Zugänglichkeit contra Sicherheit?*

Digitale Archivalien zwischen Offline-Speicherung und Online-Benutzung

Von Christian Keitel

Nach einem Jahrzehnt der grundlegenden theoretischen Überlegungen scheint sich im Diskurs der elektronischen Archivierung ein grundlegender Wandel anzubahnen. Viele Archive werden in den nächsten Jahren gezwungen sein, konkrete Schritte zur langfristigen Erhaltung digitaler Unterlagen zu unternehmen. Bisherige Grundsätze müssen erneut geprüft und die Ergebnisse praktisch umgesetzt werden. Die konkreten Möglichkeiten zur Realisierung der elektronischen Archivierung werden daher zunehmend in den Vordergrund rücken. Dabei können unter anderem die folgenden Fragen gestellt werden:

- Wie können digitale Unterlagen sicher gespeichert werden? Ist es möglich, die Unversehrtheit dieser Unterlagen über einen sehr langen Zeitraum sicherstellen?
- Wie können authentische digitale Unterlagen genutzt werden? Wie können wir den Benutzern gewährleisten, dass sie auch eine authentische Kopie der Unterlagen und nicht eine durch unberechtigte Eingriffe[1] veränderte Kopie einsehen?
- Wer kann die anfallenden Kosten bezahlen?

Der größte Teil der entstehenden Kosten dürfte bei den Personalkosten anfallen. Die Vielzahl komplexer und neuartiger Probleme erfordern gut vorbereitete und eingehend geschulte Archivare. Außerdem müssen zur Bewältigung der technischen Anforderungen auch IT-Techniker oder Informatiker in den Prozess der elektronischen Archivierung eingebunden werden. Neben diesen Personalkosten entstehen durch Refreshing, Migration, klimatisierte Räume etc. auch erhebliche Sachkosten. Bei der elektronischen Langzeitarchivierung werden daher durch

---

* Vortrag auf Elektronisches Archivgut - Metadaten, Fachverfahren, Publikationen, 6. Tagung des Arbeitskreises "Archivierung von Unterlagen aus digitalen Systemen" am 5./6. März 2002, URL: http://www.sachsen.de/de/bf/verwaltung/archivverwaltung/veroeffentlichungen_onlinepublikationen.html.

[1] Es sei hier darauf hingewiesen, dass die Unterlagen im Laufe der Zeit durch die notwendigen Migrationen auf jeden Fall verändert werden.

besonders geschultes und ausgebildetes Personal (Archivare und Informatiker) und die nötigen Sachmittel erhebliche Kosten anfallen. Drei Beispiele mögen dies verdeutlichen. Die Kosten für die elektronische Langzeitarchivierung über einen Zeitraum von 10 Jahren schätzten:

- Michael Wettengel für das Bundesarchiv auf 2,4 Mio. € (4,77 Mio. DM).[2]
- Bruce Ambacher für die National Archive and Records Administration (NARA) der Vereinigten Staaten auf 15,5 Mio. € (13,5 Mio. $).[3]
- Bruce Ambacher für ein kleineres Archiv auf 378.000 € (329.000 $).[4]

Diese Kosten können von den wenigsten Archiven alleine getragen werden. Als eine mögliche Lösung bietet sich die Kooperation zwischen mehreren Archiven an.[5] Viele Archive werden daher in kleineren oder größeren Zusammenschlüssen Zentren zur elektronischen Archivierung aufbauen oder Dienstleister wie z.B. Rechenzentren mit dieser Aufgabe betrauen. Bei einer derartigen Lösung werden die anfallenden laufenden Kosten zwischen den einzelnen Archiven aufgeteilt. Damit kommen auf das einzelne Archiv erheblich niedrigere Kosten zu, als dies bei einer eigenständigen elektronischen Archivierung der Fall gewesen wäre.

Vergleichbare Erwägungen haben die Arbeitsgruppe „Archivierung elektronischer Akten“ des Vereins Schweizerischer Archivarinnen und Archivare (VSA) bewogen, ein koordiniertes Vorgehen der Schweizerischen Archive zu empfehlen.[6] Danach übergeben die schweizerischen Archive ihre digitalen Unterlagen einem oder mehreren Kompetenzzentren, die dann für die technische Seite der Aufbewahrung sowie der Benutzung zuständig sind. Die Archive der gesamten Schweiz kommen demnach im Gebiet der elektronischen Archivierung in den nächsten 8 Jahren auf Kosten in Höhe von 16,8 Mio. € (25 Mio. SFr). Die für eine eigenständige elektronische Archivierung der einzelnen Archive aufzubringenden Mittel dürften um ein vielfaches höher liegen. Andere Beispiele für eine solche Kooperation stellen die deutschen staatlichen Archivverwaltungen, die bereits jetzt im Bereich der

---

[2] Michael Wettengel, 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, hier S. 197 f.

[3] Appendix 4 in Charles Dollar, Authentic Electronic Records: Strategies for Long-Term Access, Chicago, Illinois 2000, S. 207-213.

[4] Ebenda.

[5] Digital Culture: Maximising the Nation's Investment. A Synthesis of JISC/NPO Studies on the Preservation of Electronic Material, hrsg. v. Mary Feeney, London 1999, S. 18 f., abrufbar unter http://www.ukoln.ac.uk/services/elib/papers/other/jisc-npo-dig/dig2.pdf.

[6] Gesamtschweizerische Strategie zur dauerhaften Archivierung von Unterlagen aus elektronischen Systemen, Thomas Schärli u.a, Basel 2002.

Bestandserhaltung durch zentrale Werkstätten oder bei den audiovisuellen Medien über spezialisierte Einrichtungen verfügen, welche die Medien stellvertretend für die anderen Archive pflegen bzw. aufbewahren.
Auch bei einer Kooperation in der elektronischen Archivierung bietet es sich schon aufgrund des notwendigen technischen Equippments und der fachlichen Betreuung an, die digitalen Archivalien an einem zentralen Ort zu speichern. Abgesehen von dem Speicherarchiv werden daher die anderen zu dem Archivverbund gehörenden Einrichtungen nicht mehr Aufbewahrungsort für ihre Unterlagen sein. Die bisherige Benutzungspraxis, also Aushebung der bestellten Archivalien und Einsicht in den Lesesälen der Archive, kann nicht dadurch fortgeschrieben werden, dass dort Computer für die Nutzung digitaler Archivalien aufgestellt werden. Es sollte daher überlegt werden, ob nicht Wege gefunden werden können, die eine Nutzung dieser zentral gespeicherten Unterlagen in den am Verbund beteiligten Archiven selbst ermöglichen.
Grundsätzlich ist eine Benutzung digitaler Archivalien sowohl offline als auch online möglich. Eine Offline-Benutzung kann durch die Ausgabe von Wechseldatenträgern oder einen lokalen Zugriff auf die Festplatte eines Rechners realisiert werden. Online ist eine Zugriff auf die digitalen Archivalien entweder innerhalb eines geschlossenen Intranets oder im prinzipiell offenen Internet möglich. Die Offline-Speicherung digitalen Archivguts gehört nach Udo Schäfer zu den vier wesentlichen Maßnahmen, welche die Authentizität digitalen Archivguts im diplomatischen Sinne gewährleisten können.[7] Das deutsche Bundesarchiv hat diesen Ansatz konsequent umgesetzt. Jedes Archivale wird in zwei Kopien offline gespeichert. Der Benutzer erhält auf einem Wechseldatenträger eine eigene Benutzungskopie.[8] In dem skizzierten Modell eines Archivverbundes würde eine Offline-Lösung zu folgenden Konsequenzen führen:

- Die Erschließung erfolgt am Speicherort, da nur dort das nötige technische Equippment vorhanden ist und ein Transport der Datenträger zu den zuständigen Archiven nicht sicher und kostengünstig zu realisieren ist.[9]

[7] Udo Schäfer, Authentizität. Vom Siegel zur digitalen Signatur, in: , in: Udo Schäfer und Nicole Bickhoff (Hrsg.), Archivierung elektronischer Unterlagen (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg: Serie A, Landesarchivdirektion, H. 13), Stuttgart 1999, S. 165 – 181, hier S. 179.
[8] Wettengel, Infrastruktur, S. 195.
[9] Ob mittel- oder langfristig aufgrund der von der Behörde gelieferten Metadaten auf eine erschließung digitaler Unterlagen verzichtet werden kan, kann hier nicht weiter erörtert werden.

- Die Benutzung findet aus denselben Gründen am Speicherort oder durch Wechseldatenträger statt. Zukünftige Benutzer müssen daher bei Recherchen über größere Zeiträume zunächst in die Papierarchive, dann in den Speicherort der digitalen Archivalien gehen. Der unterschiedliche Aufbewahrungsort von papierner und digitaler Überlieferung führt dazu, dass die Überlieferung einer Provenienz nicht mehr als zusammengehörig gesehen wird. Besonders problematisch erscheint dieser Umstand bei Hybridakten. Zwar ist eine Übernahme von Akten, die sowohl papierne als auch digitale Bestandteile haben, grundsätzlich abzulehnen. Entweder sollten die digitalen Teile ausgedruckt und folglich nur eine Papierakte oder die analogen Teile eingescannt und dann nur eine digitale Akte übernommen werden. Letztere Variante ist auch im DOMEA-Konzept vorgesehen.[10] Dennoch ist es nicht unwahrscheinlich, dass in den nächsten Jahren auch Hybridakten in die Archive kommen werden. Die einzelnen Bestandteile einer Hybridakte wären dann bei reiner Offline-Speicherung des digitalen Teils in zwei verschiedenen Archiven untergebracht.
- Die anderen beteiligten Archive mittelfristig zu toten Archiven, d.h. zu Archiven ohne weitere Zugänge, weiterentwickeln.
- Aus Gründen der Datensicherung ist es empfehlenswert, die beiden Archivierungskopien an unterschiedlichen Orten zu lagern. Selbst die vollständige Zerstörung der Daten an einem Ort würde dann zu keinen größeren Datenverlusten führen.[11] Die Übermittlung einer Kopie an einen zweiten Ort muss durch den Transport des Datenträgers erfolgen und ist durch den Verzicht auf eine Übertragung via Netzwerktechnologie erschwert.
- Die archivische Betreuung der Unterlagen ist erschwert, wenn die technische Seite der Archivierung (Speicherung, Refreshing, Migration) an ein Rechenzentrum vergeben werden sollte.

Eine reine Offline-Strategie lässt sich in den Bereichen Betreuung, Sicherung und Benutzung kaum mit einer zentralen Speicherung der Archivalien innerhalb eines

---

[10] „Für die Aussonderung muss eine vollständige Ausgabe elektronischer und hybrider Akten auf nur *einem* Medium gewährleistet sein. Aus diesem Grund sind gegebenenfalls bis zur Aussonderung noch in analoger Form aufbewahrte Schriftstücke aus Hybridakten zum Zweck der Aussonderung in ein elektronisches Format zu übertragen.“ Konzept zur Aussonderung elektronischer Akten (Schriftenreihe der KBSt Bd. 40), Bonn 1998, S. 41 (Hervorhebung im Original).

[11] Kleinere Verluste könnten dann entstehen, wenn auch einer der verbliebenen Datenträger nicht mehr gelesen werden kann. In diesem Fall kann dann nicht auf einen zweiten Ersatz-Datenträger ausgewichen werden.

Archivverbundes vereinbaren. Der Einsatz von Netzwerktechnologien sollte daher auch im Bereich der elektronischen Archivierung diskutiert werden. In Deutschland spielt das Thema „Netzwerktechnologien“ bislang in den Diskursen über elektronische Archivierung nur eine marginale Rolle. Als Gefahren wurden Abhören, Beschädigung der Daten durch Viren oder technische Defekte sowie absichtliches Löschen genannt. Die Vermeidung dieser Gefahrenpotentiale ist Voraussetzung für eine Online-Übermittlung digitaler Archivalien. Dabei sind zwei Varianten denkbar.

- Einstellung in das Internet für eine theoretisch unbegrenzte Zahl unbekannter Benutzer.
- Einstellung in einem vom Internet abgeschotteten Intranet mit einer begrenzten Zahl bekannter Benutzer.

Aufgrund seiner Verbreitung und der freien Zugänglichkeit erscheint das Internet aus Sicht der Benutzer als erste Wahl. Es ist daher leicht nachzuvollziehen, dass auch bei den elektronischen Archiven der internationale Trend zur Online-Benutzung über das Internet geht. Die National Archives and Records Administration, Washington (NARA) registriert eine wachsende Erwartung, dass Information kostenlos und über das Internet abgegeben wird.[12] Ein französischer Normentwurf geht ebenfalls von einer Online-Nutzung aus.[13] Das National Digital Archive of Datasets (NDAD) in Großbritannien ist bereits jetzt vollständig webbasiert.[14] Diese vom Rechenzentrum der University of London (ULCC) betriebene Einrichtung archiviert für das Public Records Office strukturierte Daten wie Datenbanken und Geographische Informationssysteme Sämtliche Hilfsmittel sind frei über das Internet zugänglich, die elektronischen Unterlagen können nach einer einfachen Zertifizierung ebenfalls über das Netz eingesehen werden. Trägt diese Lösung aber auch in einem Archivverbund? Auch im Falle einer Benutzung durch das Internet sollten die einzelnen Unterlagen in mindestens zwei Archivkopien gespeiert werden. Wenn der Zugriff auf eine dieser Kopien aus dem Internet erfolgen sollte, muss diese Kopie mit Hilfe einer sehr aufwändigen und damit entsprechend teuren Sicherheitsarchitekur vor Veränderungen geschützt werden. Erfolgt der Zugriff auf eine andere, gespiegelte Kopie, ergeben sich ebenfalls weitere Kosten. Zwar wären in diesem Fall die beiden archivischen Kopien vor unberechtigter Änderung und Löschung

---

[12] Kenneth Thibodeau, La communication des archives électroniques, Vortrag, gehalten auf den Journées Internationales Archivage des Documents Électroniques, Paris 8.3.2001.
[13] Vgl. NF Z 42-013, nicht publiziert.
[14] http://ndad.ulcc.ac.uk/.

geschützt. Dennoch müsste durch entsprechende Sicherheitsmaßnahmen gewährleistet werden, dass die Benutzer authentische und damit unveränderte Kopien der archivischen Originale einsehen können. Aus diesen Gründen erscheint eine ausschließlich auf dem Internet basierende Archivierungslösung nur für Einzelfälle finanzierbar.

Für einen Zugang über ein Intranet stehen mit Wide Area Network (WAN) und Virtual Private Network (VPN) zwei Lösungen zur Verfügung. Bei einem Wide Area Network werden feste Telekommunikationsleitungen angemietet, über die alle Niederlassungen eines Unternehmens miteinander verbunden werden. Auf diese Weise entsteht ein Netz, das physisch vom Internet getrennt ist. Weitergehende Sicherheitsvorkehrungen werden nicht vorgenommen, d.h. ein Wide Area Network wird in der Regel ohne zusätzliche Verschlüsselung der Daten betrieben.

Bei einem Virtual Private Network wird dagegen auf der physischen Struktur des Internets ein logisches und nach außen abgeschlossenes Netz aufgebaut. Ein Ausgangsrouter verschlüsselt die Daten und schickt sie mithilfe eines Tunneling-Verfahrens (IPsec) über das Internet an den Empfänger, dessen Entschlüsselungsrouter sie dann dekodiert. Als Ergebnis liegt ein geschlossenes Netz (Intranet) auf Internetbasis vor, welches auch als Extranet bezeichnet wird.

Die beiden Möglichkeiten zum Betrieb eines Intranets unterscheiden sich hinsichtlich der Kosten, Flexibilität und Sicherheit erheblich. Ein Wide Area Network erfordert zunächst relativ geringe Einstandskosten, führt dann aber zu hohen Kosten für den laufenden Betrieb. Ein weiterer Kostenfaktor entsteht beim Betrieb eines Wide Area Network, wenn die Daten aus Sicherheitsgründen doch verschlüsselt werden sollen. Während des Betriebs ist ein Wide Area Network verhältnismäßig unflexibel, da bereits bei der Einführung die Bandbreite des Netzes definiert werden muss, die dann schnell überdimensioniert (mangelnde Auslastung) oder unterdimensioniert sein kann. Bei einem Virtual Private Network sind zwar die Einstandskosten durch Sicherheits- und Verschlüsselungsmechanismen sowie Router-Kosten höher als bei einem Wide Area Network, der laufende Betrieb gestaltet sich dagegen meist erheblich günstiger. Auch richtet sich die benötigte Bandbreite jeweils nach dem benötigten Volumen. Vor allem gilt aber ein Virtual Private Network im Vergleich mit einem Wide Area Network als sicherer.[15]

---

[15] http://www.dud.de/dud/grundschutz/bsi-gshb-online/m/m5083.htm. Die hier und im folgenden zitierten Links verwiesen am 3.7.2002 auf existierende Ziele.

Bei der Einrichtung eines Intranets ist also ein Virtual Private Network einem Wide Area Network vorzuziehen. Auch aus datenschutzrechtlicher Sicht wird die Einrichtung von Virtual Private Networks begrüsst und teilweise sogar gefordert:

- In Hamburg richtete das Landesamt für Informationstechnik (LIT) erstmals ein „virtual private network“ (Virtual Private Network) innerhalb des IP-Netzes der Freien und Hansestadt Hamburg ein. Der Hamburgische Datenschutzbeauftragte bemerkte in seinem 17. Tätigkeitsbericht hierzu: „Wir begrüßen ausdrücklich diesen ersten Ansatz zur physikalischen Verschlüsselung von Daten im Netz der hamburgischen Verwaltung und hoffen, daß er sich zukünftig auch auf andere sensible Bereiche ausdehnen läßt.“[16]
- Das IT-Grundschutzhandbuch 2001 des Bundesamts für Sicherheit in der Informationstechnik führt aus: „Erfolgt eine Übertragung personenbezogener Daten vom Standort des Arbeit- bzw. Auftraggebers zu einem "entfernten" Arbeitsplatz (z. B. eines Telearbeiters), so müssen die datenschutzrechtlichen Bestimmungen Beachtung finden. Gemäß § 9 BDSG muss in solchen Fällen insbesondere verhindert werden, dass Unbefugte mit Hilfe von Einrichtungen zur Datenübertragung IT-Systeme nutzen (Benutzerkontrolle). Weiterhin ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle).“...“ Werden über einen Transportweg regelmäßig oder dauerhaft personenbezogene Daten ausgetauscht, sollte die Übertragung mit Hilfe eines virtuellen privaten Netzes (Virtual Private Network) gesichert werden“[17]
- Die dänische Datenschutzbehörde hält einen Zugriff auf eine von einem Krankenhaus geführte medizinische Datenbank über das Internet dann vertretbar, wenn dieser über ein Virtual Private Network erfolgt.[18]

---

[16] 17. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht öffentlichen Bereich 1998/1999, Abschnitt 3.11. http://www.hamburg.de/fhh/behoerden/datenschutzbeauftragter/tb/tb17/tb17.pdf und http://www.hamburg.de/fhh/behoerden/datenschutzbeauftragter/tb/tb17/3.html.

[17] Kap. M 2.205: Übertragung und Abruf personenbezogener Daten, http://www.dud.de/dud/grundschutz/bsi-gshb-online/m/m2205.htm. http://www.dud.de/dud/grundschutz/bsi-gshb-online/menue.htm.

[18] Dritter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Gemeinschaft und in Drittländern. Berichtsjahr 1998, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp35de.pdf.

Der Einsatz eines Virtual Private Network wird daher aus datenschutzrechtlicher Sicht gerade für die Übermittlung von besonders sensiblen Daten wie z.B. personenbezogenen, medizinischen oder Haushaltsdaten empfohlen. Neben diesen unmittelbaren Aussagen über die Sicherheitsvorkehrungen eines Virtual Private Network lässt sich die gebotene Sicherheit auch daran ablesen, dass bereits heute verschiedene Einrichtungen auf ein Virtual Private Network zurückgreifen, um ihre sensiblen Daten intern auszutauschen:

- Das Notarnetz der Bundesnotarkammer realisiert auf der Basis eines Virtual Private Network den elektronischen Datenaustausch zwischen den Notaren, deren Standesorganisationen sowie den staatlichen Behörden und Gerichten.[19]
- Die Anwender des Wissenschaftsnetz Baden-Württemberg (BelWue) sind teilweise über ein Virtual Private Network an das Landesverwaltungsnetz (LVN) angeschlossen. Beispielsweise realisiert die Landesarchivdirektion Baden-Württemberg wie zahlreiche andere Dienststellen im Bereich des Ministeriums für Wissenschaft, Forschung und Kunst auf diese Weise ihren LVN-Zugang einschließlich der Übermittlung ihrer Personal- und Haushaltsdaten.[20]
- Die Kommunikation zwischen den baden-württembergischen Museen und dem Bibliotheksservice-Zentrum in Konstanz innerhalb des Projekts MusIS erfolgt über ein Virtual Private Network. MusIS steht als Abkürzung für *Mus*eums-*I*nformations-*S*ystem und will als Projekt des Ministeriums für Wissenschaft, Forschung und Kunst alle Arbeitsbereiche in den staatlichen Museen Baden-Württembergs vernetzen. Dabei werden auch sensible Daten wie der finanzielle Gegenwert der Objekte übermittelt.

Nach Abwägung der Faktoren Kosten, technische Sicherheit, Datenschutz und Einsatz erscheint daher ein Virtual Private Network auch für ein archivisches Intranet gut geeignet. Es ist mit diesem Mittel möglich, digitale Archivalien sicher online zu übermitteln. Damit stehen in zentralen archivischen Arbeitsbereichen eine Reihe neuer Möglichkeiten zur Verfügung. Bereits das DOMEA-Aussonderungskonzept

---

[19] Schreiben des Präsidenten der Bundesnotarkammer an die Bundesministerin der Justiz vom 26.07.2000 (Bericht gemäß § 82 Abs. 3 BNotO) (abgedruckt in DNotZ 2000, 564): Bericht über die Tätigkeit der Bundesnotarkammer im Jahre 1999, http://www.bnotk.de/BNotK-Service/Taetigkeitsberichte/bericht_1999.htm. http://www.bnotk.de/Informationen_Presse/Wir_ueber_uns/wirueberuns.html.

[20] BelWü/LVN Sicherheitskonzept, V 1.1 vom 20.2.2002.

sieht bei der Bewertung vor, dass über das Bundesbehördennetz auf die Akten zugegriffen werden kann.[21] Auch einer Übernahme von digitalen Unterlagen über ein Virtual Private Network stehen keine grundsätzlichen Sicherheitsbedenken im Wege.[22] Auch die Speicherung und Benutzung digitaler Archivalien sollte vor dem Hintergrund der dargestellten Ergebnisse neu überdacht werden. Die Befürworter einer reinen Offline-Lösung legen den Schwerpunkt ihrer Argumentation auf die Sicherheit der Daten. Auf der Seite der Online-Vertreter wird ein anderes Sicherheitskonzept vorgelegt und der Aspekt der Benutzung stärker berücksichtigt. Es liegt daher nahe, beide Konzepte miteinander zu verbinden. So wäre es denkbar, digitale Archivalien in zwei offline gespeicherten Kopien zu sichern und in einer dritten Kopie in einem archivischen Intranet sowie einer vierten Kopie im Internet zugänglich zu machen. Die bei diesem Verfahren zu veranschlagenden Kosten dürften aber relativ hoch sein. Auch verkennt eine solche Lösung, dass bei einem Zugang über ein archivisches Intranet hohe Sicherheitsstandards eingehalten werden können. Schließlich können die Bereiche der Benutzung und Speicherung nicht vollständig gegeneinander abgegrenzt werden, da die Benutzer stets den Anspruch stellen werden, authentische Unterlagen einsehen zu können. Auch die zur Benutzung bereitgestellten Kopien müssen deshalb umfangreichen Sicherungsmaßnahmen unterliegen. Statt einer bloßen Addition beider Ansätze sollte daher schon aus Kostengründen versucht werden, eine erhöhte Sicherheit durch die wechselseitige Ergänzung beider Sicherheitskonzepte zu erzielen und die bei der elektronischen Archivierung anfallenden Kopien nach ihren Funktionen zu unterscheiden.

Bei einer Offline-Speicherung der Erstkopie könnte ein Online-Zugang in einem archivischen Intranet auf die Zweikopie und im Internet auf eine Drittkopie ermöglicht werden. Die Erstkopie kann als Authentikum verstanden werden, da an die Integrität und Authentizität ihrer Daten die höchsten Anforderungen gestellt werden. Sie sollte auf einen nur einmal beschreibbaren Datenträger kopiert und offline an der Stelle gespeichert werden, an der auch die Eingangsbearbeitung erfolgte. Die Erstkopie sollte den Ausgangspunkt für die notwendigen Kopier- und Migrationsgänge darstellen.

---

[21] Konzept zur Aussonderung elektronischer Akten, S. 42.

[22] Vorerst dürfte dieser Weg bei den aktuellen Netzkapazitäten auf kleiner Dateien beschränkt sein.

Zweit- und Drittkopie können zur Absicherung der Überlieferung online an einen zweiten Speicherort übermittelt und dort für eine Online-Benutzung eingesetzt werden. Auf sie erfolgt der Zugriff der Archivare und der externen Benutzer. Dabei ist zu fragen, an welchen Orten welche Personengruppen auf welche Kopien zugreifen können. Zur Beantwortung dieser Frage sollte zwischen den unterschiedlichen Zugriffsformen auf die Archivalien unterschieden werden. Genutzt werden können digitale Unterlagen

1. vom Archivar im Archiv (z.B. zur Erschließung),
2. vom Benutzer im Archiv,
3. vom Benutzer zu Hause über das Internet,
4. vom Benutzer zu Hause anhand eines Wechseldatenträgers.

Zu 1. und 2.: Das speichernde Archiv und die anderen am Verbund beteiligten Archive sind über ein mittels Virtual Private Network realisiertes Intranet miteinander verbunden. Problematische Stellen sind dabei die Rechner der Archivare und der Nutzer. Die Rechner im Benutzersaal können durch technische Maßnahmen (Versiegelung bzw. Verlötung der Schnittstellen) abgesichert werden. Archivare hatten auch bisher schon unbeschränkten Zugang zu konventionellem Schriftgut. Es besteht keine Notwendigkeit, dies für elektronische Unterlagen anders zu handhaben. Für die Fälle 1 und 2 müssen daher keine eigenen Benutzungskopien angefertigt werden.

Zu 3.: Der Zugriff über das Internet kann entweder auf die Zweitkopie oder auf die Drittkopie erfolgen. Bei einem Zugriff auf die Zweitkopie wären allerdings wie bereits ausgeführt sehr hohe Sicherheitsvorkehrungen zu treffen. Es erscheint daher sicherer und günstiger, die Daten als Drittkopie auf einem eigenen Server bereitzustellen.

zu 4.: Dem Benutzer wird eine eigene Kopie angefertigt. Diese Möglichkeit ist z.B. bei sozialwissenschaftlichen Datenarchiven notwendig, die in die Struktur der digitalen Archivalien zu Zwecken der Auswertung eingreifen müssen.[23]

[23] Wettengel, Infrastruktur, S. 195.