Die elektronische Beweisführung

Die Beweisführung mit elektronischen Archivobjekten: Herausforderungen – Hypothesen – Entwicklung

Dr. iur. Bruno Wildhaber CISA/ CISM, Wildhaber Consulting, Schwerzenbach; bruno@wildhaber.com; www.wildhaber.com

Die Beweisführung der Zukunft basiert auf elektronischen Mitteln. Wie sieht diese aus und was muss bereits heute berücksichtigt werden?

Wir alle wissen, dass die heute aktive Generation noch immer in «Papierkategorien» denkt. Viele von uns legen wichtige Dokumente noch immer in Papierform ab: «man weiss ja nie…!»

Bereits die kommende Generation wird sich mit dieser Haltung wohl kaum mehr identifizieren. In Zeiten der SMS-Kommunikation und dem codierten, prozessoptimierten Datenaustausch sind «klassische» Dokumente wohl kaum mehr in dem Mass gefragt wie heute. Trotzdem müssen wir uns damit befassen, wie wichtige Dokumente, bzw. Archivobjekte für die Zukunft richtig archiviert – und wiedergegeben – werden können. Wie müssen elektronische Dokumente archiviert werden, damit sie auch in zehn Jahren noch über genügend Beweisqualität verfügen? Wie können solche Dokumente im Verfahrensfall korrekt vorgelegt werden?

Ausgangslage

Die neuen Aufbewahrungsvorschriften des Obligationenrechts wie auch andere Spezialgesetze erlauben die ausschliessliche Datenhaltung und -archivierung in elektronischer Form[1]. Bis jetzt wurde jedoch kaum darüber diskutiert, wie denn im Streitfall solche elektronischen Dokumente einem Richter, bzw. der zuständigen Instanz vorgelegt werden sollen. Heute verlassen sich die Richter in der Regel auf die Ausweichklauseln in den Gesetzen, die die Vorlage eines Dokuments «in direkt lesbarer Form» verlangen. Diese Vorschrift besagt aber lediglich, dass ein beweistauglicher Inhalt eines Dokuments in einer Form vorgelegt werden sollte, welcher vom Richter unmittelbar wahrgenommen werden kann. Wie dies in zehn Jahren geschehen wird, darüber können wir heute nur spekulieren.

Über die Beweisqualität wird damit aber keine Angabe gemacht. Da der Grundsatz der freien Beweiswürdigung weiterhin gilt, gibt es keinen absoluten Massstab für das «Richtig» oder «Falsch».

Wer weiss, welchen Bedrohungen ein ungeschütztes E-Mail ausgesetzt ist, ist sich bewusst, dass dessen Beweiswert ohne zusätzliche Sicherheitsmassnahmen gleich Null ist. Dieses Wissen bleibt heute in der Regel Sicherheitsexperten vorbehalten. In naher Zukunft wird sich dieses Wissen verbreiten und die Richter und Gegenanwälte werden mit Sicherheit vermehrt kritische Fragen zur Herkunft einzelner Beweismittel stellen.

Dieser Artikel soll die angesprochenen Themen etwas näher beleuchten. Es besteht indes nicht der Anspruch, die angesprochenen Fragen zu lösen. Vielmehr soll ein Anreiz an interessierte Kreise gegeben werden, sich mit den angesprochenen Themen vermehrt auseinander zu setzen.

Fallstudien

Fall 1: Kurzfristige Beweisführung

Ein Bauherr gibt den Auftrag an einen Unternehmer, die Fertigtreppe Typ 123 zu liefern. Der Auftrag läuft über den Architekten. Der Unternehmer liefert die falsche Treppe, nämlich Typ 456. Dadurch ergibt sich eine Bauverzögerung von 6 Wochen. Wer trägt den Schaden?

Der Unternehmer argumentiert, die Bestellung sei ihm per E-Mail zugegangen und legt das E-Mail als Beweis vor.

Fall 2: Geldwäscherei

In einer Geldwäschereiuntersuchung wird festgestellt, dass von einer Treuhandfirma in Liechtenstein offenbar diverse Beträge an ein Konto in Zürich verschoben wurden. Das Treuhandunternehmen verfügt nicht mehr über die Unterlagen, da der Fall 12 Jahre zurückliegt und der Kunde nur 2 Jahre aktiv war. Die Bank hat die Transaktionsunterlagen in ihrem internen Archivsystem gespeichert und herausge-

geben. Das Archivsystem wurde auf der Basis von digitalen Signaturen gesichert.

Die Beschuldigte argumentiert, dass diese Daten nicht vertrauenswürdig seien, weil die damals eingesetzte Technologie nicht mehr als sicher betrachtet werden könne.

Problemstellung

Wo liegt die Problemstellung bei diesen Fällen? Wir sehen, dass es sich um zwei völlig verschiedene Szenarien handelt, die auf den ersten Blick nichts miteinander zu tun haben. Es lassen sich jedoch gemeinsame Elemente erkennen:

1. Es geht um Beweisführung, d.h. das Belegen eines vermuteten, bzw. behaupteten Sachverhalts.
2. In beiden Fällen geht es um elektronische Dokumente oder um elektronische Daten.
3. In einem Fall geht es um eine zivilrechtliche Streitigkeit, im anderen um eine strafrechtliche Untersuchung.
4. Die finanziellen Konsequenzen können in beiden Fällen gross sein.
5. Die Diskussion dreht sich um die Urheberschaft der Daten, den Originalbegriff, die Art der Datenspeicherung und um die Erstellung der Dokumente.
6. Wie kann das elektronische Beweisstück dem Richter vorgelegt werden und was braucht es dazu?
7. Die zeitliche Dimension spielt eine wichtige Rolle.

Wo lassen sich nun mögliche Schwachstellen im gezeigten Prozess finden? Wie könnte ein möglicher Gutachter die Beweisqualität des Dokuments anfechten und somit die Beweisführung durch die Gegenpartei beeinflussen, bzw. verunmöglichen?

Einwände gegen die Beweisqualität

Grundsätzlich kann man drei Bereiche unterscheiden, welche von Bedeutung sind:

- Die Qualität der Ur-/Rohdaten (Archivobjekte) und die damit verknüpften Prozesse
- Die Präsentation/Vorlage der Dokumente
- Die Auslegung der Präsentation

Im Rahmen der Archivierung befassen wir uns hauptsächlich mit der ordnungsgemässen Abwicklung der Speicherung der Rohdaten, selten oder fast nie mit der Präsentation, geschweige denn mit deren Auslegung.

Der Geschäftsprozess als Ausgangspunkt

Man kann sich den gestellten Fragen von verschiedenen Ebenen her nähern. Der Zugang hängt nicht zuletzt vom Erfahrungsschatz und der damit mitgebrachten Praxis ab. Als Jurist betrachtet man das Thema vielleicht eher vom Objekt her, d.h. vom vorgelegten Beweismittel. Als Betriebswirtschafter oder Informatiker eher von der organisatorischen, bzw. technischen Seite.

Ich entscheide mich meist für den Geschäftsprozess. Jedes Dokument ist Teil eines Geschäftsprozesses. Eine Bestellung wie im Fall 1 wird über mehrere Stationen zum Ziel übermittelt und es wird eine Aktion ausgelöst. Wird das Dokument nicht mehr benötigt, kann es entweder direkt vernichtet werden oder es wird abgelegt, bzw. später archiviert.

Der Lebenszyklus eines Dokuments ist im Wesentlichen in 2 Hauptphasen zu unterteilen, nämlich in die aktive Phase und die Archivphase. Die Dauer der aktiven Phase kann unterschiedlich lang sein[2]. In der Regel dürfte sich die Mehrzahl der Dokumente aber einer sehr kurzen, aktiven Phase «erfreuen». Je nach Archivierungsanforderung werden die Dokumente zum Archivierungszeitpunkt, d.h. vom Übergang von der aktiven in die Archivphase, in den Status «archiviert» überführt. In der Praxis hat sich eine klare Trennung dieser Phasen etabliert. Sie wird auch vom Gesetz gefordert (Art. 1 Abs. 7 GeBüV). Der Zeitpunkt des Übergangs in das Archiv kann aber stark variieren[3].

Das Verfahren der digitalen Signatur dient als Mittel zur Integritätssicherung von Dokumenten und zum Nachweis der Urheberschaft.

Kurz und bündig

Archivierung ist nur dann von Wert, wenn die gespeicherten Objekte auch richtig wiedergegeben werden können. Bei der Umsetzung von Archivlösungen muss dieser Grundsatz im Vordergrund stehen.
In Zukunft werden viele Beweisverfahren mit elektronischen Beweismitteln geführt werden. Damit diese Daten auch in Zukunft noch über die notwendige Beweisqualität verfügen, müssen verschiedene Massnahmen getroffen werden. Dazu gehört die Wahl des Archivformats, aber auch die Auswahl der zur Beweisvorlage notwendigen Mittel. Die Präsentation von Daten kann zudem zum Problem werden, wenn die Darstellung nicht mehr dem Originalformat entspricht, bzw. auf völlig anderen Geräten wiedergegeben wird.
Elektronische Signaturen sind universell einsetzbar, verlangen aber nach neuen Standards, um die Beweisqualität der archivierten Objekte zu erhalten.

Bei der Betrachtung der Präsentationsproblematik spielt dieser Phasenübergang eine wesentliche Rolle, weil die Archivformate möglichst einheitlich sein müssen. Nur durch eine Reduktion der Formatvielfalt kann eine langfristige Wiedergabe garantiert werden. Dies im Gegensatz zur aktiven Phase, in welcher eine Vielzahl von Formaten vorliegt.

Ordnungsmässigkeit

Die Gutachter werden sich in jedem Fall auf die Ordnungsmässigkeit stützen: Was war zum Zeitpunkt der Speicherung allgemein anerkanntes Verfahren zur Bearbeitung der Daten? Beispielsweise dürfte man an die operative Behandlung von E-Mails im Jahr 1995 wesentlich geringere Anforderungen stellen können als an ihre heutigen Pendants.

Wer weiss, welchen Bedrohungen ein ungeschütztes E-Mail ausgesetzt ist, ist sich bewusst, dass dessen Beweiswert ohne zusätzliche Sicherheitsmassnahmen gleich Null ist.

Die Ordnungsmässigkeit bezieht sich auf alle Aspekte des Dokumentenmanagements und auch auf den Betrieb der IT. Die Beweisqualität hängt demnach wesentlich von der Qualität der eingesetzten Betriebsprozesse und der IT ab. Eine ex post-Betrachtung ist meist kaum möglich, da Aussagen über die Qualität der IT höchstens bei grossen Organisationen vorhanden sind (Revisionsberichte). Kann das Unternehmen nachweisen, dass es die IT Governance im Griff hatte und über die entsprechenden Verfahren verfügte, stellt dies ein wichtiges Indiz für die Qualität der damaligen Prozesse dar. Aus diesem Grund wird auf die IT Governance hoher Wert gelegt[4]. Ansonsten wird sich ein Gutachter an einem damaligen Durchschnittsstand orientieren müssen.

Die folgenden Kriterien sind für die Qualität der Archivobjekte von Bedeutung:

Vollständigkeitsprüfung

Die Vollständigkeitsprüfung bei der Archivierung von zusammengehörenden Dokumenten ist wichtig, weil einzelne Dateien in der Regel nicht aussagekräftig sind. Dateien müssen mit zusammengehörenden, langfristig gültigen Metadaten gespeichert werden[5]. Diese Metadaten geben Auskunft über den zugrunde liegenden Geschäftsfall, bzw. die Vollständigkeit eines Dokumentensatzes, der im Rahmen eines bestimmten Prozesses anfällt.

Mehrfachhaltung von Archivdaten

Die redundante Haltung von Archivdaten kann eine bedeutende Schwachstelle darstellen, weil dadurch eine effiziente Überwachung der Archivobjekte nicht möglich ist. Zudem werden dadurch wesentliche Geldmittel gebunden. Die vollständige Vernichtung kann damit ebenfalls zum Problemfall werden, dies auch im Lichte der Datenschutzvorschriften.

Unklarer Archivzeitpunkt

Wie kann beweisen werden, dass ein bestimmter Datenbestand zum Zeitpunkt T tatsächlich ins Archiv überführt wurde? Hier gibt es unterschiedliche Lösungsansätze. Im Extremfall wird man diesen Prozess durch eine externe Stelle beglaubigen lassen (Notariatsdienste). Die von uns untersuchten Verfahren orientieren sich in der Regel an den Time Stamping-Methoden, wobei es unterschiedliche Implementierungen gibt, die alle ihre Vor- und Nachteile aufweisen. Der Einsatz dieser oder jener Methode ist Risk Management-basierend und bedeutet, dass die Organisation über die entsprechende Entscheidungskompetenz verfügt.

Der Einsatz digitaler Signaturen

Das Verfahren der digitalen Signatur dient als Mittel zur Integritätssicherung von Dokumenten und zum Nachweis der Urheberschaft. Im Wesentlichen geht es auch nicht um den Einsatz der Signatur zur Authentifizierung, sondern um die Integritätsabsicherung. Man kombiniert eine Signatur mit einem Zeitstempel, dessen Zeitquelle als vertrauenswürdig gilt.

Wo liegen die hauptsächlichen Schwierigkeiten beim Einsatz solcher Signaturen? Im Gegensatz zu traditionellen WORM-Medien nimmt die Qualität der Verfahren und Kom-

Literatur

Beglinger Jacques/Lehmann Beat/Neuenschwander Peter/Wildhaber Bruno, Records Management (RM), Zollikon 2004, (zitiert: RM), www.aufbewahrung.ch

Pordesch Ulrich, Die elektronische Form und das Präsentationsproblem, Baden-Baden 2002

Projekt ARCHISIG: www.archisig.de

Long Term Archiving and Notary Services (LTANS) der Internet Engeneering Task Force (IETF): Brandner, R./ Hunter B., Evidence Record Syntax (ERS) http://www.ietf.org/internet-drafts/

ponenten (Algorithmen, Schlüssel) ab. Man muss demnach sicherstellen, dass die Verifikation der Daten jederzeit auf einem sicheren Ausgangsbestand basiert. Dies bedeutet, dass man diese Daten regelmässig migrieren muss[6].

Die heute in den Signaturgesetzen beschriebenen Verfahren und Standards erlauben es nicht, digital signierte Dokumente über einen langen Zeitraum (> 5 Jahre) in der notwendigen Qualität zu archivieren. Will man dies tun, so benötigt man eine Erweiterung der erwähnten Standards[7].

Die Präsentation (Beweisvorlage)

Herausforderungen

Bei der Wiedergabe können Probleme auftreten, wie wir sie von den klassischen Dokumenten heute nicht gewohnt sind. So kann durch die Substitution eines Fonts ein falsches Schriftbild entstehen. Daten können auf zu kleinen Bildschirmen unrichtig angezeigt werden (Handys, PDAs). Wenn Software und Hardware benötigt werden, kann es sein, dass die notwendigen Komponenten nicht mehr vorhanden sind.

Hier zeigt sich wieder die Wichtigkeit des gewählten Archivformats. Müssen Daten vor ihrer Darstellung interpretiert werden, bedeutet dies einen zusätzlichen Unsicherheitsfaktor[8]. Können die Daten aus sich selbst heraus interpretiert werden, dann ist dies ein Vorteil, ähnlich gut sind Formate, die auf Open Source-Standards basieren. Je weniger Hilfsmittel zur Interpretation notwendig sind, umso weniger kann die Qualität der Wiedergabe angezweifelt werden.

In diesem Zusammenhang stellt sich natürlich die Frage, was die «richtige» Wiedergabe sei. Dabei steht das richtige Verständnis für den Begriff «Integrität» im Mittelpunkt.

Integrität ist nicht gleich Integrität

In der Diskussion um die ordnungsgemässe Archivierung wird meist vergessen, dass es DIE Integrität nicht gibt. Niemand verlangt, dass ein archiviertes Objekt auf immer und ewig in der ursprünglichen Form archiviert wird. Es ist vielmehr damit zu rechnen, dass bei langen Aufbewahrungsdauern Migrationen (Kopieren ohne Veränderung) und Transformationen stattfinden. Transformation bedeutet, dass Daten verändert werden. Damit dies möglich ist, müssen bereits während der aktiven Phase die Integritätsanforderungen definiert werden. Diese sind Teil der Dokumentenklassierung. So ist für einzelne Objekte die bildliche Wiedergabe ein Muss, für die Mehrheit wird dies jedoch kaum der Fall sein. Die Wiedergabe muss aber den definierten Integritätskriterien entsprechen. Nur so kann die Beweisqualität erhalten werden. Gleiches gilt in Fällen, wo logisch zusammengehörige Objekte zu einem Geschäftsfall gebündelt wurden, auch diese dürfen nicht auseinander gerissen werden.

Schlussfolgerungen

Die Wiedergabe eines Dokuments sollte bei allen Betrachtungen rund um die Archivierung im Vordergrund stehen, nicht die Speicherung! Die Vielzahl der Faktoren, welche die Qualität eines Archivobjektes beeinflussen, hat direkte Auswirkung auf die zukünftige Beweisqualität. In der Praxis zeigt sich, dass diese Themen noch kaum beachtet werden.

Die Verfahren der digitalen Signatur können hier Abhilfe schaffen, doch sind auch sie nur auf den Kurzfristbeweis ausgelegt. Die Langfristarchivierung mit elektronischen Signaturen ist heute keineswegs gelöst und wird sicher zu einem wichtigen Thema in der nahen Zukunft. ■

Fussnoten und Links

1 RM, 34 ff.
2 RM, 101
3 RM, 126
4 RM, 18 ff.; Risk Management ist dabei Teil der IT Governance
5 RM, 128
6 RM, 108
7 RM, 107 ff.; LTANS; Archisig
8 Sehr umfassend Pordesch 51 ff.