Revisionssichere Dokumentenarchivierung

Herausforderungen Digitaler Archivierung

Zusammenfassung

Im digitalen Zeitalter beinhaltet die Archivierung von Informationen, Unterhaltung und anderem Material nicht nur die Sicherung der gewünschten Inhalte, sondern auch die Pflege und Wartung der Speichermedien, auf denen die Daten gespeichert sind. Die digitale Archivierung ist gerade heute von entscheidender Bedeutung da immer weniger Informationen als Hardcopy gespeichert sind.

Die sichere und nachvollziehbare Speicherung wichtiger Dokumente in elektronischer Form, auch „revisionssichere Archivierung" genannt, ist ein unverzichtbares Verfahren, dessen gesetzliche Grundlage jedes Unternehmen kennen sollte.

DI Dr. techn. Peter Tomsu

RISE

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektentwicklung GmbH

www.rise-world.com • welcome@rise-world.com

Vorwort

In einer Welt, die zunehmend von Digitalisierung und datengetriebenen Prozessen geprägt ist, gewinnt die revisionssichere Dokumentenarchivierung an zentraler Bedeutung. Unternehmen, Institutionen und Organisationen aller Größen stehen vor der Herausforderung, ihre Dokumente nicht nur digital, sondern auch gesetzeskonform und dauerhaft sicher zu speichern. Dabei spielen Aspekte wie Rechtssicherheit, Datensicherheit und Effizienz eine entscheidende Rolle.

Dieses Whitepaper widmet sich den vielschichtigen Herausforderungen der digitalen Archivierung und beleuchtet, wie moderne Technologien und Strategien dazu beitragen können, diese zu bewältigen. Es bietet einen umfassenden Überblick über die rechtlichen und technischen Anforderungen, stellt Best Practices vor und gibt konkrete Handlungsempfehlungen für Unternehmen, die ihre Archivierungsprozesse zukunftssicher gestalten wollen.

Unser Ziel ist es, Entscheidungsträger und Fachkräfte gleichermaßen zu unterstützen, indem wir praxisnahe Lösungen aufzeigen und Denkanstöße für eine nachhaltige und revisionssichere Dokumentenarchivierung liefern. In diesem Zusammenhang freuen wir uns, Ihnen wertvolle Einsichten und Werkzeuge an die Hand geben zu können, die Ihnen helfen, die Digitalisierung Ihrer Archivierungsprozesse erfolgreich zu gestalten.

Wir danken Ihnen für Ihr Interesse an diesem Whitepaper und hoffen, dass es Ihnen als wertvolle Ressource auf Ihrem Weg zu einer rechtskonformen und effizienten digitalen Archivierung dient.

Inhaltsverzeichnis

1 Digitale Archivierung

Digital Archivierung beschreibt die aktive Aufbewahrung von digital gespeicherten Informationen. Als Teil der formalisierten Bemühungen der Bibliotheks- und Archivwissenschaften umfasst digitale Archivierung Praktiken die sicherzustellen, dass Informationen vor dem Ausfall von Medien sowie dem Altern von Software und Hardware geschützt sind.

Im digitalen Zeitalter beinhaltet die Archivierung von Informationen, Unterhaltung und anderem Material nicht nur die Sicherung der gewünschten Inhalte, sondern auch die Pflege und Wartung der Speichermedien, auf denen die Daten gespeichert sind. Die digitale Archivierung ist gerade heute von entscheidender Bedeutung da immer weniger Informationen als Hardcopy gespeichert sind.

Seit Beginn des elektronischen Zeitalters hat die Informationstechnologie bei der Aufbewahrung von Dokumenten mitgeholfen und wird heute generell als digitale Archivierung bezeichnet. Die Informations- und Kommunikationstechnologie (Information and Communication Technology - ICT) hat revolutionäre Veränderungen bei der Organisation und Verwaltung von Informationen gebracht und bringt heute die einzigartige und großartige Möglichkeit, den Bereich der Archivierung mit der digitalen Speicherung nicht digitaler Dokumente zu kombinieren.

Digitale Materialien umfassen Texte, Datenbanken, stehende und bewegte Bilder, Audio, Grafiken, Software und Webseiten, unter anderem eine breite und wachsende Palette von Formaten. Sie sind häufig flüchtig und bedürfen einer gezielten Produktion, Pflege und Verwaltung, um erhalten zu bleiben. Viele dieser Ressourcen haben bleibenden Wert und Bedeutung und sollten daher für heutige und künftige Generationen geschützt und erhalten werden. Digital Archivierung ist daher auch der Prozess der Aufrechterhaltung der Zugänglichkeit von digitalen Objekten im Laufe der Zeit und gewinnt immer mehr an Bedeutung.

Da wie bereits erwähnt die Überalterung von Software als auch Hardware von Speichermedien imminent sind gehören das Aktualisieren von Daten und das Übertragen auf neue Medien desselben Typs, um Datenverluste aufgrund von Medienausfällen zu verhindern zu den wichtigsten Aufgaben der digitalen Konservierung. Die Migration (Übertragung auf neue Medien) verhindert Datenverluste aufgrund veralteter Hardware. Im Falle von veralteter Software werden manchmal Emulatoren verwendet, um Inhalte wiederzugeben. Diese Emulatoren werden dann Teil dessen, was bewahrt werden muss. Die schiere Menge an digitalen Inhalten stellt dabei eine nicht zu unterschätzende Herausforderung dar.

Auch Inhaltspiraterie spielt eine Rolle bei der digitalen Archivierung. Raubkopierer stellen oft redundante Kopien von digitalen Inhalten bester Qualität zur Verfügung. File-Sharing-Software wie BitTorrent ermöglicht die Verteilung und geografisch getrennte Backups. Digitale Archivierung erfordert in vielen Fällen den Schutz des geistigen Eigentums.

Organisationen wie die Digital Preservation Coalition arbeiten daran Inhale die als wichtig erachtet werden sicher zu speichern, wie gesagt mit besonderem Augenmerk auf digitale Inhalte. Sowohl digital erzeugte als auch digitalisierte Materialien durchlaufen hierbei die gleichen Prozesse, einschließlich:

- Begutachtung der Erhaltungswürdigkeit
- Identifikation
- Überprüfung der Integrität
- Charakterisierung des Inhalts
- Sicherung der Nachhaltigkeit
- Überprüfung der Authentizität
- Zugriffserlaubnis und Protokollierung
- Das Hinzufügen von Metadaten über den Bewahrungsprozess

Digitales Material bezieht sich auf jedes Material, das von einem Computer verarbeitet wird, und umfasst sowohl digitalisierte als auch solche Ressourcen, die bereits digital generiert wurden. Der Begriff Langfristigkeit sollte in diesem Zusammenhang so verstanden werden, dass alle Auswirkungen sich ändernder Technologien erfasst und berücksichtigt werden und sollte Zeiträume von Jahrzehnten und sogar Jahrhunderten einbeziehen.

1.1 Aufgaben und Probleme der Digitalen Archivierung

Bei der digitalen Archivierung geht es um eine Reihe von Maßnahmen die ergriffen und verwaltet werden müssen, um sicherzustellen, dass der Zugriff auf digitale Materialien so lange wie nötig aufrechterhalten wird. Solange es notwendig ist, kann bedeuten

- Langfristig - bis in die unbestimmte Zukunft
- Kurzfristig - für eine bestimmte zeitlich begrenzte Geschäftsanforderung

1.1.1 Definitionen der Digital Archivierung

- Nach der Definition der American Library Association ALA aus 2007 umfasst Digital Preservation (Digitale Archivierung) Richtlinien, Strategien und Maßnahmen, die den Zugang zu digitalen Inhalten über einen längeren Zeitraum sicherstellen
- Nach der Encyclopedia of Information Technology wird der Begriff digitale Archivierung definiert als "Der Prozess der Erhaltung von Materialien, die in digitalen Formaten erstellt wurden, in einem für die Nutzung geeigneten Zustand zu erhalten". Die Probleme der physischen Bewahrung werden verstärkt durch die Veralterung von Computerausrüstung, Software und Speichermedien.

1.1.2 Arten von Dokumenten

Bei der digitalen Konservierung unterscheidet man zwei Arten von Dokumenten:

- Geborene digitale Dokumente: Dies bezieht sich auf jene Materialien, die ursprünglich bereits mit einer Form von digitaler Technologie erstellt wurden. Sie werden oft als elektronische Aufzeichnungen bezeichnet.
- Digital erstellte Dokumente: Dies bezieht sich auf jene Materialien, die von analoger in digitale Form umgewandelt wurden z. B. durch Umschreiben der Informationen oder Scannen des Dokuments oder der Objekte usw.

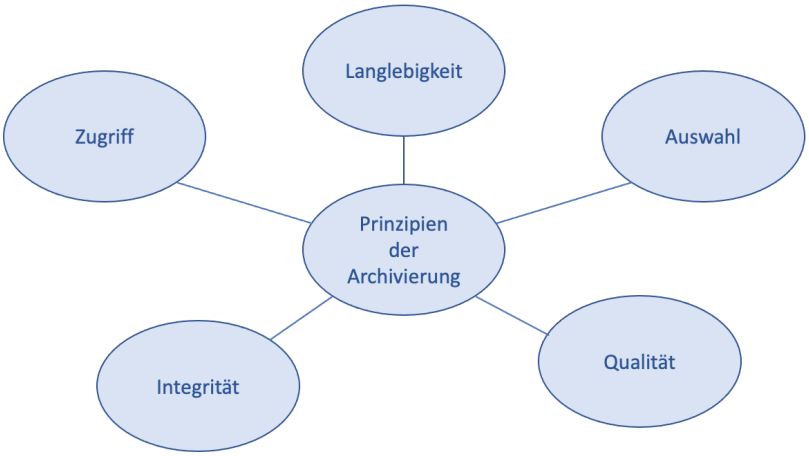
1.1.3 Ziele der digitalen Archivierung

Hauptziel ist es, digitales Material zu bewahren und weiterhin zugänglich zu machen indem folgende Punkte erfüllt werden:

- Garantie der Authentität der erhaltenen digitalen Materialien
- Verhindern der Beschädigung und des Verfalls der physischen Medien, indem eine Umweltkontrolle sichergestellt wird
- Schäden rückgängig zu machen, wenn dies möglich ist
- Änderung des Formats digitaler Materialien, um ihren intellektuellen Inhalt zu bewahren, wenn es notwendig ist

1.1.4 Prinzipien digitaler Dokumentenarchivierung

Die Grundprinzipien der Dokumentenarchivierung die für die Bewahrung von analogen Medien angewendet werden, gelten auch für die Archivierung in der digitalen Welt.



Langlebigkeit: Informationen, die in einem digitalen Format gespeichert sind, leben nicht ewig, da sie auf fragiler digitaler Basis aufbauen. Durch Replikationsübernahmen und Redundanz von Hardware, Software und Datenformaten wird impliziert, dass das, was heute lesbar und interpretierbar ist, in der Zukunft noch lange nicht nutzbar sein wird.

Auswahl: Die Auswahl ist ein mehrstufiger Prozess. In jeder Stufe gibt es mögliche Wege mit unterschiedlichen Optionen. Entweder ist es eine Auswahl von Materialien für die digitale Archivierung oder eine Auswahl von Werkzeugen und Technologien oder die Auswahl von Medien und Formaten. Jede Auswahl spielt eine sehr wichtige Rolle für den Erfolg des Archivierungsplans.

Qualität: Die Qualität digitaler Inhalte wird in folgenden drei Stufen gefordert:

1. Bei der Erstellung der Spezifikation für den Workflow
2. Bei der Auswahl und Handhabung der digitalen Erfassung
3. Bei der Auslieferung oder beim Zugriff, um die Downloadzeit und die benutzerfreundlichen Formate zu bewerten

Konsistenz ist dabei der Schlüssel die Qualität der digitalen Dateien zu gewährleisten.

Integrität: Integrität ist erforderlich, um den Zugriff auf digitale Inhalte zu schützen, auch wenn das ursprüngliche Speichermedium, Software und Hardware, auf denen die digitalen Inhalte erstellt wurden nicht mehr vorhanden sind. Die Bewahrung der digitalen Integrität digitaler Inhalte beinhaltet auch die Entwicklung von Techniken zur Überprüfung ihrer Veränderung gegenüber dem Originalformat.

Zugriff: Der Zugang zu digitalen Inhalten ist ein weiterer wichtiger Faktor, der berücksichtigt werden muss, wenn Ressourcen für den Online-Zugriff bereitgestellt werden. Es ist eine grundsätzliche Verantwortung jeder Bibliothek und jeder Archivierung, garantierten Zugriff zu ihren digitalen Inhalten zu gewähren.

1.1.5 Dimensionen digitaler Dokumentenarchivierung

Aktivitäten bei der digitalen Archivierung können grob in zwei Komponenten unterteilt werden

- Fördern der langfristigen Erhaltung des digitalen Inhalts
- Gewährleisten der kontinuierlichen Zugänglichkeit der Inhalte

Langfristige Konservierung: Fortgesetzter Zugang zu digitalen Materialien, oder zumindest zu den darin enthaltenen Informationen, auf unbestimmte Zeit.

Mittelfristige Konservierung: Fortgesetzter Zugriff auf digitale Materialien über technologische Veränderungen hinweg für einen definierten Zeitraum, aber nicht auf unbestimmte Zeit.

Kurzfristige Konservierung: Zugang zu digitalen Materialien entweder für einen definierten Zeitraum, während der Nutzung aber nicht über die absehbare Zukunft hinaus und/oder bis zur Unzugänglichkeit aufgrund von Änderungen in der Technologie.

2 Governance für zeitgemäße digitale Informationsbestände

Das 20. Jahrhundert scheint so lange her zu sein - eine Zeit, in der Unterlagen geheftet und gelocht wurden und Aufbewahrungspläne noch einfach waren. Mit dem Aufschwung des digitalen Zeitalters sind die zu verwaltenden Informationsbestände in ihrer Komplexität und Vielfalt immens gestiegen, und die Regeln sind heute weitaus zahlreicher und unbeständiger.

Zugriffskontrollen, Änderungsrechte, Übertragungsbeschränkungen, Vorschriften zur Technologiekontinuität, Regeln zur verschlüsselten Aufbewahrung - all diese neuen Anforderungen verändern, wie Datensätze verwaltet werden müssen. Innovationen lassen ständig neue Datentypen entstehen, darunter soziale Medien, Cloud-basierte Anwendungen und Datenbanken, Sicherheitsprotokolle, Videos, digitale Audiodateien und Ausführungsdateien für 3-D-Modelle, um nur einige Beispiele zu nennen.

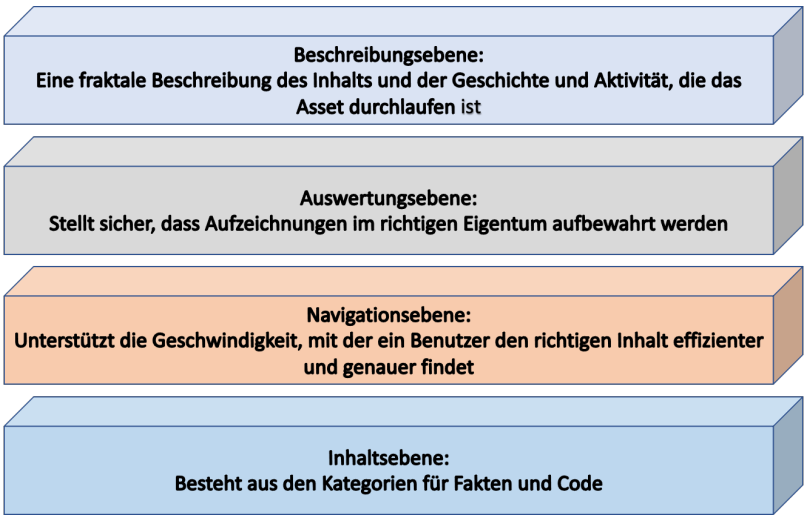
Der Aufbewahrungsplan bleibt jedoch als Mittel der ersten Wahl bestehen und erzwingt einen Regelungsmechanismus, der nicht mehr zu den neuen digitalen Informationsbeständen passt. Ein neues Design für die Klassifizierung von Informationen ist erforderlich, damit die neuen Regeln an die neuen Assets angepasst und ordnungsgemäß ausgeführt werden können. Dieser Artikel bietet eine Einführung, wie man mit der Konstruktion dieses neuen Designs beginnen kann.

2.1 Moderne digitale Informationsbestände erfordern einen neue Governance

In der Vergangenheit wurde jeder Datensatz als eine vollständige Einheit betrachtet. Seine Historie war gebündelt mit den Inhalten, die sich in den sichtbaren Hin- und Rückverzeichnissen, Datumsstempeln, Durchschlägen und Revisionsnummern zeigten. Heute sind diese Verwaltungsdaten vom materiellen Inhalt entkoppelt, oft über mehrere Datenbanken verteilt, in verschiedenen Systemen verwaltet und zunehmend nicht mehr in Papierform vorhanden.

Betriebsprotokolle, Zugriffsaufzeichnungen, Metadaten, Systemleistungsprotokolle, eingebettete und versteckte Inhalte - all das sind die neuen Arten von Informationsbeständen, die Unternehmen verwalten müssen, um die auferlegten Compliance-Pflichten zu erfüllen. Es handelt sich dabei nicht um "Aufzeichnungen", die in das Konstrukt des 20. Jahrhunderts passen; es sind neue Arten von Assets, auf die die Regeln angewendet werden müssen.

Diese neuen Assets unterscheiden sich so sehr von traditionellen Records, dass es hilfreich ist, sie unter anderen Aspekten zu betrachten. Anstatt einen digitalen Datensatz als ein einzelnes Asset zu betrachten, sollten Sie jeden Datensatz als ein Asset betrachten, das aus digitalen Informationen besteht, die in vier Schichten präsentiert werden. Zusammen fügen die Ebenen das, was früher als Datensatz existierte, zu einem einheitlichen Asset zusammen. Aber die Ebenen und die Kategorien innerhalb jeder Ebene ermöglichen es, die Regeln besser auf die Gesamtheit der Daten abzustimmen.



2.1.1 Die Beschreibungsebene

Um ein Asset zu verwalten, müssen wir wissen, was es ist. Das ist die Essenz der Klassifizierung. Daher wird die oberste Ebene als beschreibende Ebene bezeichnet. Im digitalen Zeitalter hängt die Beschreibung eines Assets von zwei Informationsbündeln ab: einer sachlichen Beschreibung des Inhalts (Größe, Volumen, Quellanwendung, Datentyp, Verschlüsselung) und der Historie und Aktivität, die das Asset durchlaufen hat (Erstellungsdatum, Autor oder Autoren, Revisionshistorie, Zugriffsprotokolle).

Die beschreibende Ebene ist es, auf die sich so viele der neuen Regeln konzentrieren. Und warum? Weil die Daten in dieser Schicht aussagekräftige, objektive Beweise für die Aktivitäten sind, die rechtliche Bedeutung haben: Wer hat was getan? Wann? Und wo? Für wen? Aber die beiden Kategorien (der Inhalt und die Historie und Aktivität eines Assets) helfen bei der Unterteilung und Fokussierung der Daten, auf die diese Regeln angewendet werden sollen.

2.1.2 Die Auswertungsebene

Regeln verlangen zunehmend, dass Daten und ihre Qualitäten bewertet werden. Tatsächlich führen die IT-Systeme und -Anwendungen eine Qualitätskontrolle durch und generieren Datensätze, die dokumentieren, wie gut andere Regeln auf Daten angewendet werden. Diese auswertenden Daten sind entscheidend, um sicherzustellen, dass die Datensätze ordnungsgemäß aufbewahrt werden.

Verbraucherkreditanträge, Beschäftigungsanträge und Datensätze mit Gesundheitsinformationen sind hervorragende Beispiele. Für jeden von ihnen erzeugen die Softwaresysteme intern administrative Datensätze, die dokumentieren und auswerten, ob alle gesetzlich vorgeschriebenen Prüfungen für jeden Datensatz durchgeführt werden.

Gleichzeitig sollten zunehmend externe Überprüfungen von digitalen Inhalten durchgeführt werden. Die Bewertungen von Quartalsberichten durch das Teammanagement und die sternchenbasierten Bewertungen von Songs, Auktionsartikeln und Filmen sind allesamt Daten, die Inhalte bewerten. Externe Bewertungen können als Metrik oder als subjektive Bewertung gemessen werden.

Mehr und mehr verlässt man sich heute auf die bewertende Ebene, bevor weitere Maßnahmen ergriffen werden. Wenn die gewonnenen Erkenntnisse über die Qualität eines Assets nicht gewissen Mindestregeln entsprechen, werden diese eher verworfen, als dass auf den Inhalt selbst zugegriffen wird. Die Bewertungsebene enthält Regeln mit definierten Prozessen, die sich als vorteilhaft für die Einhaltung von Regeln erweisen.

2.1.3 Die Navigationsebene

Sobald ein Content-Asset beschrieben und bewertet wurde, muss das Gesuchte gefunden werden. Die Navigationsebene präsentiert die Daten, um diese Arbeit zu vereinfachen und zu erledigen. Digitale Informationsbestände sind meist viel komplexer als das, was ein Inhaltsverzeichnis oder ein Index leisten kann. Die

Navigationsebene ermöglicht es den Benutzern, den richtigen Inhalt effizienter und genauer zu finden. Daten-Tags, Datenverzeichnisse und ähnliche Werkzeuge und Ausgaben befinden sich in dieser Schicht. Dies sind die Werkzeuge zum Auffinden von Inhalten.

Regierungsbehörden haben erkannt, dass diese Werkzeuge auch für ihre Arbeit äußerst nützlich sind, und auf globaler Basis verlangen Vorschriften zunehmend, dass diese Werkzeuge erhalten und verfügbar gemacht werden.

2.1.4 Die Inhaltsebene

Die letzte Schicht ist der primäre Inhalt selbst.

Die Inhaltsschicht besteht aus der Kategorie "Fakten" und der Kategorie "Code". In der Faktenkategorie befinden sich die Transaktionen und primären Geschäftsdatensätze. Eine weitere Klassifizierung wird hier nicht vorgeschlagen; die Unternehmenssysteme sind viel zu vielfältig und unterschiedlich in der Art und Weise, wie ihre Sachdaten tatsächlich verteilt werden. Wichtig ist, dass jede vorangehende Schicht effektiv mit dem faktischen Inhalt verbunden ist. So kann ein Unternehmen einen Datensatz (eine Rechnung, einen medizinischen Leistungsbericht, eine strukturierte Finanzierungsvereinbarung) rekonstruieren und anschließend an den relevanten Compliance-Verpflichtungen ausrichten.

Die Code-Kategorie ist ebenso wichtig, wenn nicht noch wichtiger. Im Großen und Ganzen wenden Records Management-Experten - ob sie nun Records Manager, Enterprise Content Manager oder Information Governance Executives genannt werden - nicht routinemäßig Governance-Kontrollen auf die Softwareanwendungen an, die die Schnittstelle zwischen den Benutzern und den digitalen Informationsbeständen bilden. Die IT-Abteilung übernimmt diese Verantwortung, einschließlich der zugehörigen Architekturentwürfe und Systemdokumentation. Richtig konzipierte Data-Governance-Prozesse für Datensätze bieten jedoch eine weitaus geeignetere Struktur, in der dies geschehen kann.

Auch hier handelt es sich um Informationsbestände, die oft von Behörden gesucht werden. Die Ausrichtung der Data-Governance-Prozesse unter einem derartigen System verbessert die Reaktionsfähigkeit und reduziert die Risiken. Die IT-Abteilung kann immer noch die Kontrolle behalten; wichtig ist die Fähigkeit, die Informationsbestände des Unternehmens zu dokumentieren und in einer einheitlichen Ansicht zusammenzufassen.

2.2 Das einheitliche Datenmodell

Zusammengesetzt ermöglicht dieses einheitliche Informationsmodell Records Management Fachleuten einen Ausgangspunkt für Diskussionen mit IT-Unternehmensarchitekten, Geschäftsmanagern, Compliance-Beauftragten, Dienstanbietern und Aufsichtsbehörden darüber, wie Regeln auf das Portfolio der zu verwaltenden modernen Assets verwaltet werden müssen. Mit einer derartigen Architektur können diese Regeln präziser auf die zu verwaltenden Informationsbestände ausgerichtet werden, und alle Verpflichtungen, nicht nur die Aufbewahrungspflichten, können aufeinander abgestimmt werden, um Nutzen, Integrität und Zugänglichkeit zu gewährleisten.

3 Unterschied zwischen Datensicherung und Archivierung

Der Hauptunterschied zwischen Backup und Archivierung besteht darin, dass Datensicherungen für die schnelle Wiederherstellung von Betriebsdaten konzipiert sind, während die Datenarchivierung Daten speichert, die nicht mehr im täglichen Gebrauch sind, aber dennoch aufbewahrt werden müssen.

Datensicherungen sollen eine schnelle Möglichkeit zur Wiederherstellung aktueller oder kürzlich genutzter Daten in Fällen bieten, die von Datenbeschädigung oder versehentlichem Löschen bis hin zu vollständigen Disaster Recovery (DR)-Szenarien reichen. Die Geschwindigkeit der Wiederherstellung ist von entscheidender Bedeutung.

Die Datenarchivierung ist als Repository für Daten gedacht, die über Zeiträume von bis zu Jahrzehnten aufbewahrt werden müssen. Die Geschwindigkeit der Wiederherstellung aus einem Datenarchiv ist in der Regel nicht so kritisch wie aus einer Datensicherung, aber die Durchsuchbarkeit ist von entscheidender Bedeutung.

Backup-Anwendungen neigen dazu, Daten in einem proprietären Format zu speichern, was ein Problem für die langfristige Datenaufbewahrung darstellen kann. Viele Unternehmen haben innerhalb eines Jahrzehnts eine Reihe von Upgrades der Datensicherungssoftware durchlaufen, was dazu führen kann, dass alte Backups bald nicht mehr lesbar sind. Aus diesem Grund sollte die Datenarchivierung von einer Anwendung übernommen werden, die speziell für diese Aufgabe entwickelt wurde und die Dateien im nativen Format in das Archiv verschiebt.

3.1 Sicherung vs. Archivierung

Die Möglichkeit, ein Datenarchiv zu durchsuchen, ist aus geschäftlichen und Compliance-Gründen von entscheidender Bedeutung, insbesondere dann, wenn eine formale juristische Suche Strafen für die verspätete Vorlage von Informationen nach sich ziehen kann.

Bei Datensicherungen weiß man oft, welche Dateien und Ordner man finden will und wo sich die Medien befinden. Bei Datenarchiven, die sich über mehrere Jahre hinweg angesammelt haben, ist das nicht der Fall, sodass man wahrscheinlich nach Stichworten suchen muss. Datenarchivierungssoftware baut Metadaten-Indizes zu den gespeicherten Daten auf, um eine einigermaßen schnelle Suche zu ermöglichen.

Man sollte jedoch Datensicherung und Datenarchivierung nicht vermischen. Jede Technologie hat ihre eigenen Eigenschaften und Anforderungen in Bezug auf die Aufbewahrungs- und Wiederherstellungsziele, und wenn man beides kombiniert schafft man nur noch mehr Probleme bei der Datenspeicherung.

4 Revisionssicherheit bei Dokumentenarchivierung

4.1 Was bedeutet Revisionssicherheit?

Der Begriff „revisionssicher" ist häufig im Zusammenhang mit der (elektronischen) Speicherung von Dokumenten zu lesen. Revisionssicher bedeutet "vor einer Revision (Abänderung) geschützt" – sprich manipulationssicher im Sinne der Compliance. Der Begriff wird sowohl im technischen wie organisatorischen Kontext der elektronischen Speicherung von Daten verwendet.

Allgemein wird unter einer revisionssicheren Archivierung verstanden, dass digitale Daten aufbewahrt werden und zwar so, dass die rechtlichen Anforderungen in Bezug auf Ordnungsmäßigkeit, Vollständigkeit, Sicherheit, Verfügbarkeit, Nachvollziehbarkeit, Unveränderlichkeit und Zugriffsschutz erfüllt sind. Doch was bedeutet dieser Begriff im Zusammenhang mit der (elektronischen) Speicherung von Dokumenten?

Im Gesetzestext selbst ist weder „revisionssicher" noch „Revisionssicherheit" zu finden. Der Begriff stammt ursprünglich aus dem Umfeld von Dokumentenmanagementsystemen, denen diese Eigenschaft zugeschrieben wird. Der Gesetzgeber hat den Begriff der Revisionssicherheit im Gesetzestext nicht definiert.

Jedoch bezieht sich „revisionssicher" im Zusammenhang mit der elektronischen Archivierung nicht nur auf die technischen Komponenten sondern auf die gesamte Lösung zur Dokumentenablage. Das bedeutet, dass hier gleichermaßen Aspekte wie sichere Abläufe, die Organisation des Anwenderunternehmens, die ordnungsgemäße Nutzung, der sichere Betrieb und der Nachweis des Prozesses über eine Verfahrensdokumentation zum Tragen kommen. Folglich kann es keine allgemein gültige Zertifizierung für die Revisionssicherheit einzelner Hardware- oder Softwaresysteme geben, da der individuelle Einsatz beim Anwender, die Ordnungsmäßigkeit des gesamten Verfahrens, die Qualität der Informationen und Prozesse sowie der sichere Betrieb ebenfalls zwingend Bestandteil der Revisionssicherheit sind.

Ob all diese Aspekte erfüllt werden und somit eine revisionssichere Anwendung (elektronisches Archivsystem bzw. die entsprechende Komponente innerhalb einer kaufmännischen Software oder eines DMS) vorliegt, prüfen und bestätigen in der Regel Wirtschaftsprüfer anhand der vorliegenden Verfahrensdokumentation. Gemäß den Finanzbehörden kann nur durch eine korrekte Verfahrensdokumentation der Nachweis der Revisionssicherheit erbracht werden.

4.2 GoBD Revisionssicherheit

Die sichere und nachvollziehbare Speicherung wichtiger Dokumente in elektronischer Form, auch „revisionssichere Archivierung" genannt, ist ein unverzichtbares Verfahren, dessen gesetzliche Grundlage jedes Unternehmen kennen sollte. Wer in diesem Bereich recherchiert, stößt mit hoher Wahrscheinlichkeit schnell auf den Begriff GoBD. Was sich hinter dem Kürzel versteckt und was daran für Unternehmen so wichtig ist, wird im Folgenden erklärt.

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, kurz „GoBD", gelten seit 1. Januar 2015 und regeln insbesondere die elektronische Erfassung von Gelderlösen. Unternehmer tragen die volle Verantwortung für die Umsetzung der Regelung, auch wenn die Datenverarbeitung an externe Dienstleister ausgelagert sein sollte. Die „GoBD" sind insofern für die revisionssichere Archivierung von Dokumenten bedeutsam, als dass sie das vielleicht wichtigste Regelwerk sind, auf den sich der Begriff „Revisionssicherheit" stützt.

Der ursprünglich vom Fachautor und Unternehmensberater Ulrich Kampffmeyer entwickelte Begriff der „revisionssicheren Archivierung" ist vom Verband Organisations- und Informationssysteme (VOI) in einem 1996 erstmalig veröffentlichten und in den vergangenen Jahren ständig aktualisierten „Code of Practice" systematisiert worden. Die „GoBD"sind dabei eins von drei Regelwerken, aus denen die Anforderungen revisionssicherer Archivierung abgeleitet werden: Die anderen beiden sind das Handelsgesetzbuch (HGB) und die Abgabenordnung (AO).

Im Rahmen der Revisionssicherheit von Unternehmen genügt es nicht, sich allein auf den gesetzlichen Rahmen zu konzentrieren, um ihre Archivierungsverfahren revisionssicher zu gestalten. Mindestens genauso wichtig sind die Handhabung der internen Prozesse und deren technische Umsetzung.

4.3 Die Verfahrensdokumentation

Zusätzlich zu den bisher genannten Kriterien schreibt der Gesetzgeber eine sogenannte Verfahrensdokumentation zur rechtskonformen Archivierung vor. In dieser Dokumentation müssen alle Archivierungsvorgänge und deren Kontrollmechanismen in einem Unternehmen sowohl technisch als auch organisatorisch beschrieben werden. Inhalte einer solchen Dokumentation enthalten

- Erfassen, Empfangen und Digitalisieren
- Indizieren, Verarbeiten, Wiederfinden und Ausgeben
- Aufbewahren und Vernichten von Dokumenten

Praktische Tipps für die Erstellung einer Verfahrensdokumentation findet man in der bitkom Checkliste für die Auswahl von Dokumentenmanagement-Systemen. Dort werden weiters die Anforderungen an einen ordnungsgemäßen IT-Betrieb nach GoBD beschrieben.

4.4 Revisionssicherheit – Versuch einer Definition

Wie bereits erwähnt bedeutet Revisionssicherheit die Erfüllung rechtlicher Anforderungen bei der Archivierung von digitalen Daten. Obwohl Revisionssicherheit in Gesetztestexten nicht erwähnt wird können wir versuchen eine Definition zu finden:

Der Begriff Revisionssicherheit bezieht sich in erster Linie auf elektronische Archivierungssysteme, die den Anforderungen des Handelsgesetzbuches (§ 239, § 257 HGB), der Abgabenordnung (§ 146, § 147 AO), der Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) und anderen rechtlichen Vorgaben entsprechen.

Um zu prüfen, ob ein elektronisches Archiv als revisionssicher gelten kann, ist es sinnvoll, die vom VOI (Verband Organisations- und Informationssysteme) definierten zehn Grundsätze zur Revisionssicherheit anzuwenden.

4.5 Zehn Grundsätze der Revisionssicherheit des VOI

Ein elektronisches Archiv gilt demnach als revisionssicher, wenn die vom Verband Organisations- und Informationssysteme (VOI) definierten zehn Grundsätze zur Revisionssicherheit auf die Lösung angewendet werden.

1. Jedes Dokument wird unverändert archiviert
Um die Forderung nach Revisionssicherheit zu erfüllen, ist es zunächst einmal notwendig, dass jedes Dokument unverändert, originär archiviert wird. D.h. das Dokument kann nicht mehr verändert, bearbeitet oder gelöscht werden.

In der Revisionssicheren Ablage können Eingangsdokumente z.B. in Form von PDF-Dokumenten archiviert werden. Ist ein Dokument einmal dort abgelegt, kann der Anwender es weder physikalisch löschen noch durch eine Bearbeitung verändern. Es ist ausschließlich möglich, das Dokument wieder aufzurufen und anzeigen zu lassen.

Die Revisionssichere Ablage verhindert zusätzlich das Überschreiben eines vorhandenen Dokuments. Wird dieses noch einmal eingescannt, beispielsweise nach handschriftlichen Ergänzungen, wird es entsprechend als eigenständige neue Version des Dokuments gespeichert.

2. Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen
Eine lückenlose und vollständige Archivierung eines Dokuments ist eine weitere Anforderung an die Revisionssicherheit einer Lösung. D.h. dass weder während der Übertragung in die Ablage noch im Archiv selbst Dokumente verloren gehen dürfen. Das kann z.B. durch einen Archiv-Key erfolgen den ein Dokument automatisch erhält sobald es die Ablage erreicht – gleichsam eine Eingangsbestätigung.

3. Jedes Dokument muss mit geeigneten Retrieval-Techniken wieder auffindbar sein
Innerhalb einer revisionssicheren Lösung muss jedes Dokument mit geeigneten Abruf-Techniken wie zum Beispiel durch das Indexieren mit Metadaten wieder auffindbar, also verfügbar sein.

Dies kann durch verschiedene Maßnahmen erfolgen wie z.B. Zugriffsregelung ausschließlich über vorgegebene Suchoberflächen von Archivierungsprogrammen. Daher existiert keine auch keine gesonderte Suchoberfläche für die Revisionssichere Ablage, sondern es kann nur über die Suchoberfläche des Archivierungsprogramms gesucht werden.

Die abgelegten Dokumente sind durch Belege im Archivierungsprogramm indexiert und lediglich Barcode oder Archiv-Key dienen als Schlüssel und erlauben den Zugriff auf ein Dokument in der Revisionssicheren Ablage.

4. Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist
Soll ein Dokument wieder auffindbar sein, ergibt sich daraus natürlich die Anforderung, dass tatsächlich dieses eine Dokument wiedergefunden wird, das gesucht ist. Als Voraussetzung dafür muss ein Dokument eindeutig identifiziert werden können. Diese wird durch Barcode und Archiv-Key erfüllt. Es ist daher technisch unmöglich, ein nicht zu diesen Schlüsseln passendes Dokument aufzurufen oder anzeigen zu lassen.

5. Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können
Um die Revisionssicherheit zu gewährleisten muss jede verwendete Softwarelösung dafür sorgen, dass kein Dokument während seiner Lebenszeit und den gesetzlich definierten Aufbewahrungszeiten zerstört werden kann, es kann also auch nicht einfach vom Anwender gelöscht werden. Soll ein Archiv z.B. um Zeiträume, die nicht mehr aufbewahrungspflichtig sind, verkleinert werden, so muss dies gesondert beantragt und durchgeführt werden.

6. Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können
Ein Dokument muss in der ursprünglichen Formatierung wieder angezeigt und gedruckt werden können. Grundsätzlich erfüllt das PDF-Format erfüllt diese Anforderung. PDF ist ein portables Dateiformat welches unabhängig vom Betriebssystem bzw. Textverarbeitungsprogramm ist und weiters bewahren PDF-Dateien die Formatierung der Dokumente und sind selbst gegen Änderungen geschützt.

7. Alle Inhalte müssen zeitnah wiedergefunden werden können
Diese Anforderung ergänzt den vierten Grundsatz und besagt, dass alle Inhalte, die gespeichert sind, ohne langwieriges Suchen wiedergefunden werden können.

Wenn also archivierte Dokumente jeweils mit einem direkten Archiv-Key versehen sind, mit dem ein abgelegtes Dokument in der Revisionssicheren Ablage eindeutig identifiziert wird, reicht ein einziger Klick, um das Dokument aus dem Archiv aufzurufen.

8. Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist
Dieser Grundsatz verlangt die Protokollierung aller Veränderungen der Organisation und Struktur des Archives, um den ursprünglichen Zustand rekonstruieren zu können.

Oft wird heute dazu eine eigene Ablage in der Cloud zur Verfügung gestellt. Aus Sicherheitsgründen darf dabei der innere Aufbau der Ablagestruktur nach außen nicht sichtbar und auch nicht veränderbar sein. Darüber hinaus darf ein direkter Zugriff auf diese Struktur nicht möglich sein.

9. Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist
Ein revisionssicheres elektronisches Archiv muss den Wechsel auf neue Plattformen, Medien, Softwareversionen und Komponenten erlauben, ohne dass es zu Informationsverlusten kommt. Solange die Dokumente im plattformunabhängigen PDF-Format abgelegt sind, ist ein Wechsel auf eine neue Plattform oder Softwareversion unkompliziert. Die weitere revisionssichere Aufbewahrung der Dokumente ist durch den Kunden selbst sicherzustellen.

10. Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen

Dieser Grundsatz fordert die sichere Aufbewahrung der Daten in einem elektronischen Archiv gemäß sowohl gesetzlicher als auch betrieblicher Bestimmungen. Um den unbefugten Zugriff auf die Dokumente auszuschließen, darf nur über sichere Oberflächen auf das Archiv zugegriffen werden können (siehe auch Anforderungen 1 und 2).

Zum zusätzlichen Schutz sollten die Dokumente im Archiv verschlüsselt abgelegt werden, so dass ein direktes Lesen bzw. Anzeigen der Dokumente nicht möglich ist. Die Revisionssichere Ablage sollte auch automatisch datengesichert sein, sodass sogar im Falle der physikalischen Zerstörung des Archives selbst die Dokumente erhalten bleiben.

4.6 GoBD und ECM

Die GoBD betreffen grundsätzlich alle DV-Systeme, wozu auch ECM (Enterprise Content Management Systeme) / DMS (Dokumentenmanagement Systeme) zählen. So müssen GoBD-Grundsätze wie z.B. Unveränderbarkeit, Vollständigkeit, Nachvollziehbarkeit oder Unveränderbarkeit von Daten und Dokumenten auch von einem ECM-System erfüllt werden.

Sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden bzw. dort eingegangen, sind sie laut den GoBD in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Unternehmen müssen demnach sicherstellen, dass diese Daten nicht mehr ausschließlich in ausgedruckter Form aufzubewahren sind, sondern für die Dauer der Aufbewahrungsfrist unveränderbar erhalten bleiben.

Für die Führung elektronischer Bücher gelten gemäß den GoBD die gleichen gesetzlichen Ordnungsmäßigkeitsanforderungen wie bei einer manuellen Buchhaltung auch.

5 Revisionssicheres Archivieren heute wichtiger den je

Wenn Daten sicher und besonders noch revisionssicher aufbewahrt werden sind diese gut organisiert, so dass es einfacher ist, die richtigen Dokumente zu finden, wenn sie gebraucht werden. Viele Arten von digitalem Material, das für die Langzeitarchivierung ausgewählt wurde, können vertrauliche und sensible Informationen enthalten, die geschützt werden müssen, um sicherzustellen, dass kein nicht autorisierter Benutzer auf sie zugreifen kann. In vielen Fällen kann es sich dabei um gesetzliche oder regulatorische Verpflichtungen der Organisation handeln.

Die Bedeutung der Dokumentenarchivierung wächst in modernen Unternehmen stetig. Im gleichen Maße gilt es, den zunehmenden gesetzlichen Regelungen für die Aufbewahrung und Verwaltung der Daten gerecht zu werden, auch Datenschutz spielt hierbei eine entscheidende Rolle. Zum Schutz der eigenen und der Kundendaten hat die Sicherheit der Dokumente höchste Priorität.

Noch immer zählen heute Backup und Archivierung in zahlreichen Unternehmen zu vernachlässigten Aufgaben der IT, obwohl es wie wir gesehen haben klare gesetzliche Bestimmungen für die Aufbewahrung wichtiger und auch sensibler Informationen gibt. Um die Anforderungen an revisionssichere Archivierung zu erfüllen muss auch nicht immer auf kommerzielle Lösungen zurückgegriffen werden, denn heute leisten auch Open Source Lösungen gute Dienste, wenn sie nur richtig konfiguriert sind.

Das Löschen einer E-Mail oder eines Office-Dokuments hat im privaten Umfeld selten gravierende Folgen, kann aber Unternehmen in erhebliche Schwierigkeiten bringen. Je nach Dateninhalten bestimmen unterschiedliche Gesetze, wie lange Dokumente in welcher Form aufbewahrt werden müssen – Stichwort "Compliance". Die Compliance definiert, welche rechtlichen Mindestanforderungen in punkto Sicherheit, Integrität und Verfügbarkeit gewahrt werden müssen.

Mitarbeiter, die E-Mails oder andere Daten auf eigene Faust als archivierungswürdig oder -unwürdig einordnen, verändern oder löschen, handeln hinsichtlich der Aufbewahrungspflicht grob fahrlässig, werden allerdings nicht zur Verantwortung gezogen. Das Unternehmen haftet für den falschen Mausklick eines Mitarbeiters. Schlimmstenfalls wird der Chef persönlich zur Rechenschaft gezogen, wenn er die entsprechenden E-Mails oder Daten nicht vorlegen kann. Das Handelsrecht sieht hier sogar Geld- oder Freiheitsstrafen vor, wenn Handelsbücher oder wichtige Unterlagen vor Ablauf der Aufbewahrungsfrist nicht mehr auffindbar sind.

Angesichts dieser Problematik benötigen alle Unternehmen, insbesondere auch kleine und mittelständische Unternehmen eine umfassende Backup- und Archivierungsstrategie. Wichtig dabei ist nicht nur, dass gesetzliche Vorgaben für das Archivieren von handels- und steuerrechtlich relevanten Informationen erfüllt werden. Vor dem Hintergrund der Beweisrelevanz und des firmeninternen Informationsmanagements ist auch die vollständige Dokumentation von Geschäftsvorgängen Pflicht. Mit einer Volltextindizierung abgespeichert, lässt sich jedes einzelne Schriftstück per Mausklick im Archiv schneller und leichter auffinden. Die Herausforderung besteht darin, das zunehmende E-Mail-Datenvolumen sowie wichtige Dokumente, die täglich im Unternehmen auflaufen, richtig zu verwalten und zu gewährleisten, dass der elektronische Schriftverkehr – wenn erforderlich – effizient und lückenlos nachweisbar ist.

Heute gibt es zahlreiche kommerzielle Programme, aber auch Open Source Lösungen, die auf unterschiedlichen Medien wie Bändern, Festplatten oder optischen Datenträgern sichern und auch das Auffinden verlorener Informationen ermöglichen. Die Sicherungen können dabei entweder als komplettes, inkrementelles oder differentielles Backup erfolgen. Das differenzielle Backup sichert alle Dateien, die seit der letzten Vollsicherung erstellt oder modifiziert wurden. Das inkrementelle Backup, manchmal auch als Zuwachssicherung bezeichnet, sichert alle Informationen, die seit der letzten Sicherung – gleich ob vollständig oder nicht – erstellt oder verändert wurden.

Open Source Sicherungsprogramme lassen sich vor allem integriert in ein Linux-Betriebssystem an nahezu alle Bedürfnisse eines Unternehmens anpassen, aufgrund der Komplexität sollte diese Aufgabe jedoch besser in die Hände eines Linux- und Backup-Experten gegeben werden.

Zur Archivierung unter Linux eignen sich miteinander verzahnte Tools, um die sensiblen Informationen oder E-Mails revisionssicher und mit der geforderten Zuverlässigkeit auf eine eigenständige Festplatte zu sichern. Eine Suchfunktion für einen Auditor oder für Anwender und die Möglichkeit für eine endgültige Archivierung - etwa auf CDs oder DVDs – sollte dabei natürlich auch unterstützt werden. Auch für diese Anforderungen können Systemintegratoren Unterstützung bei der Umsetzung leisten.

Concorde Business Park F
2320 Schwechat
Austria, Europe

Firmenbuch: FN 280353i
Landesgericht Korneuburg
UID: ATU62886416

www.rise-world.com
welcome@rise-world.com

RISE