Zeitschrift Informatik-Spektrum der deutschen Gesellschaft für Informatik

Ursula Sury

Escrow Management bei elektronischer Archivierung

Elektronische Archivierung

Die elektronische Archivierung ist ein Thema, das heute sehr viele Unternehmungen und auch staatliche Organe beschäftigt. Zum einen, weil zwischenzeitlich die notwendigen gesetzlichen Bestimmungen zur rechtsgültigen Erstellung und Aufbewahrung elektronischer Dokumente erlassen wurde. Zum andern, weil für viele Unternehmungen die lückenlose **elektronische Bearbeitung von Dokumenten** während ihres ganzen Lebenszyklus ohne Medienbruch aus Kostengründen sehr attraktiv ist.

Von den vorhandenen gesetzlichen Grundlagen sind speziell zu erwähnen die **elektronische Buchführung** (Finanzbuchhaltung und Betriebsbuchhaltung) inkl. der elektronischen Aufbewahrung der Bücher und der dazugehörenden Belege. Die Möglichkeit der **elektronischen Rechnungsstellung,** welche von den Steuerbehörden akzeptiert wird und der Abschluss von Verträgen in schriftlicher Form auf digitalem Weg. Letzteres ist seit 1. Januar 2005 mit dem Inkrafttreten des Bundesgesetzes über elektronische Zertifizierung auch in der Schweiz möglich.

Anforderungen an die elektronische Archivierung

Die Hauptherausforderung bei der Archivierung ist die Festlegung der **organisatorischen und verfahrenstechnischen Anforderungen,** um die Beweiskraft der elektronischen Daten und Dokumente während der gesamten Dauer der Aufbewahrung sicherstellen zu können. In technischer Hinsicht ist zu beachten, dass die digitalen Dokumente schon in einer Art und Weise erstellt

werden, die auf einfache und kostengünstige Art über mehrere Jahre eine beweisgültige Archivierung ermöglichen.

Dabei muss vorerst der **Ursprung,** dass heisst die ursprüngliche, grundsätzliche, korrekte Erstellung des digitalen Dokumentes nachgewiesen werden. Die wesentlichen Elemente sind hier die Integrität, die Nichtabstreitbarkeit von Versand, Empfang und die Authentizität. Wird zur Absicherung die Signatur eingesetzt, ist es wichtig, dass diese als solche wiederum auf Integrität, Authentizität und Berechtigung zu prüfen und damit verbunden das zugrundeliegende Zertifikat oder mitverwendete Zeitstempel zu kontrollieren. Werden anderen Methoden als die Signatur zur sicheren Archivierung verwendet, sind wieder andere Elemente für kontinuierliche Sicherheit zu beachten.

Während der Aufbewahrung muss das gesamte Datenverarbeitungsverfahren sicherstellen, dass die Dokumente in nachweisbarer Beweisqualität die ganze Zeit über verfügbar sind. Damit dieses Ziel erreicht werden kann, sind eine Vielzahl von Vorkehrungen notwendig, welche in den verschiedenen gesetzlichen Grundlagen oder Selbstregulierungen gefordert werden. Dazu zählen nebst der **Verfügbarkeit** der **Daten** die Verfügbarkeit der **Software,** mit der die Daten lesbar gemacht werden können, und die Verfügbarkeit der **Hardware,** respektive der Lesegeräte.

Das verwendete **Verfahren** zur elektronischen Archivierung muss grundsätzlich **dokumentiert** werden, sowohl von der Sache her (Systematik der Ablage, Datenbestände, Verarbeitungsregeln, Schnittstellen zu anderen Systemen etc.) als auch von der technischen Seite her (verwendete Software, Releasestand, verwendete Tabellen etc.). Zudem sind die notwendigen Prozesse für den Anwender in Form von Arbeitsanweisungen festzuhalten.

Um die **Beweisqualität über mehrere Jahre** sicherzustellen, müssen Daten vielleicht umkopiert oder konvertiert werden. Solche Vorgänge müssen detailliert dokumentiert werden. Die Beweisqualität wird deshalb auch dadurch sichergestellt, dass keine auch nur kleinste Veränderung ohne Dokumentation vorgenommen wird und die Daten während der ganzen Aufbewahrungsdauer innert nützlicher Frist wieder in ausgedruckter Form lesbar gemacht werden können. Es stellt sich aber die Frage, ob die reine Dokumentation von Veränderungen genügt, oder ob ergänzend nicht noch Stichproben die Vollständigkeit und ausreichende Überführung oder Konvertierung belegen sollen.

Restrisiko

Auch bei sorgfältigster Einhaltung der Anforderungen an die elektronische Archivierung verbunden mit der Umsetzung von IT-Governance gibt es immer wieder Situationen, die einen Zugriff auf beweistauglich archivierte Daten verunmöglichen. Exemplarisch wird dies im folgenden aufgezeigt.

- Es wurden Daten auf einer Compact Disc abgespeichert, und diese wurde korrekt in einem Tresor aufbewahrt. Der spätere Versuch, auf die Daten zuzugreifen, war aber unmöglich. Abklärungen ergaben, dass die Beschriftung der Compact Disc (verwendete Methode und Farbe) bewirkt hatte, dass diese diffundierte und die Compact Disc zerstörte und die Daten unlesbar machte. Die Auswirkungen der verwendeten Schriften waren im Zeitpunkt der Compact Disc Erstellung nicht bekannt, im Gegenteil, es war ein sehr verbreitetes Verfahren.

- Um auf gespeicherte Daten greifen zu können und diese wieder lesbar zu machen, muss Software mitverwendet werden. Die dafür notwendige Software (Applikationssoftware, Betriebssysteme, Bibliotheken, Framework, Datenbankrelease etc.) ist in der notwendigen Version nicht mehr vorhanden. Dies kann eintreten, weil man vergessen hat, die dazu gültige Version für Archivzwecke zu lizenzieren oder weil die notwendigen Lizenzen wegen Kündigung oder Konkurs des Softwarehauses nicht mehr gültig sind.

- Mit den Daten wurden auch Lesegeräte, das heisst sämtliche notwendige Hardware, archiviert. Beim Versuch, auf die Daten zuzugreifen und diese wieder lesbar zu machen, stellt sich heraus, dass die Hardware nicht mehr funktioniert (Stillstandsschäden oder ähnliches). Ersatzteile oder Ersatzgeräte sind aber nirgends mehr beschaffbar.

- Um die Daten in beweisbarer Qualität wieder lesbar zu machen, muss auf die Dokumentation zurückgegriffen werden. Bei der Lektüre und Analyse der Dokumentation stellt sich heraus, dass diese in wenigen, aber doch wesentlichen, Punkten, wie beispielsweise Passwörter, ungenügend ist. Dass diese Erläuterungen aus heutiger Sicht zur Verfahrensdokumentation, beispielsweise Prüfbarkeit sehr wichtig sind, war dazumal nicht bekannt.

Die oben aufgeführten Beispiele lassen sich sicher beliebig ergänzen. Dabei ist allen gemeinsam, dass im Rahmen der Archivierung in guten Treuen **sämtliche gesetzlichen Anforderungen eingehalten** wurden und sich nachträglich **wider Erwarten Probleme** ergeben haben.

Konsequenzen der Beweislosigkeit

Wenn es auf Grund eines technischen oder organisatorischen Problems nicht mehr möglich ist, auf archivierte Daten zuzugreifen oder die Beweistauglichkeit archivierter Daten nachzuweisen, ist die Folge Beweislosigkeit. **Die Konsequenzen der Beweislosigkeit sind dieselben, wie das Fehlen eines Rechtsanspruches.** Konkret heisst dies, dass die beweislose juristische oder natürliche Person rechtlich mit denselben Konsequenzen konfrontiert wird, wie wenn sie gar nie zu diesem elektronischen Dokument bzw. elektronischen Daten gelangt wäre, weil der Lebenssachverhalt nicht vorlag oder wie wenn sie sich die Mühe der Archivierung gar nie genommen hätte.

Dies ist mit **Kostenfolgen** verbunden, denke man nur an mögliche Forderungen oder Nachforderungen der Mehrwertsteuerbehörden, der Sozialversicherungsanstalten, von Lieferanten, Arbeitnehmern oder weiteren potenziellen Gläubigern. Aber auch der (vielleicht erfolglose) Versuch, den Zugriff auf beweistaugliche Daten irgendwie wieder zu bewerkstelligen, ist mit hohen Kosten verbunden.

Verantwortlichkeiten für die Folgen der Beweislosigkeit

In erster Linie ist es sicher Aufgabe der Führungsorgane jeder Stufe sicherzustellen, dass eine rechtsgenügliche elektronische Archivierung dauernd sichergestellt werden kann. Dies impliziert die notwendigen Zielsetzungen und entsprechenden Massnahmen und Mittel auf der strategischen und operativen Führungsebene. Da die strategische Führung letztlich die Gesamtverantwortung trägt, sollten Archivierungsfragen Eingang in **IT-Governance** Konzepte finden. Diesbezügliche Unsorgfalt führt zu **persönlicher Haftung der Führungsverantwortlichen** (Verwaltungsräte, Stiftungsräte etc.).

Auch die operativ mit der Archivierung betreuten Personen, welche diesbezügliche einzelarbeitsvertragliche Pflichten inne haben, können sich bei deren Verletzung verantwortlich machen.

Archivierungskonzepte und Systeme werden in der Regel von spezialisierten Anbietern eingeführt. Liegt der Grund für die entstandenen Probleme bei einer **Nicht- oder Schlechterfüllung** der diesbezüglichen Leistungen, kann (beim Vorliegen klarer und guter Verträge!) auf diese Unternehmungen Rückgriff genommen werden.

Ergibt sich ein Problem, das, auch bei der Einhaltung maximaler Führungs- und Arbeitssorgfalt, von einem Spezialisten nicht voraussehbar war, so wird dieser Schaden nicht abwälzbar sein und somit von der Unternehmung selber getragen werden müssen.

Escrow-Risiko-Management

Um das Risiko von Beweislosigkeit zu verringern, drängen sich ergänzende weitere Massnahmen auf. Eine mögliche Lösung dieser Probleme wäre der Abschluss von Escrow-Agreements, analog der bekannten Modelle, bei denen unter bestimmten Voraussetzungen (beispielsweise Konkurs eines Softwarelieferanten) auf Quellcodes etc. zugegriffen werden kann. Es kann Sinn machen, **Notfall-Escrow-Regelungen für Archivierungsfragen,** verbunden mit Risikoprophylaxe-Massnahmen zu installieren. Eine auf Archivierung spezialisierte Unternehmung, folglich mit spezifischem Know-how in technischen und rechtlichen Fragen, müsste gegen Entgelt folgende Dienstleistungen erbringen:

- Aufbewahrung sämtlicher verwendeter **Software** (Betriebssystem, Applikationssoftware, Datenbankversionen etc.) in kompilierter und nicht komplizierter (Source-Code) Form inklusiv Dokumentation, welche für einen Zugriff notwendig ist.
- Kontrolle und Aufbewahrung sämtlicher Dokumentationen (Konvertierungen, Emulationen, Prüfpfad etc.).
- Aufbewahrung und Wartung, regelmässige Inbetriebnahme von **Hardware und Datenträgern,** um rechtzeitig Probleme feststellen zu können.

Damit die Archivierungs-Escrow-Spezialistin diese Aufgaben erfüllen kann, müsste sie den tatsächlichen, regelmässigen und physischen Zugriff auf alle notwendigen Komponenten haben. Zudem muss ihr vertraglich das Recht eingeräumt werden (Lizenzen), diese Tätigkeiten auszuführen. Darauf muss bei der Aushandlung der Verträge mit den verschiedenen Archivierungsanbietern (Hardware und Software) geachtet werden.

Zusammenfassung

Zusammenfassend kann Folgendes festgehalten werden:

- Die Erstellung und Aufbewahrung elektronischer Dokumente ist aufgrund von immer mehr Gesetzen möglich und in wirtschaftlicher Hinsicht attraktiv.

- Um die Beweistauglichkeit der archivierten Dokumente von der Erstellung bis zum Ende der Aufbewahrungsdauer sicherzustellen, ist eine Vielfalt von technischen und organisatorischen Anforderungen einzuhalten.
- Kann auf ein elektronisches Dokument nicht mehr zugegriffen werden oder verliert es die Beweistauglichkeit, entstehen für die betroffene Unternehmung sehr hohe Kosten.
- Das Risiko der Beweislosigkeit kann mit spezifischen Escrow-Management-Vorkehrungen verringert werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und leitet den Fachhochschul-Lehrgang Wirtschaftsinformatik an der Hochschule für Wirtschaft HSW Luzern der Fachhochschule Zentralschweiz. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig. Informieren Sie sich unter www.hsw.fhz.ch

18.1.2005