich praktikable Norm für die langfristige optische Speicherung von Informationen.

Angesichts der raschen Entwicklung auf dem Gebiet der Speichermedien und der sich dauernd wandelnden Normen werden also für die Aufbewahrung von digitalen Informationen über einen längeren Zeitraum in relativ kurzen Zeitabständen Konvertierungen erforderlich sein.

4.1.3.1 MO

Bei der magneto-optischen Technologie werden magnetische und optische Verfahren kombiniert. Die Speicherung der Daten erfolgt magnetisch.

Zum Tragen kommt hier eine Besonderheit des verwendeten Medienmaterials.

Im Gegensatz zu traditionellen magnetischen Speichern - wie Festplatten oder Magnetbändern - reicht zum Beschreiben magnetooptischer Medien das Anlegen eines Magnetfeldes allein nicht aus.

Aufgrund des verwendeten Oberflächenmaterials ist eine Magnetisierung, das heißt eine Datenbeschreibung oder eine Entmagnetisierung (Datenlöschung) erst dann möglich, wenn das Speichermedium erhitzt wird.

Dies passiert optisch, mit Hilfe eines Laserstrahls. Ein starker Laserimpuls erhitzt die Speicheroberfläche punktuell und kurzzeitig auf den sogenannten Curie-Punkt. Er kennzeichnet die Temperatur, bei der ein Material seine magnetischen Eigenschaften verliert. Durch Anlegen eines schwachen Magnetfeldes erfolgt jetzt eine Ausrichtung (Polarisierung) der Oberflächenbeschichtung.

Mit der Abkühlung des Punktes »erstarrt« die Polarisierung und die Daten sind gespeichert. Das Lesen der Daten erfolgt rein optisch mit Hilfe eines schwächeren Laserstrahls (ca. 10 % der Schreibintensität) durch Reflexion an der nun unterschiedlich polarisierten Speicheroberfläche.

Durch die auf einen kleinen fest definierten Temperaturbereich beschränkte Magnetisierungsfähigkeit können die Daten nicht - wie bei traditionellen magnetischen Speichermedien (Festplatte, Magnetband) - versehentlich oder mutwillig durch magnetische Felder zerstört werden. MO-Medien weisen deshalb eine extrem hohe Datensicherheit auf, die aufgrund der Tatsache, dass sich MO-Medien, ähnlich einer früheren 3,5-Zoll-Diskette in einer Schutzhülle (Cartridge) befinden, noch verstärkt wird. Diese verhindert zum einen mechanische Beschädigungen (Kratzer), zum andern federt sie beispielsweise Stürze vom Schreibtisch auf einen harten Untergrund ab.

MO-Laufwerke und Medien gibt es im 3,5-Zoll- und 5,25-Zoll-Format. Die maximale Kapazität liegt bei 2,3 bzw. 9,1 GByte. Im Gegensatz zu herkömmlichen magnetischen Laufwerken (Festplatten), bei denen der Magnetkopf über der Speicherplatte liegt, kann es bei MO zu keinem sogenannten "Head-Crash" kommen, der bei Berührung von Kopf und Platte fast immer den Verlust der gespeicherten Daten zur Folge hat.

MO – die Vorteile

MO-Disketten sind äußerst robust und langlebig. Daten können über 50 Jahre erfahrungsgemäß sicher archiviert werden.

MO-Speichermedien sind hochrobust, resistent gegen mechanische Beschädigung und Umwelteinflüsse wie Stoß, extreme Temperaturen, Staub oder Magnetfelder und lassen sich nach aktuellem Erkenntnisstand millionenfach wiederbeschreiben und lesen. MO-Laufwerke verhalten sich im Datenzugriff und bei der Datenübertragung ähnlich wie Festplatten. Auf die Daten kann jederzeit direkt und schnell zugegriffen werden.

MO-Laufwerke bieten volle Abwärtskompatibilität, d.h. neue Gerätegenerationen können auch alte MO-Medien mit einer Kapazität von 128 MB, 230 MB, 540 MB, 640 MB 1,3 und 2,3 GB beschreiben und lesen.

MO-Medien sind nach dem DICOM-Standard zertifiziert. DICOM steht für "Digital Imaging and Communications in Medicine" und ist ein weltweit gültiger Standard für den Datenaustausch von medizinischen Informationssystemen. Mit ihm können Bilder und Daten von unterschiedlichen bildgebenden und bildverarbeitenden Geräten untereinander ausgetauscht werden.

Die MO-Technologie ist nach CD-RW die günstigste Speicherlösung. Entscheidend ist dabei der Laufwerkspreis und der Preis der dazugehörigen Datenträger. "Alte" MO-Disketten können stets auf neuen MO-Laufwerken gelesen und beschrieben werden.

Auch wenn CD-RW die günstigste Lösung zu sein scheint, muß die Datensicherheit und das Einsatzgebiet berücksichtigt werden.

CD-RW und DVD-RW Datenträger sind nur limitiert wiederverwendbar.

Und während das technologische Entwicklungspotential für MO noch lange nicht ausgereizt ist, steht die CD am Ende ihrer Entwicklung und bei DVD sind bereits jetzt physikalische Grenzen sichtbar.

Mit einer Speicherdauer von bis zu fünfzig Jahren übertreffen MOs nicht nur die Haltbarkeit magnetischer Medien, sondern auch die optischer Medien wie CD oder DVD (üblicherweise fünf, qualitativ hochwertige Rohlinge zehn Jahre) deutlich. Magneto-optische Medien können quasi unbegrenzt oft gelöscht und wieder beschrieben werden.

Nachteile der MO-Technologie sind die im Vergleich zu anderen rein magnetischen bzw. rein optischen Technologien hohen Laufwerkspreise sowie die relativ geringe Schreibgeschwindigkeit. Da Wechselmedien häufig auch zur Datenverteilung benutzt werden, erweist sich auch der geringe Verbreitungsgrad der MO-Technologie als Defizit.

4.1.3.2 MO / WORM

WORM steht für "Write Once Read Many". Bei MO/WORM-Medien handelt es sich im Gegensatz zu normalen MO-Medien um nur einmal beschreibbare Datenträger. Es ist unmöglich, Daten unbemerkt zu manipulieren oder zu löschen.

Jede Veränderung an einem Dokument wird automatisch protokolliert, jede Version ist in ihrer Historie jederzeit wieder rückgängig zu machen.

Auch Viren können den gespeicherten Daten nichts anhaben. Jedes MO/WORM-Medium hat darüber hinaus eine eigene Signatur; ein Original läßt sich damit immer sicher von einer Kopie unterscheiden.

Umfangreiche Reportfunktionen geben jederzeit verläßliche Informationen über den Zustand und den Inhalt des MO/WORM-Mediums.

Der Vorteil der MO/WORM-Laufwerke liegt nicht nur in dem Plus an Datensicherheit und Performance gegenüber beispielsweise CD-R und DVD-R, anders als bei CD-R oder DVD-R kann der Anwender jederzeit Daten auf die WORM-Disketten übertragen. Eine Finalisierung oder Multisession von MO/WORM-Disketten ist nicht erforderlich.

MO/WORM-Laufwerke können aber auch normale MO-Medien lesen und beschreiben.

Die unkomplizierte Einbindung von MO- Wechselspeicherlaufwerken in Betriebssystemumgebungen wie MS WINDOWS XP/2000/2003, Mac OS und LINUX sowie die einfache Handhabung ohne spezielle Zusatzsoftware machen MO-Wechselspeicherlaufwerke zu universell einsetzbaren Multifunktions-Tools für die Datenverwaltung, den Datenaustausch und die Datensicherung/ Backup ebenso, wie für die fälschungssichere Dokumentenarchivierung mit der MO/WORM-Technologie.

Nachteile der WORM-Technologie sind die im Vergleich zu anderen rein magnetischen bzw. rein optischen Technologien hohen Laufwerkspreise sowie die relativ geringe Schreibgeschwindigkeit. Da Wechselmedien häufig auch zur Datenverteilung benutzt werden, erweist sich auch der geringe Verbreitungsgrad der WORM-Technologie als Defizit.

4.1.4 Weitere Systeme

4.1.4.1 Jukeboxen

Jukeboxen sind softwaregesteuerte, automatische Medienverwaltungssysteme für rotierende optische Speichermedien.

Eine Jukebox stellt damit im eigentlichen Sinne kein Speichermedium dar, sondern ein Gerät zur Bereitstellung einer Menge bereits beschriebener einzelner Speichermedien.

Die verwalteten Medien können dabei grundsätzlich in drei Zuständen des Zugriffs vorgehalten werden :

Online : das Medium befindet sich im Laufwerk.

Nearline : das Medium befindet sich in der Jukebox und wird von der Steuersoftware automatisch gefunden und in ein freies Laufwerk eingelegt.

Offline : das Medium muß auf Anforderung der Steuersoftware der Jukebox manuell zugeführt werden.

Eine mögliche Alternative zur Online-Speicherung auf einem Server bietet die Nearline-Speicherung. Hierunter ist die Verwendung eines Robots (Jukebox) zu verstehen, der automatisch auf Wechselträger zugreifen kann (zur Zeit z.B. Realisierung bei der Gemeinde Gauting). Im Unterschied zum Offline-Gebrauch erfolgt keine manuelle Eingabe des Datenträgers.

Allerdings verlängern sich die Antwortzeiten im Vergleich zu einer Online-Speicherung. Bei einer Auftragsarchivierung kann ein Zugriff auf die Daten durch die Archivverwaltung nur Online oder Nearline erfolgen. Es liegt dann an dem beauftragten Rechenzentrum, die günstigere Variante zu ermitteln.

Im Falle der Eigenarchivierung stehen jedoch alle drei Speichermöglichkeiten zur Auswahl an. Neben den bereits oben ausgeführten Überlegungen zur Sicherheit und Zugänglichkeit der Daten sind hier vor allem die auftretenden Kosten zu beachten.

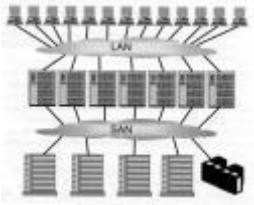
Berücksichtigt man nur die Hardware-Kosten, dann ist die Offline- Speicherung die günstigste Möglichkeit.

Nach der **V**ictorian **E**lectronic **R**ecords **S**trategy sprechen jedoch zahlreiche Gründe gegen eine Offline- und für eine Nearline-Speicherung:

- Verringerte Betriebskosten (manuelles Laden und Entladen entfällt).
- Niedrigere Kopier- und Migrationskosten.
- Geringere Chance einer fehlerhaften Etikettierung bzw. Reponierung der Medien.
- Kürzere Reaktionszeit auf Nachfrage nach Daten.
- Durchgehende Betriebsbereitschaft.
- Größere Zuverlässigkeit.

VERS kommt daher zum Ergebnis, dass Robots einen weitaus besseren Service und nach Berücksichtigung der Personalmittel auch niedrigere laufende Kosten bieten würden. Für Archive mit sehr kleinen Datenbeständen könnte alternativ eine Offline-Speicherung erwogen werden.

4.1.4.2 SAN



Ein **S**torage **A**rea **N**etwork ist ein sekundäres Netz parallel zu einem primären LAN.

Die Konsolidierung aller gespeicherten Daten wird so vereinfacht, da diese im SAN immer direkt verfügbar sind. In einem SAN ist der Massenspeicher für Daten nicht mehr nur ein Peripheriegerät an einem bestimmten Rechner oder Server. Gespeicherte Daten und Informationen sind das zentrale Element in den vernetzten Systemen. Dies wird durch die logische Zusammenfassung verteilter Datenspeicher in ein Gesamtsystem, das SAN, erreicht.

Mit einem **SAN** lassen sich die stetig steigenden Datenfluten besser bewältigen, die vorhandenen Storage-Kapazitäten besser ausnutzen sowie übergreifende Backup-Konzepte realisieren. SAN tragen weiterhin zur Verbesserung der Datenverfügbarkeit und zur Datensicherheit bei, bieten eine höhere Performance und ermöglichen problemlose Erweiterungen.

Zu den geldwerten Vorteilen von Speichernetzwerken zählt nicht zuletzt auch das einfachere, unternehmensweite Daten-Management. Die Speichersysteme tauschen ihre Daten auf direktem Wege aus, ohne eine Belastung des primären LAN. Die Datensicherung kann im SAN bei laufendem Betrieb erfolgen. In vielen Anwendungen wird erst durch den Einsatz eines SAN eine komplette, zeitnahe Datensicherung im laufenden Betrieb möglich.

In einem SAN haben alle Server Zugriff auf alle Daten und den gesamten freien Datenspeicher. Die Datenspeicher sind eine von den Servern getrennte eigene logische Einheit.

Somit kann ein gerade freier Server die vom Client angeforderten Daten aus dem Datenspeicherpool bereitstellen. Redundante Wege zwischen Daten und Anwender beugen möglichen Ausfällen oder Datenstaus vor.

Im SAN wird der gesamte Speicher, unabhängig von seinem physikalischen Standort oder einem bestimmten Betriebssystem, zentral verwaltet und gegebenenfalls zu virtuellen Einheiten zusammengefaßt. Die Speichereinheiten können dabei an unterschiedlichen Orten stehen.

Es gibt jedoch keine einheitliche SAN-Lösung, die für alle Systemumgebungen gleichermaßen geeignet ist. Bevor eine bestimmte SAN-Topologie realisiert wird, muß daher exakt bestimmt werden, wie diese Umgebung, die das SAN unterstützen soll, aktuell aussieht.

Weiterhin müssen auch zukünftige Entwicklungen mit einbezogen werden.

Auf der Basis einer solchen Bestandsaufnahme lassen sich dann Kriterien für die Wahl der passenden Switching-Komponenten und der optimal zugeschnittenen SAN-Topologie ermitteln.

4.1.4.3 Archivieren in der Cloud

Cloud-Dienste sind Segen und Fluch zugleich und eigentlich zur sicheren Archivierung von Unternehmensdaten / Behördendaten **nicht geeignet**.

Cloud-Speicherdienste erfreuen sich bei Unternehmen sowie privaten Nutzern großer Beliebtheit. Schließlich helfen sie, Dateien unabhängig von einem Gerät immer dabei zu haben sowie vor Verlust durch einen Gerätedefekt zu schützen. Die meisten Anwender nutzen dafür bekannte Dienste wie Dropbox, Google Drive & Co., die eine einfache Konfiguration und Einbindung in bestehende Systeme bieten.

Seit den zahlreichen Enthüllungen über die Arbeit internationaler Geheimdienste setzen jedoch immer mehr Nutzer und Firmen auf eigens betriebene Cloud-Server, um die Sicherheit zu erhöhen. Doch das ist – wie sich zeigt – nicht immer erfolgreich: wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) nämlich mitteilt, weisen in Deutschland mehr als 20.000 Internet-Speicher gefährliche Sicherheitslücken auf.

Gelingt es einem Angreifer, durch Ausnutzung einer Lücke auf den Server zuzugreifen, erhält er Einsicht in sämtliche Daten. Im schlimmsten Fall läßt sich sogar die Kontrolle über den Server gewinnen.

Cloud-Provider betonen gern die hohen Sicherheitsstandards in ihren Rechenzentren. Amazon Web Services (AWS) etwa wirbt mit „hervorragender Sichtbarkeit und Kontrolle“, „tief integrierten Services“ und „höchsten Standards für Datenschutz und Datensicherheit“. Als Beweis für diese Aussagen werden zahlreiche Sicherheitszertifikate ins Feld geführt. Das Unternehmen listet auf der Seite „AWS-Compliance-Programme“ rund 40 globale, regionale und nationale Zertifikate auf, welche die Sicherheit und Regelkonformität der Services belegen sollen.

Tatsächlich bieten die Rechenzentren der Cloud-Anbieter ein hohes physikalisches, technisches und organisatorisches Sicherheitsniveau.

Das Problem ist nur: es nützt nichts - im Gegenteil.

Die vollmundigen Versprechen der Provider wiegen die Anwender in trügerischer Sicherheit. Obwohl alle großen Public-Cloud-Anbieter die „gemeinsame Verantwortung“ (Shared Responsibility) von Provider und Kunde betonen, ignorieren viele Anwender ihren Teil der Abmachung. „In vielen Fällen wird davon ausgegangen, dass der Cloud-Anbieter auch für die Security zuständig ist“, sagt Roger Scheer, Vertriebsvorstand beim Cloud-Security-Service-Provider Veronym. „Das ist aber nur sehr eingeschränkt der Fall.“

Einer vom Sicherheitsunternehmen Ermetic in Auftrag gegebenen IDC-Studie zufolge verzeichneten fast 80 Prozent der befragten US-Unternehmen in den vergangenen 18 Monaten mindestens eine cloudbasierte Datenpanne, bei 43 Prozent gab es sogar mehr als zehn Vorfälle. Nur ein Bruchteil davon wird bekannt - oft erst Jahre nach dem Datendiebstahl.

Zusammenfassung

Auf dem Markt existieren eine Vielzahl unterschiedlicher Speichermedien für digitale Daten. Die Eignung der unterschiedlichen Medientypen für eine revisionssichere Langzeitarchivierung von Daten im Sinne der Archivgesetze kann zunächst in Bezug auf die zugrundeliegende Speichertechnologie bewertet werden.

Magnetische Speicher erscheinen unter diesen Aspekten ungeeignet, da ein unbeabsichtigtes Löschen der Daten nicht ausgeschlossen werden kann und auch eine Manipulation von Daten leicht möglich ist. Auch wenn magnetischer Speicher bspw. in Bezug auf Zugriffsgeschwindigkeit, Speicherkapazität und Verwaltung/Reorganisation von Daten unbestreitbare Vorteile gegenüber den übrigen Medientypen und Technologien bieten, so kann eine Verwendung im Bereich der langfristigen Datenarchivierung heute nicht empfohlen werden.

Wenn es jedoch gelingt, eine überzeugende Lösung für die genannten Problembereiche zu entwickeln und sich eine entsprechende Produktlösung langfristig am Markt etablieren kann, so könnte dies die unter Kosten-, Nutzen- und Sicherheitsaspekten geeignete Lösung der Zukunft darstellen.

Optische Speicher können nur einmal beschrieben, aber mehrere Male gelesen werden (Read Only Memory). Damit haben sie aus Sicht der Datensicherheit einen entscheidenden Vorteil gegenüber der Magnetspeicher-Technologie. Da bei der Betrachtung von Aspekten der revisionssicheren Archivierung die Nachteile der optischen Speicher im Vergleich zu Magnetspeicher in Hinblick auf Zugriffsgeschwindigkeit, Speicherkapazität und der Handhabbarkeit in Bezug auf Datenreorganisation keine Rolle spielen, ist optische bzw. magneto-optische Speichertechnologie im Marktsegment der elektronischen Archivierung heute der Magnetspeicherung vorzuziehen.

Optische wie auch magneto-optische Speichertechnologie erfüllt die Anforderungen an eine revisionssichere Langzeitarchivierung aus datensicherheitstechnischer Sicht am besten. Unter Beachtung weiterer relevanter Aspekte, wie der Robustheit und der Lebensdauer der Speichermedien sowie der bisherigen Erfahrung und Erprobung von Medien im Zusammenhang mit der Langzeitarchivierung elektronischer Daten wird die Verwendung von WORM-Medien empfohlen.

Auch die Verwendung einmal-beschreibbarer CDs oder DVDs kann in Betracht gezogen werden, jedoch stehen diese Medien in Bezug auf Robustheit und Lebensdauer gegenüber der WORM zurück. Entscheidet man sich dennoch für den Einsatz von CD bzw. DVD für die Datenspeicherung, so sind Aspekten wie Medienchecks auf physikalischer Ebene und Reorganisation der Daten hohes Gewicht beizumessen (vergl. Kap. 5.3).

4.2 Speicherformate

Um eine **langfristige** Lesbarkeit der archivierten Dokumente sicherzustellen, sollten grundsätzlich nur **Standardformate** und **Standardkomprimierungsverfahren** eingesetzt werden. Spezifische Dateiformate, deren langfristige Verwendbarkeit im Sinne einer vollständigen Reproduzierbarkeit und Darstellbarkeit nicht sichergestellt werden kann, müssen daher vor der Archivierung in ein entsprechendes Format konvertiert werden.

4.2.1 Formatkonvertierung

Innerhalb des aktiven Datenbestandes eines Vorgangsbearbeitungssystems sollten elektronische Dokumente in dem Format vorgehalten werden, in welchem sie ursprünglich erstellt wurden (z.B. name.DOCX).

Auf diese Weise können die Dokumente bei einem späteren Zugriff innerhalb der Originalanwendung, mit der sie erstellt wurden weiterverarbeitet werden und beispielsweise als Vorlage für neu zu erstellende Dokumente Verwendung finden.

Nach einer bestimmten Aufbewahrungsfrist im System ist es zweckmäßig eine Konvertierung in ein Format durchzuführen, welches eine dauerhafte originalgetreue Reproduzierbarkeit der Inhalte garantiert (z.B. PDF).

In diesem Zusammenhang ist insbesondere zu beachten, dass mit der Formatkonvertierung eines elektronischen Dokuments dessen Struktur verändert wird und eine ggf. vorhandene elektronische Signatur dadurch ihre Gültigkeit verliert.

In der Neufassung des Aussonderungskonzepts wird empfohlen die Formatkonvertierung automatisch zum Zeitpunkt der Verlagerung eines Dokuments von der elektronischen Registratur in die elektronische Altregistratur durchzuführen.

Der Zeitpunkt der Verlagerung wird dabei auf Basis des hinterlegten Metadatums der Transferfrist bestimmt. Spätestens jedoch zum Zeitpunkt der Auslagerung der elektronischen Dokumente auf Medien zur Langzeitdatenspeicherung sollte eine Formatkonvertierung in ein einheitliches Format erfolgen.

Grundsätzlich besteht bei der Konvertierung die Möglichkeit, dass elektronische Dokumente weiterhin zusätzlich in ihrem Originalformaten gespeichert bleiben und auf diese Weise auch nach der Verlagerung in den passiven Datenbestand innerhalb der Anwendung, in der sie ursprünglich erstellt wurden, weiterverwendet werden können.

Als geeignete Formate zur Speicherung von Primärinformationen elektronischer Dokumente haben sich das TIF-Format oder das PDF-Format bewährt.

Für das Speichern vom Metadaten wird grundsätzlich ein klarschriftlesbares TXT(ASCII)-Format empfohlen.

Mit Blick auf die zunehmende Bedeutung des interbehördlichen Datenaustauschs, die diesbezüglichen Standardisierungsbemühungen und die Weiterentwicklung des DOMEA®-Organisationskonzepts wird außerdem empfohlen, die Metadaten von Akten, Vorgängen und Dokumenten direkt in einheitlichen, vorgegebenen Datenstrukturen zu speichern.

Auch für Bearbeitungs- und Protokollinformationen sollten die entsprechenden XML-Datenstrukturen zukünftig generiert und gespeichert werden können.

4.2.2 Formate zur Archivierung

Die nachfolgend aufgeführten Formate orientieren sich an den Vorgaben des SAGA-Standards, der Empfehlungen an Entscheider aus den Bereichen Organisation und Informationstechnik in der deutschen Verwaltung ausspricht.

Ziel von SAGA ist es, durch die Vorgabe von Standards, Formaten und Spezifikationen die Interoperabilität von Informations- und Kommunikationssystemen zu erreichen. Für die dauerhafte Speicherung von Dokumenten sollten nur einige wenige Formate zur Anwendung kommen.

Das Nebeneinander unterschiedlichster Formate in einem elektronischen Archiv erhöht zunehmend die Gefahr, das einzelne Datentypen in Zukunft nicht mehr originalgetreu reproduziert werden können.

Zu unterscheiden ist bei den zu archivierenden Daten zwischen der Bildinformation eines Dokuments einerseits und der Inhaltsinformation andererseits.

Während SAGA in Bezug auf die Bildinformation mehrere Formate angibt, beschränkt sich der Standard für die Speicherung von Metadaten / Textinformation auf die Empfehlung für den erweiterten ASCII-Datensatz. Für die Langzeitarchivierung kommen folgende Dateiformate in Frage:

TIF

Das “Tagged Image File Format” erlaubt das informationsverlustfreie Speichern von Graphikinformationen. (*.tif) ist ein Dateiformat für Rastergraphiken, wobei verschiedene Formatierungen es Anwendungen erlauben, Teile der Graphik zu verarbeiten oder zu ignorieren.

Die Verwendung des TIF-Formats ist immer dann angezeigt, wenn die Graphikinformation von entscheidender Bedeutung für die Aussagekraft eines Dokuments ist und keine Notwendigkeit besteht, die Textinformation des Dokuments als intelligente Information (Volltextauszug) und als Bestandteil der Datei mitzuspeichern.

Das TIF-Format eignet sich damit insbesondere für das Speichern von nur in Papierform vorliegenden Dokumenten, die durch Scannen in ein digitales Datenformat überführt werden und die anschließend manuell indexiert werden.

JPEG

Ein Standardformat für das Speichern und den Austausch von Bildern stellt das Format Joined Photographic Experts Group (*.jpg) dar. Es ermöglicht das Ändern des Komprimierungsgrades und die Angabe der Dichte, sodass ein Kompromiss zwischen Dateigröße und Qualität in Abhängigkeit vom Verwendungszweck gefunden werden kann. Es wird eine Farbtiefe von 16,7 Mio. Farben unterstützt.

Die Verwendung des JPEG-Formats kann alternativ zum TIF-Format gewählt werden, sofern die genannten Vorteile des JPEG-Formats gegenüber der Speicherung im TIF-Format für die Dokumente von Belang ist.

Gründe für die Speicherung der Bildinformation im JPEG-Format können die Anforderung an eine definierte Bildauflösungsstufe von Dokumenten sein, die geforderte Einhaltung eines Mindestqualitätsstandards in Bezug auf die Bildqualität bei jeweils minimaler Dateigröße oder die individuelle Skalierbarkeit von Dateigröße oder Qualität für einzelne Dokumente.

PNG

Das Format „Portable Network Graphics“ (*.png) kann lizenzfrei angewendet werden. Es unterstützt 16,7 Mio. Farben, Transparenz, verlustfreie Kompression, inkrementelle Anzeige der Graphik (während des Ladens zunächst grobgerasterte Darstellung) und das Erkennen beschädigter Dateien.

TXT (ASCII / ANSI)

Insbesondere für die Speicherung von Metadaten ist die Verwendung eines einfachen Textformates angezeigt. Das Format stellt eine größtmögliche Lesbarkeit sicher und ist daher für die Speicherung von Metadaten zu verwenden. Der anzuwendende Zeichensatz ist in der Norm ISO 8859-1 beschrieben und bezeichnet ASCII plus Umlaute. Auch beim Metadatenaustausch wird zukünftig die Verwendung von klarschriftlesbaren Zeichensätzen gefordert. Der Datenaustausch wird dabei in Form von XML-Datenstrukturen erfolgen, die auf einfache Art die Einbindung der archivierten ASCII-Metadaten ermöglichen.

PDF (v1.3)

Das Portable Document Format (*.pdf) von Adobe eignet sich für nicht zur Veränderung vorgesehene Textdokumente. Das Dokumenten-Format ist plattformunabhängig nutzbar und wird von der Acrobat-Software ab Version 4 unterstützt.

Das PDF-Format bietet wesentliche Vorteile gegenüber der Speicherung von Dokumenten im TIF- bzw. JPEG-Format, wenn Dokumente bereits in einem CI-Format[2] vorliegen und archiviert werden sollen.

[2]CI-Format **CI Dokument**. **CI** (Coded Information) sind Informationen, die so codiert sind, dass sie eine Software interpretieren und damit arbeiten kann.

Das Konvertieren von CI-Dokumenten zum Zweck der Archivierung in ein NCI-Format (z. B. TIF, JPEG ...) bedeutet immer einen Informationsverlust, da die enthaltenen Textinformationen bei der Konvertierung verlorengehen und lediglich die optische Information erhalten bleibt.

Das PDF-Format ermöglicht es jedoch, neben der graphischen Information auch die enthaltene Textinformation zu speichern, so daß beide Informationsebenen erhalten und nutzbar bleiben.

Insbesondere die Nutzung der Volltextrecherche innerhalb des Textes des Dokuments ist mit PDF-Dokumenten möglich, so daß zukünftige Ansätze des Wissensmanagements, die auf intelligenten Suchen im Volltext basieren auch mit den archivierten Dokumenten durchführbar sind.

Darüber hinaus verfügt das PDF-Format über weitere Funktionalitäten (digitales Signieren von Dokumenten, Gliederungsfunktionen usw.), die das Format für die Archivierung geeignet erscheinen lassen.

Empfohlen wird daher, dass PDF-Format jetzt sofort und zukünftig für die Archivierung von in CI-Formaten bereitgestellten Textdokumenten einzusetzen.

Zusammenfassung

Für die Langzeitarchivierung von Dokumenten sollten wenige, einheitliche Formate verwendet werden. Wichtiges Entscheidungskriterium ist dabei das bestehende Datenformat des zu archivierenden Textdokuments : liegt das Dokument in einem CI-Format vor, so sollte das PDF® - Format für die Archivierung gewählt werden (Speicherung von Text und Graphikinformation).

Liegt das Dokument hingegen lediglich in NCI-Form vor, so ist vorrangig das TIF-Format zu verwenden. Unter bestimmten Voraussetzungen (s.o.) kann auch das JPEG-Format Anwendung finden. Die Verwendung des PNG-Formats für die Archivierung von NCI-Dokumenten ist gemäß des SAGA-Standards erlaubt, und kann ggf. als Alternative in Betracht gezogen werden.

Multimedia Formate

Einen Sonderfall stellen heute Multimedia-Dateiformate dar, die zunehmend auch Bestandteil elektronischer Behördenakten werden.

Heute kann nicht abgesehen werden, welche der zahlreichen Formate sich langfristig am Markt behaupten werden und doch muß auch hier gewährleistet sein, dass die Dateien auch in Zukunft auswertbar bleiben. Das Speichern in einem einheitlichen Format, wie es für alle Schriftstücke der elektronischen Akte möglich ist, scheidet für Multimedia-Formate aus. In jedem Falle ist bei der Formatwahl der jeweilige SAGA-Standard für die unterschiedlichen Multimedia-Typen zu beachten.

5 GEWÄHRLEISTUNG DER KONSISTENZ ELEKTRONISCHER DATEN

5.1 Revisionssicherheit

Unternehmensdokumente und behördliche Unterlagen müssen auch in elektronischer Form den Kriterien Vollständigkeit, Integrität und Authentizität, Zusammenfassung aufgabenbezogener und zusammengehöriger Schriftstücke, Nachvollziehbarkeit und Rechtmäßigkeit des Verwaltungshandelns genügen.

Elektronische Akten müssen wie ihre Vorgänger im Papierformat über die unmittelbare Bearbeitung hinaus ihre Nachweisfunktion erfüllen. Unter „revisionssicherer elektronischer Archivierung“ versteht man Archivsysteme, die beliebige Informationen sicher, unveränderbar, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar verwalten.

Bei der Betrachtung der Anforderungen an eine revisionssichere Archivierung sind unterschiedliche Aspekte zu berücksichtigen. Die Möglichkeit zur Rekonstruktion von Indexinformationen muß bestehen, damit elektronisch archivierte Daten dauerhaft zuverlässig recherchiert werden können, ein nicht-authorisierter Zugriff muß durch entsprechende Möglichkeiten zur Rechtevergabe verhindert werden und die Gültigkeit elektronisch signierter Dokumente muß über den gesamten Lebenszyklus eines elektronischen Dokuments gesichert sein.

Ein weiterer Aspekt ist die verlustfreie Reproduzierbarkeit der Daten auch nach langen Zeiträumen.

Auch wenn die ursprüngliche Anwendung, mit der ein Dokument ursprünglich erstellt wurde, nicht mehr zur Verfügung steht, so ist sicherzustellen, dass entsprechende Viewerkomponenten vorhanden sind, welche die originalgetreue Reproduzierbarkeit des Dokuments uneingeschränkt sicherstellen.

5.1.1 Rekonstruktion von Indexinformationen

Damit archivierte Objekte mittels Recherchefunktionalitäten aufgefunden werden können, muß eine Indexdatenbank aufgebaut werden, die bei entsprechenden Suchanfragen eine Liste der aufgefundenen Treffer bereitstellt und auf die zugehörigen archivierten Objekte verweist.

Sollte es im Laufe des Archivbetriebs zu einem Verlust oder einer Beschädigung der Indexdatenbank kommen, so hat dies zur Folge, dass der archivierte Datenbestand nicht mehr zugänglich ist. Die Rekonstruierbarkeit des Indexes kann gewährleistet werden, wenn zusätzlich zu den archivierten Objekten auch deren Indexinformationen bei der Verlagerung auf ein Langzeitspeichermedium mitgespeichert werden. Auf diese Weise kann bei einem Datenverlust des Indexservers der gesamte Index mit Hilfe der mit den Objekten gespeicherten Indexinformationen aus dem Archiv heraus rekonstruiert werden.

5.1.2 Zugriffsberechtigungen auf archivierte Objekte und Metadaten

Elektronisch archivierte Objekte und deren Metadaten unterliegen ebenso wie die im Tagesgeschäft der Behörden bearbeiteten und erzeugten Dokumente strengen Zugriffsbeschränkungen.

Es muß daher gewährleistet sein, dass Zugriffsberechtigungen für archivierte Objekte vergeben werden können.

Das Zugriffsrecht kann dabei über die Inhalte bestimmter Indexfelder definiert werden. So könnte der Zugriff z. B. über den Wert eines Metadatums für die Sicherheitsklassifikation eines Dokuments reglementiert werden.

Der Zugriff auf Indexinformationen und archivierte Objekte kann danach folgendermaßen geregelt werden : ein Benutzer meldet sich zunächst über das Betriebssystem an seinen Arbeitsplatz an. Über seine Zugehörigkeit zu einer Benutzergruppe hat er zunächst die Rechte zum Aufruf der Archivanwendung bzw. zum Vorgangsbearbeitungssystem mit seiner zugehörigen Archivkomponente.

Gegebenenfalls ist zum Anmelden an das Archivsystem eine weitere eigene Benutzerkennung nötig. Innerhalb der Anwendung stehen dem Nutzer nun die ihm zugewiesenen Funktionalitäten und Zugriffsbereiche des Archivsystems zur Verfügung.

Das aktivierte Benutzerprofil kann zusätzliche Informationen dazu beinhalten, welche Art von Metainformationen / Dokumente der Benutzer recherchieren darf.

So kann ein Benutzer beispielsweise zusätzlich zum Recht der Recherche nach Dokumenten nach Dokumenten mit hoher Sicherheitsklassifikation recherchieren und diese auch einsehen, während ein anderer Benutzer nur das Recht zur Recherche nach Dokumenten mit niedriger Sicherheitsklassifikation besitzt.

5.1.3 Elektronische Signatur

Elektronische Signaturen bieten die Möglichkeit, die Integrität und Authentizität digitaler Daten zu sichern.

Im Unterschied zu Papierdokumenten kann die Beweiseignung elektronisch signierter Dokumente mit der Zeit abnehmen. Ursachen hierfür sind insbesondere, dass die verwendeten kryptographischen Algorithmen und Schlüssel im Laufe der Zeit ihre Sicherheitseignung verlieren und dass nicht gewährleistet ist, dass die für die Überprüfung von Zertifikaten notwendigen Verzeichnisse und Unterlagen über 30 Jahre und mehr verfügbar sind.

In dem vom Bundesministerium für Wirtschaft und Arbeit geförderten Konsortialprojekt "Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (ArchiSig)" werden Archivierungskonzepte und - techniken aufgegriffen und dahingehend erweitert, dass sie die sichere und beweiskräftige Langzeitarchivierung digital erzeugter und signierter Daten über 30 Jahre und mehr ermöglichen.

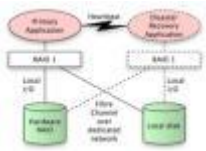
Dabei werden Systemarchitekturen mit neuen technischen Komponenten und organisatorischen Konzepten zur Gewährleistung der Sicherheit digitaler Signaturen entwickelt. Um eine rechtssichere Archivierung elektronisch signierter Dokumente zu gewährleisten, sind die Ergebnisse des genannten Projektes bei der Konzeption und Realisierung eines elektronischen Archivsystems entsprechend zu berücksichtigen.

5.2 Ausfallsicherheit von Archivsystemen

Da eine hohe Verfügbarkeit aller Komponenten von entscheidender Bedeutung ist, sollte das System so ausgelegt werden, dass z. B. bei Ausfällen einzelner Rechner die Funktionalität des Systems weiterhin gegeben ist.

Dies betrifft sowohl die redundante Auslegung von Komponenten, als auch Möglichkeiten zum Wiederanlauf (Restart) und zur Wiederherstellung (Recovery). Hierbei ist zu beachten, dass die Ausfallsicherheit in starkem Maße von der Qualität der eingesetzten Hardware abhängig ist.

5.2.1 Hot-Standby



Bei Hot-Standby handelt es sich um eine fehlertolerante Einrichtung, die solange in einer Wartefunktion ruht, wie die begleitende primäre Komponente einwandfrei arbeitet.

Erst wenn die primäre Komponente oder Übertragungsstrecke ausfällt, tritt die Hot-Standby-Komponente in Aktion und übernimmt die Funktion der primären Komponente (bei der Gemeinde Gauting z.B. bei den Linux – Systemen der Firewalls so realisiert).

Solche Hot-Standby-Einrichtungen werden überall dort eingesetzt, wo Daten oder andere Informationen verlorengehen könnten, deren unmittelbare Verfügbarkeit von höchster Wichtigkeit ist. Hot-Standby-Systeme finden z. B. beim Betrieb sicherheitsrelevanter Einrichtungen Verwendung.

Ob die Einrichtung eines Hot-Standby-Systems zur Gewährleistung der Ausfallsicherheit von Archivierungssystemen eingesetzt werden soll, muß in erster Linie daran gemessen werden, ob ein jederzeit unmittelbarer Zugriff auf die innerhalb des Systems archivierten Daten erforderlich ist.

Wird das Archivsystem also im wesentlichen oder ausschließlich zur Verwahrung von Daten innerhalb der Aufbewahrungsfrist genutzt und nicht zu Auskunfts- oder Bearbeitungszwecken, so wird die Notwendigkeit eines Hot-Standby-Systems i.d.R. nicht gegeben sein.

Der Einsatz eines Systems zur Gewährleistung des jederzeitigen unmittelbaren Datenzugriffs (Hot-Standby) ist für Archivierungssysteme in bestimmten Anwendungsszenarien erforderlich. Die Einführung eines solchen Systems begründet sich im Einzelfall anhand der Art und Nutzung der archivierten Daten.

5.2.2 Backup

Ein Backup ist die Duplizierung von Datenfiles, Directorys oder Programmen zum Zwecke der Datensicherung, die auf eine Speichereinheit kopiert werden.

Backups dienen im Falle der Datenbeschädigung oder des Datenverlustes der Wiederherstellung der Originaldaten. Die Methoden und die Häufigkeit der Backup-Erstellung hängen von der Aktualität und dem Alter der Daten ab.

Backups finden normalerweise auf Dateiebene statt. Eine geänderte Datei wird dabei komplett an den Server übertragen und in den Massenspeichern gespeichert. Man spricht in diesem Fall von der Sicherung auf Volumen-Ebene.

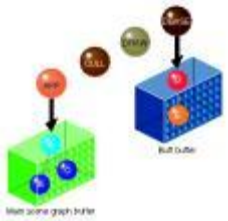
Findet vor der Sicherung eine Optimierung der Dateien statt, in dem nur die geänderten Blöcke einer Dateien zur Sicherung übertragen werden, spricht man von einer Sicherung auf Blockebene. Dieses Verfahren kommt vorwiegend bei geringen Übertragungskapazitäten zum Einsatz.

Ein periodisches Datenbackup ist für diejenigen Daten eines Dokumentenmanagementsystems geboten, die noch nicht zum Zwecke der Langzeitarchivierung auf Langzeitspeichermedien gesichert wurden, die über das Archivsystem verwaltet werden.

Es handelt sich bei den durch ein Backup zu sichernden Dateien also um Daten, die innerhalb eines Vorgangsbearbeitungs- oder Archivierungssystems noch für den Direktzugriff auf Magnetplatten vorgehalten werden, also den „lebenden“ Datenbestand eines solchen Systems. Mittels Backup zu sichernde Daten werden innerhalb eines VBS deshalb immer die Daten sein, die noch nicht auf Medien zur Langzeitarchivierung transferiert wurden.

Daten, die innerhalb eines Vorgangsbearbeitungssystems noch für den Direktzugriff auf Magnetplatten vorgehalten werden, sind periodisch per Backup zu sichern.

5.2.3 Caching



Der Cache stellt einen schnellen Zwischenspeicher (Puffer) dar, der häufig angeforderte Daten aus dem Arbeitsspeicher oder vom tatsächlichen Speicherort aufnimmt und bei Bedarf wieder zur Verfügung stellt.

Dazu speichert der Cache den Inhalt häufig angesprochener Speicherzellen des Arbeitsspeichers sowie die Adressen, unter denen diese Daten gespeichert sind.

Wenn Daten von einer bestimmten Speicherdresse angefordert werden, prüft der Cache, ob er diese bereits enthält. Ist das der Fall, werden die betreffenden Daten direkt aus dem Cache übergeben, andernfalls werden sie aus dem regulären Speicher abgerufen.

Ein Cache trägt auf diese Weise dazu bei, die Arbeitsgeschwindigkeit des Rechners zu erhöhen, da die im Cache zwischengespeicherten Daten nicht erneut angefragt werden müssen und der Cache eine wesentlich höhere Zugriffsgeschwindigkeit bietet als der Hauptspeicher.

Caching ist ein bewährtes Mittel, um die Skalier- und Verfügbarkeit von Systemen zu steigern sowie die Latenzzeit für Benutzeranforderungen zu verkürzen.

Im Gegensatz zum Web-Caching, setzt Datenbank-Caching „ausgewachsene“ Datenbanksysteme als Caches ein, um dort Satzmengen entfernter Datenbanken möglichst adaptiv verwalten und Anfragen darauf auswerten zu können.

Verfahren dazu reichen von separat verwalteten materialisierten Sichten über

überlappende, aber replikationsfrei gespeicherte Sichten bis hin zu Cache-Groups, in denen parametrisierte Cache-Constraints den Cache-Inhalt spezifizieren.

Ein Cache stellt vor allem ein Mittel zur Verringerung des Net-Traffics und zur performanten Datenbereitstellung dar. Ein Cache ist als temporärer Speicherort für häufig benötigte Daten grundsätzlich nicht als Instrument zur dauerhaften Datensicherung geeignet.

5.2.4 Medienkopien

Die Daten werden nicht nur einmal, sondern identisch auf mehreren Datenträgern abgespeichert.

Ist die Wahrscheinlichkeit, dass ein einzelner Datenträger nicht mehr gelesen werden kann, 1/1.000 (einer auf Tausend), so ist bei 3 identischen Datenträgern (dreifache Redundanz) die Wahrscheinlichkeit, dass alle 3 Datenträger nicht mehr gelesen werden können 1/1.000.000.000 (einmal auf eine Milliarde Fälle).

Das Vorhalten von insgesamt mehr als 3 Kopien erscheint nicht sinnvoll, da es mit jeder Kopie immer schwerer wird, die gegenseitige Übereinstimmung der wachsenden Zahl von Kopien zu belegen.

Aus Gründen der Datensicherung ist es geboten zumindest eine vollständige Kopie des archivierten Datenbestandes vorzuhalten.

Die Sicherungskopie(n) sollte(n) dabei an geographisch anderen Orten als der im Archivsystem des Unternehmens / der Behörde zur Nutzung vorgehaltene Archivdatenbestand gelagert werden (anderer Brandschutzabschnitt). Selbst die vollständige Zerstörung der Daten an einem Ort würde dann zu keinen größeren Datenverlusten führen.

Die Kopie(n) sollte(n) auf einen nur einmal beschreibbaren Datenträger geschrieben werden und auch den Ausgangspunkt für die notwendigen Kopier- und Migrationsgänge darstellen.

Die Kopien dienen im Wesentlichen als Sicherung für den im Archivsystem zur Nutzung vorgehaltenen Datenbestand. Sie könnten aber auch für einen Zugang via Inter-/Intranet angeboten werden.

Auch die für die Benutzung freigegebenen Kopien bedürfen strenger Sicherheitsvorkehrungen, um die Authentizität der archivierten Daten garantieren zu können. Sowohl bei der Benutzung als auch bei der Langzeitarchivierung sind daher erhöhte Sicherheitsanforderungen zu beachten.

5.3 Medienüberprüfung und Qualitätssicherung

Es ist nicht auszuschließen, dass eingesetzte Medien ggf. von vornherein fehlerhaft sind bzw. im Laufe der Nutzungszeit entweder komplett oder zumindest teilweise ausfallen können.

Das bedeutet, dass ein erfolgreich auf ein Medium geschriebenes Objekt nicht für die gesamte Aufbewahrungsfrist bzw. Medienlebensdauer auch vollständig und korrekt wiedergegeben werden kann.

Es gibt in der digitalen Domäne keinen kontinuierlichen Zerfall. Eine digital aufgezeichnete Information kann daher entweder vollständig (und richtig) gelesen werden, oder es treten Fehler auf, welche im Prinzip den ganzen betroffenen Datensatz wertlos machen. Um das Auftreten von Fehlern überhaupt erkennen zu können, müssen spezielle Algorithmen eingeführt werden. Bei heutigen Datenträgern ist die Berechnung und Prüfung von „Checksums“ meistens in die Hardware integriert. Im Falle von Lesefehlern wird oft der ganze Datensatz als unleserlich bezeichnet und übersprungen bzw. der Lesevorgang ganz abgebrochen.

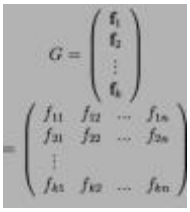
Insofern gibt es bei digitalen Daten nur zwei Möglichkeiten : der Datensatz kann gelesen werden und ist deshalb auch „korrekt“, oder der Datensatz ist unleserlich und verloren.

5.3.1 Medienchecks auf physikalischer Ebene

Bei digitalen Datenträgern, die für die Langzeitarchivierung bestimmt sind, müssen, sofern vorhanden, regelmäßig Verfahren durchgeführt werden, die eine Aussage über die Langzeitstabilität eines bestimmten Materials erlauben.

Datenträger sind relativ kurzlebig. Um die Lebensdauer nicht weiter zu verkürzen, müssen für die Lagerung der Medien unbedingt die Vorschriften des Herstellers beachtet werden.

5.3.1.1 Prüflesen



Bei allen heute bekannten digitalen Aufzeichnungsverfahren sind Aufzeichnungsfehler in einem kleinen Ausmaß unvermeidbar, z. B. bedingt durch nicht perfekte Medien (Materialfehler).

Diese intrinsischen Aufzeichnungsfehler werden aufgefangen, indem Fehlerkorrekturverfahren („error-correction“ der „recoverable errors“) angewandt werden.

Somit kann trotzdem garantiert werden, dass die Daten korrekt wiedergegeben werden.

Erlaubt ein Aufzeichnungsgerät, die Anzahl der erfolgreichen Fehlerkorrekturen zu bestimmen, so erhält man damit ein Maß für die Qualität der Kombination Medium plus Lesegerät.

Ein regelmäßiges Prüflesen erlaubt festzustellen, ob die Anzahl Fehler zugenommen hat, und ist somit ein guter Indikator, um schadhafte (vorschnell alternde) Medien frühzeitig zu erkennen.

5.3.1.2 Medienchecks

Die Qualität von Datenträgern variiert von Hersteller zu Hersteller, und kann auch beim selben Hersteller in der Zeit erheblich variieren.

Deshalb sollte im Prinzip jede Charge von Medien stichprobenartig auf die Qualität überprüft werden, um rechtzeitig herstellungsbedingte Qualitätsmängel (Materialfehler) zu erkennen.

Bei einigen Medien (z.B. CD-R) ist eine optimale Abstimmung von Aufzeichnungsgerät und Medium notwendig, um eine optimale Qualität und damit Langzeitsicherheit zu erhalten.

Im Falle von CD-R sind gute Ergebnisse (d.h. CD's mit sehr wenig Fehlern) nur durch eine optimal aufeinander abgestimmte Kombination von CD-Brenner – Rohling – Schreibgeschwindigkeit erreichbar.

Da mit normaler Aufzeichnungshardware kaum Aussagen über die Güte gemacht werden können, muß spezielle Prüfhardware eingesetzt werden, um die optimale Kombination herauszufinden. Dieser Test sollte für jede neue Charge von Medien wiederholt werden.

5.3.1.3 Abgleich zwischen Medienkopien (Konsistenzprüfung der Kopien)

Um die Wahrscheinlichkeit zu verringern, dass das Originalmedium Fehler aufweist, müssen die Daten früh genug auf ein neues Medium kopiert werden, bevor ein Datenverlust durch Alterung des Mediums oder durch Technologiewandel auftreten kann.

Diese Fehlerkorrekturverfahren beruhen auf mathematischen Verfahren, welche einerseits das Erkennen von Fehlern und deren Korrektur in einem Schritt erlauben. Diese Verfahren garantieren bis zu einer gewissen Fehlerhäufigkeit, dass die digitalen Daten im streng mathematischen Sinn absolut korrekt wiedergegeben werden. Ein weitverbreitetes Verfahren beruht auf dem „cyclic redundancy check“ und wird als CRC-Verfahren bezeichnet.

Ein Abgleich von Medienkopien kann erfolgen, indem mehrere (redundant vorhandene) Datenträger mit identischen Daten miteinander verglichen werden.

Alle Kopiervorgänge müssen mit Null Fehlertoleranz durchgeführt werden, um jedem Informationsverlust vorzubeugen. Dies kann erreicht werden, indem jede Kopie sofort nach dem Schreiben mit dem „Original“ verglichen wird.

Die Vernichtung von Originaldokumenten darf erst nach garantierter konsistenter Speicherung auf mehreren Medien erfolgen. Entsprechend müssen Prozesse etabliert werden, welche die zuvor genannten Tätigkeiten beinhalten.

5.4 Echtes Löschen archivierter Objekte

Echtes Löschen von archivierten Objekten nach Ablauf der Aufbewahrungspflicht erfordert oftmals eine Medienreorganisation.

Unter Umständen läßt sich diese vermeiden, falls es in Abhängigkeit der zu archivierenden Daten und deren Volumina möglich ist, durch geschickte Speicherkonzepte die Vernichtung einzelner archivierter Objekte durch eine Vernichtung ganzer Medien zu ersetzen.

Nach Ablauf der Aufbewahrungspflicht und ggf. der Übergabe der Daten an das zuständige Archiv, werden die entsprechenden elektronischen Daten aus dem Archivierungssystem gelöscht.

Ein echtes Löschen der Daten ist dabei i.d.R. zunächst nicht möglich, da Daten auf WORM-Speichermedien grundsätzlich nicht mehr manipuliert oder gelöscht werden können. In diesem Fall erfolgt zunächst ein logisches Löschen der Objekte, so dass sie nicht mehr recherchierbar sind. Objekte können gesperrt/logisch gelöscht werden, indem ihre Indexinformationen aus der Indexdatenbank entfernt werden.

Damit ist gewährleistet, dass auf die Daten nicht mehr zugegriffen werden kann, obwohl sie physikalisch noch auf einem Speichermedium abgelegt sind. Nur durch eine Reorganisation der Speichermedien kann in diesem Fall ein echtes Löschen der betreffenden Objekte erreicht werden: Alle Medien, auf denen sich einzelne zu löschende Objekte befinden, müssen zu diesem Zweck auf Magnetplatte zurückgelesen werden und nur diejenigen Daten, welche weiterhin im Archiv verbleiben, werden anschließend erneut indexiert und auf neue Medien zur Langzeitspeicherung transferiert.

Die alten Medien werden nach der erfolgreichen Reorganisation physikalisch zerstört.

Der aufwendige Vorgang der Reorganisation von Speichermedien kann erheblich vereinfacht werden, wenn es gelingt, die zu archivierenden Daten nicht wahllos nacheinander auf ein Medium zu transferieren, sondern sie statt dessen in Abhängigkeit vom Datum des Ablaufs ihrer Aufbewahrungsfrist zu transferieren.

Dieses setzt jedoch voraus, dass die Aufbewahrungsfrist Bestandteil des Metadatensatzes aller archivierten Objekte ist. Zu diesem Zweck werden Daten vor der Verlagerung auf Wechselspeichermedien nach dem Metadatum der Aufbewahrungsfrist und dem Aktenzeichen sortiert.

Nach der Transformation sollten sich auf einem Medium immer nur elektronische Daten bzw. Vorgänge befinden, deren Aufbewahrungsfrist im gleichen Jahr abläuft.

Die Speichermedien verbleiben nun bis zum Fristeintritt im passiven Datenbestand des Archivs und werden anschließend der zuständigen Archivbehörde zur Übernahme angeboten. Ein entsprechend definiertes Anbiete- und Bewertungsverfahren regelt die dabei zu beachtenden Verfahrensschritte und ist nicht Bestandteil dieses Papiers.

Nach der bestätigten Übergabe der Daten an das zuständige Archiv kann der Datenträger vernichtet werden und es sind keine weiteren Reorganisationsläufe zur Neustrukturierung der weiterhin innerhalb der Behörde verbleibenden Daten nötig.

Zu vernichtende Datenträger müssen vollständig gelöscht, oder aber physikalisch zerstört werden. Eine vollständige Löschung der auf CD-R-, WORM- bzw. DVD-R-Platten enthaltenen Informationen ist derzeit nur möglich durch Zerstörung der Speicherfläche (Ätzen, Zerkratzen) oder durch physikalische Vernichtung des gesamten Datenträgers (Einschmelzen, Verbrennen, Schreddern).

6 BERECHTIGUNGSKONZEPT

In einem Archivierungssystem werden umfangreiche personen- oder abteilungsbezogene Datenbestände verwaltet.

Zur Einhaltung der Bestimmungen des Datenschutzgesetzes sind geeignete technische und organisatorische Maßnahmen zu treffen. Sie müssen gewährleisten, daß Unbefugte keinen Zugriff auf Daten bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung haben.

Deshalb ist es unabdingbar, die Zugriffsmöglichkeiten z. B. auch durch **bauliche Maßnahmen** (z. B. Schließanlage) und eine Benutzerverwaltung (zentral oder produktspezifisch) zu regeln. Die Benutzerverwaltung muß Vertretungen und Ersetzungen von Personen und Rollen sowie deren Rechten erlauben.

Bei der Einführung eines Archivierungssystems muß darauf geachtet werden, bis zu welcher Berechtigungstiefe innerhalb des Systems einzelne Rechte vergeben werden können, da bei zu geringer Berechtigungstiefe ggf. nur begrenzte Archivierungsszenarien realisiert werden können. Es ist daher zu prüfen, ob das geplante Archivierungsszenario mit dem zur Verfügung stehenden Berechtigungskonzept des Systems umgesetzt werden kann.

Das Berechtigungskonzept kann funktions- oder objektbezogen realisiert sein. Natürlich können auch beide Ansätze bzw. eine Kombination beider Ansätze realisiert werden. Funktionsbezogen bedeutet, dass z. B. eigene Rechte für das Lesen, Ändern, Anlegen, Löschen und Drucken von Objekten vergeben werden können.

Ein objektbezogenes Konzept ermöglicht dagegen die Vergabe von Zugriffsrechten auf die unterschiedlichen Objekttypen (Dokumente, Akten, Vorgänge, Indexdatensätze, einzelne Indexfelder etc.). Die größtmögliche Anpassungsfähigkeit bietet ein System, das neben der objekt- und funktionsbezogenen Rechtevergabe eigene User-Exits bzw. Schnittstellen für eigenständig programmierbare Berechtigungsprüfungen besitzt, so dass auch sehr spezielle Anforderungen an die Rechtevergabe durch Eigenanpassungen des Systems ermöglicht werden.

Einen wichtigen Punkt des Datenschutzes kann die Problematik des Löschens von personenbezogenen Daten (DSGVO) innerhalb des vorgeschriebenen Zeitraumes darstellen.

Diese können nach der Archivierung normalerweise nur noch logisch gelöscht werden. Hier muß entschieden werden, ob diese Art der Löschung ausreicht. Andernfalls kann nur durch Migration der Medien (Umkopieren der nicht gelöschten Bereiche) eine echte Löschung der Daten erfolgen.

Behörden : Seitens des Bundesarchivs und der Bayerischen Archivverwaltung wird derzeit die Rechtsauffassung vertreten, dass sämtliche elektronische Akten, Vorgänge und Dokumente solange unverändert und vollständig vorgehalten werden müssen, bis diese dem zuständigen Archiv angeboten wurden.

Entscheidet sich das zuständige Archiv für die Übernahme der Daten, so sind diese vollständig zu übergeben.

Das vorzeitige Löschen einzelner Daten oder vollständiger Datensätze ist somit nicht zulässig, solange die Datenbestände innerhalb der Aufbewahrungsfrist in der aktenführenden Stelle verwahrt werden und noch keine Übernahmeentscheidung seitens des zuständigen Archivs gefallen ist.

7 MIGRATION

Die Lebenszeit von Archivsystemen ist i. d. R. viel kürzer als die Aufbewahrungsfrist der in ihnen gespeicherten Objekte (bspw. Dokumente).

Dies ist vor allem im technologischen Fortschritt der Computer-Hardware begründet, der einhergeht mit Weiterentwicklungen der für den Betrieb dieser Hardware erforderlichen Software. Des weiteren muß man davon ausgehen, dass Produktanbieter, die die entsprechende Software entwickeln und vertreiben, ebenfalls nicht für den gesamten Aufbewahrungszeitraum am Markt verfügbar sein werden. Ein Wechsel vom Archivsystem eines Anbieters zu einem Archivsystem eines anderen Anbieters, bzw. ein Wechsel von einer Archivsystemtechnologie hin zu einer moderneren, ist unumgänglich.

Man kann nach Erfahrungswerten davon ausgehen, dass eine solche Migration alle fünf bis sieben Jahre stattfindet.

Ggf. ist bei einem solchen Wechsel nicht das Archivsystem selbst zu migrieren, sondern es sind nur die verwendeten Formate in neue den aktuellen Stand der Technik entsprechende Formatversionen zu konvertieren, die bis auf Weiteres allgemein lesbar sind.

Damit ist es wichtig, bereits bei der Planung eines Archivsystems eine spätere Migration zu berücksichtigen und möglichst zu vereinfachen.

7.1 Vollständige Migration inkl. Medienwechsel, Benutzerverwaltung,Index

Bei einer vollständigen Migration findet eine Komplettübernahme sämtlicher Daten des Altsystems in die entsprechenden Module/Komponenten des neuen Systems statt.

Dies hat den Vorteil, dass auch nach der Migration ein Archivsystem zur Verfügung steht, dessen Einzelkomponenten optimal aufeinander abgestimmt sind.

Der Kostenaufwand für die Migration ist allerdings im Vergleich zu den anderen Migrationsvarianten beträchtlich.

Durch einen Medienwechsel wird sichergestellt, dass auch hier die jeweils neuesten Speichertechnologien zum Einsatz kommen können.

Die Anzahl der eingesetzten Speichermedien wird damit insgesamt zurückgehen, da die Speicherkapazitäten zukünftig weiter zunehmen werden. Aufgrund der kurzen zu erwartenden Migrationszyklen von fünf bis sieben Jahren ist zudem sichergestellt, dass die Lebensdauer der Medien nicht überschritten wird und daher kein Datenverlust zu befürchten ist.

Es bietet sich an, zum Zeitpunkt der Migration eine Reorganisation der Speichermedien vorzunehmen, so dass aufgrund des Ablaufs der Aufbewahrungsfrist logisch gesperrte Objekte auch physisch eliminiert werden können.

Bei einer vollständigen Migration besteht immer die Gefahr, dass bestimmte im Altsystem vorhandene Information keine Entsprechung im neuen System hat und daher nicht 1:1 übernommen werden kann.

Auch ist zu bedenken, dass die Funktionalitäten und das „Look-and-Feel“ des neuen Systems nicht der gewohnten Altumgebung entsprechen werden.

Eine Entscheidung für eine Komplettmigration sollte daher nicht alleine aus technischen Gesichtspunkten erfolgen.

7.2 Migration ohne Wechsel der Medienverwaltung

Bei einer Migration ohne Wechsel der Medienverwaltung bleiben die eigentlichen Daten auf den Original-Datenträgern und die Hardware zum Auslesen und Bereitstellen der Informationen unverändert.

Neben dem Kostenvorteil gegenüber einer Komplettmigration bestehen weitere Vorteile : da auf eine Datenmigration komplett verzichtet werden kann, besteht auch keine Gefahr eines Datenverlustes, der z. B. durch die Überführung der Daten in ein anderes Datenmodell entstehen kann.

Voraussetzung für eine solche Teilmigration ist das Vorhandensein einer entsprechenden Schnittstelle zwischen dem neuen System und der Medienverwaltung des Altsystems.

Bereits bei der erstmaligen Entscheidung einer Behörde für ein elektronisches Archivierungssystem ist daher darauf zu achten, dass eine grundsätzliche Entkopplung des Systems zwischen der Medienverwaltung mit den angeschlossenen Hardwarekomponenten und den weiteren Komponenten des Archivsystems möglich ist.

Nachteile dieser Form der Migration sind in der Gefahr der Überalterung und der damit zunehmenden Fehleranfälligkeit im Bereich der eingesetzten Archivierungshardware zu sehen. Es besteht die Gefahr, daß einzelne Hardwarekomponenten zukünftig nicht mehr lieferbar bzw. nicht mehr gewartet werden und dass Anbieter und Hardwarelieferanten mit der Zeit vom Markt verschwinden. Gleiches gilt für die Software der Medienverwaltung und die Speicherformate der eingesetzten Medien : werden diese nach Jahren nicht mehr unterstützt, so besteht auch hier die Gefahr eines Totalverlustes der gespeicherten Daten.

Eine laufende Marktbeobachtung ist bei einer Migration ohne Wechsel der Medienverwaltung daher von großer Bedeutung für den langfristigen Erhalt der archivierten Daten, um im Falle einer „ungünstigen“ Marktentwicklung frühzeitig reagieren zu können.

Eine Reorganisation der Speichermedien ist auch bei dieser Form der Migration in periodischen Abständen geboten, auch wenn dies aus hardwaretechnischen Gründen nicht zwingend ist.

Es ist Aufgabe des Systemanbieters, eine eindeutige und fundierte Migrationszusage abzugeben und das Verfahren der Migration zu beschreiben.

Hierbei kann auch eine Aufteilung von Zuständigkeiten zwischen Anwender und Anbieter erfolgen.

Die Zusage sollte auch für eingesetzte fremde Produkte bei Nichtverfügbarkeit einer Folgeversion - sofern deren Einsatz zur Aufrechterhaltung des Betriebes notwendig ist - gelten. Falls der Anbieter dieses Produkt nicht selbst vertreibt, sollte er ein funktional vergleichbares Produkt eines Drittherstellers anbieten.

8 ANHANG

Der **V**erband **O**rganisations- und **I**nformationssysteme (VOI) hat eine Aufstellung der wesentlichen Anforderungen an eine revisionssichere elektronische Archivierung herausgegeben. Es handelt sich dabei um die 10 Merksätze des VOI.

8.1 Die 10 Merksätze des VOI zur elektronischen Archivierung

- Jedes Dokument muß unveränderbar archiviert werden.
- Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument muß mit geeigneten Retrieval-Techniken wieder auffindbar sein.
- Es muß genau das Dokument wiedergefunden werden, das gesucht worden ist.
- Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
- Jedes Dokument muß in genau der gleichen Form, wie es erfaßt wurde, wieder angezeigt und gedruckt werden können.
- Jedes Dokument muß zeitnah wiedergefunden werden können.
- Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.
- Das System muß dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB, AO etc.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

8.2 Interpretation zu § 17 Signaturverordnung (SigV) durch ArchiSig (Zitat)

Stellungnahme zur Erneuerung qualifizierter elektronischer Signaturen nach § 17 Signaturverordnung (SigV) vom 06.02.2003

Die angefügte Interpretation zu § 17 SigV entspricht grundsätzlich der Ansicht der Regulierungsbehörde für Telekommunikation und Post (RegTP) als zuständige Behörde nach § 3 Signaturgesetz (SigG).

Wichtig für den Erfolg und die Durchsetzung technischer Konzepte ist ein gemeinsames, einheitliches Verständnis der gesetzlichen Regelungen, die ihnen zugrunde liegen. Die folgende Interpretation des § 17 SigV entspricht Sinn und Zweck der Regelung, ist mit ihrem Wortlaut vereinbar und ermöglicht eine effektive, wirtschaftliche Realisierung der Signaturerneuerung in großen Archiven.

1 Wortlaut

§ 17 SigV: Zeitraum und Verfahren zur langfristigen Datensicherung. Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für die Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen und der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muß mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

2 Interpretation

1. Die Beweiswerterhaltung qualifizierter elektronischer Signaturen nach § 17 SigV erfordert den Einsatz erneuter qualifizierter elektronischer Signaturen und qualifizierter Zeitstempel. Andere Sicherungsmittel wie z. B. die Speicherung auf einmal beschreibbaren Datenträgern, die Hinterlegung bei Notaren etc. erfüllen nicht die Anforderungen der Vorschrift.

2. Die erneute qualifizierte elektronische Signatur ist keine Willenserklärung, sondern ein Sicherungsmittel vorhandener Willenserklärungen. Sie muß daher keine persönliche Signatur z. B. eines Archivars sein.

3. Werden elektronisch signierte Daten mit einem qualifizierten Zeitstempel versehen, der mindestens eine qualifizierte elektronische Signatur enthält, so genügt dies für eine erneute elektronische Signatur im Sinn des § 17 Satz 3 SigV. Eine weitere qualifizierte elektronische Signatur ist nicht notwendig, da sie keinen Sicherheitsmehrwert bietet.

4. Die Daten müssen entsprechend der fehlenden Eignung des Sicherungsmittels, d. h. der eingesetzten Algorithmen und Parameter, neu signiert werden.

Da die Daten durch einen Hashwert repräsentiert werden, reicht es aus, allein die Signaturen des elektronischen Dokuments erneut mit einem Zeitstempel zu versehen und somit neu zu signieren, vorausgesetzt der verwendete Hashalgorithmus ist noch sicherheitsgeeignet und nur der asymmetrische Verschlüsselungsalgorithmus ist in seiner Sicherheitseignung gefährdet. In diesem Fall repräsentiert der Hashwert die Daten weiterhin und die erneute elektronische Signatur umfasst damit auch die ursprünglich signierten Daten. Die Berechnung eines neuen Hashwertes der gesamten Daten mit einem neuen sicherheitsgeeigneten Hashalgorithmus und ein erneuter Zeitstempel unter Einbeziehung einer erneuten qualifizierten elektronischen Signatur sind dann notwendig, wenn auch der eingesetzte Hashalgorithmus in seiner Sicherheitseignung gefährdet ist. In diesem Fall ist nicht mehr sichergestellt, dass der Hashwert die ursprünglichen Daten repräsentiert und die erneute elektronische Signatur diese damit umfasst.

5. Die erneute Signatur muß rechtzeitig, d. h. vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter, und mit neuen nach der Bewertung der zuständigen Behörde sicherheitsgeeigneten Algorithmen und zugehörigen Parametern erfolgen.

6. Die erneute elektronische Signatur muß mindestens die gleiche Qualitätsstufe haben wie die Ausgangssignatur, um deren ursprüngliche Qualität zu erhalten. Qualifizierte elektronische Signaturen mit Anbieterakkreditierung müssen durch qualifizierte Zeitstempel akkreditierter Zertifizierungsdiensteanbieter erneuert werden; für die Signaturerneuerung qualifizierter elektronischer Signaturen muß der Zertifizierungsdiensteanbieter, der den qualifizierten Zeitstempel zur Signaturerneuerung erzeugt, nicht akkreditiert sein.

7. Die erneute elektronische Signatur muß alle vorherigen qualifizierten elektronischen Signaturen zu den Daten umschließen, d. h. sowohl parallele und sequentielle Mehrfachsignaturen als auch frühere erneute elektronische Signaturen. So bleibt der Beweiswert der Daten in vollem Umfang erhalten. Selbst ein nachträgliches Löschen einzelner zu den Daten gehörender Signaturen wird erkennbar, so dass nach der ersten Signaturerneuerung der Beweiswert sogar zunimmt.

8. Eine erneute elektronische Signatur kann beliebig viele Daten umschließen. Dies müssen nicht die Daten eines, sondern können die Daten vieler Dokumente sein. Auch verschlüsselte Daten, die qualifizierte elektronische Signaturen enthalten, können erneut elektronisch signiert werden, wenn die verschlüsselten Daten die signierten Daten eindeutig repräsentieren.

9 QUELLENVERZEICHNIS

AWV - Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. [Hrsg.]:
Sicherheit, Haltbarkeit und Beschaffenheit optischer Speichermedien. 2. vollst. überarb. und erw. Auflage 2003.

Bischoff, Frank M., Archivierung digitaler Unterlagen - Neue Anforderungen an die Archive, Vortrag auf dem Hessischen Archivtag am 5. Juli 2000 in Frankfurt.

Brandner, R.; Pordesch, U.; Rossnagel, A.; Schachermeyer, J. (2002): Langzeitsicherung qualifizierter elektronischer Signaturen. Datenschutz und Datensicherheit 26 (2), 97 - 103.

Bredow, Felix von; Kampffmeyer, Dr. Ulrich (2003): Verfahrensdokumentation, Rechtsfragen.
http://www.project-consult.net/ Files/ Download_Verfahrensdokumentation_20020523.pdf

Bundesministerium des Innern [Hrsg.] (2003): SAGA: Standards und Architekturen für E-Government-Anwendungen, Version 2.0, 2003 In: Schriftenreihe der KBSt, Bd.59. Bundesministerium des Innern [Hrsg.] (1998): Konzept zur Aussonderung elektronischer Akten. In: Schriftenreihe der KBSt, Bd.40.

Dollar, Charles (2000): Authentic Electronic Records. Strategies for Long-Term Access, Chicago, S. 57 f.

Friedrichs, Christian (2003): Paradigmenwechsel in der Archivierung? GDA.

Gschwind, Rudolf ; Frey, Franziska ; Rosenthaler, Lukas (2002): Digitale Archivierung von fotografischen Sammlungen. Ein Grundlagenbericht.

Härder, Theo ; Bühmann, Andreas (2004): Datenbank-Caching – Eine systematische Analyse möglicher Verfahren.Technische Universität Kaiserslautern.

Henstorf, Karl-Georg ; Kampffmeyer, Dr. Ulrich ; Prochnow, Jan (1999): Grundsätze der Verfahrensdokumentation nach GoBS „Code of Practice“ zur revisionssicheren Archivierung, In: VOI-Schriftenreihe Kompendium Band 4.

Kampffmeyer, Dr. Ulrich (1996): Restart, Recovery und Konsistenzsicherung von elektronischen Archivsystemen. In: VOI NEWS, Ausgabe 1/96.

Kampffmeyer, Dr. Ulrich (1996): Anforderungen an Verfahrensbeschreibungen für Archivsysteme mit digitalen optischen Speichern In: VOI Kompendium Band 2, Rechtsinitiative.

Kampffmeyer, Dr. Ulrich (2003): Revisionssichere Archivierung im Licht neuer rechtlicher Anforderungen.

Kampffmeyer, Dr. Ulrich ; Rogalla, Jörg (1997): Grundsätze der elektronischen Archivierung „Code of Practice“ zum Einsatz von Dokumenten- Management- und elektronischen Archivsystemen, In: VOI-Schriftenreihe Kompendium Band 3.

Keitel, Christian (2002): Die Archivierung elektronischer Unterlagen in der baden-württembergischen Archivverwaltung. Eine Konzeption (12.6.2002),

Köpke, Gernot; Scherer, Mathias (2002): Leitfaden „Aufbewahrung von Dokumenten“ für Hersteller, Lieferanten und Anwender von Elektronischen Bauelementen und Baugruppen auf dem deutschen Markt. Frankfurt.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder [Hrsg.]: Datenschutzgerechtes E-Government. Handlungsempfehlungen.

Rathje, Ulf (2002): Technisches Konzept für die Datenarchivierung im Bundesarchiv. In: Der Achivar, Jg. 55 (2002), S.117-120.

Richter, Rolf D. (2003): Storage-Infrastrukturen nach Maß. http://www.speicherguide.de/magazin/background.asp?theID=189

Schäfer, Udo ; Nicole Bickhoff [Hrsg.] (1999): Archivierung elektronischer Unterlagen (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg:
Serie A, Landesarchivdirektion, H. 13), Stuttgart, S. 165–181.

Verein schweizerischer Archivarinnen und Archivare (VSA) [Hrsg.]: Arbeitsgruppe „Archivierung elektronischer Akten“: Aktionsprogramm 1999/2000: Basisdukument.

Victorian Electronic Records Strategy (VERS): http://www.prov.vic.gov.au/vers/standards/pros9907vers2/default.htm

Wettengel, Michael: Technische Infrastruktur für die Archivierung von digitalen Datenbeständen - Anforderungen und Verfahrensweisen. In: INSAR Beilage II (1997) (Vorträge und Ergebnisse des DLM-Forums über elektronische Aufzeichnungen), S. 190 - 198.

Aktuelle Information und Charakteristika elektronischer Speichermedien finden sich unter folgenden Webadressen:

http://de.wikipedia.org/wiki/Speichermedien

http://www.speicherguide.de/

Copyright © 2005-2021 by id-newmedia, Ralf Kimmelmann

Alles verwendete Bildmaterial : licensed by Vital Imagery Ltd. / id-newmedia