HTW Chur
Hochschule für Technik und Wirtschaft

Fachhochschule Ostschweiz
University of Applied Sciences

Churer Schriften
zur Informationswissenschaft
Herausgegeben von
Robert Barth, Nadja Böller, Sonja Hierl, und Hans-Dieter Zimmermann

Arbeitsbereich
Informationswissenschaft

Schrift 28

Datensicherung in Bibliotheksverbünden

Analyse der Sicherung von Benutzer- und bibliographischen Daten am Bsp. ausgewählter Institutionen

Nadine Wallaschek

Chur 2009

Churer Schriften zur Informationswissenschaft
Herausgegeben von Robert Barth, Nadja Böller, Sonja Hierl, und Hans-Dieter Zimmermann
Schrift 28

Datensicherung in Bibliotheksverbünden

Analyse der Sicherung von Benutzer- und bibliographischen Daten am Bsp. ausgewählter Institutionen

(Originaltitel der Diplomarbeit: Datensicherung in Bibliotheksverbünden. Empfehlungen für die Entwicklung von Sicherheits- und Datensicherungskonzepten in Bibliotheksverbünden)

Nadine Wallaschek

Diese Publikation entstand im Rahmen einer Diplomarbeit zum Abschluss als dipl. Informations- und Dokumentationsspezialistin FH.

Referent: Prof. Dr. Bernard Bekavac

Korreferent: Prof. Dr. Rüdiger Buchkremer

Verlag: Arbeitsbereich Informationswissenschaft

ISSN: 1660-945X

Chur, März 2009

Abstract

Bibliotheksverbünde koordinieren die Zusammenarbeit der Bibliotheken untereinander durch einheitliche Regelungen der Katalogisierung und Fernleihe. Neben den beratenden, betreuenden und unterstützenden Aufgaben stellen sie den teilnehmenden Bibliotheken i.d.R. auch weitreichende Informatik-Dienstleistungen zur Verfügung. Auf zugehörigen Datenbank-Servern werden dabei sowohl bibliographische als auch Benutzerdaten zentral verwaltet. Um eine Beschädigung oder gar einen Verlust dieser Daten zu verhindern, müssen präventive und reaktive Massnahmen zur Datensicherung konzipiert und umgesetzt sein.

Die vorliegende Arbeit ermöglicht – ausgehend von einem theoretischen Teil über generelle Möglichkeiten zur Gewährleistung der Datensicherheit – Einblicke in die Sicherheits- und Datensicherungskonzepte zweier wissenschaftlicher Bibliotheksverbundorganisationen aus der Schweiz und einer aus Deutschland. Basierend auf den dabei gewonnenen Erkenntnissen sowie weiteren Literaturanalysen werden Empfehlungen für die Planung und/oder Überarbeitung von sicherheitsspezifischen Konzepten in Bibliotheksverbünden gegeben.

Inhaltsverzeichnis

Abkürzungsverzeichnis

bspw.	beispielsweise
BSZ	Bibliotheksservice-Zentrum Baden-Württemberg
bzw.	beziehungsweise
ca.	circa
CD-ROM	Compact Disc Read-Only Memory
DVD	Digital Versatile Disc
DMZ	Demilitarisierte Zone
ggf.	gegebenenfalls
IDS	Informationsverbund Deutschschweiz
IP	Internet Protocol
IT	Informationstechnik
o. ä.	oder ähnlich/e/s
RAID	Redundant Array of Inexpensive/Independent Disks
s.	siehe
SAN	Storage Area Network
SWB	Südwestdeutscher Bibliotheksverbund
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP/IP	User Datagram Protocol / Internet Protocol
USV	Unterbrechungsfreie Stromversorgung
u. w.	und weitere/r
vgl.	vergleiche
WORM	Write Once Read Multiple Times
z.B.	zum Beispiel

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Die der vorliegenden Ausarbeitung zugrundeliegende Diplomarbeit entstand im Sommer 2007 zum Abschluss des Studiengangs Information Sciences an der HTW Chur. Ermöglicht wurde sie durch die Bereitschaft einiger im Bibliothekswesen tätiger Personen, mich durch die Preisgabe von Informationen zu internen Massnahmen zu unterstützen. Hierfür möchte ich mich bedanken.

Meinem Referenten, Herrn Prof. Dr. Bernard Bekavac, danke ich für die Betreuung meiner Diplomarbeit.

Ebenso bedanke ich mich bei Herrn Dr. Cornel Dora und Herrn Bernhard Bertelmann für die Idee, und Herrn Prof. Robert Barth für den Vorschlag des Themas.

Ich danke Frau Dr. Marion Mallmann-Biehler, Leiterin des Bibliotheksservice-Zentrums Baden-Württemberg, und Frau Esther Straub, IDS Verbundkoordinatorin der Universität Zürich, die meine Anfrage kurzerhand an die entsprechenden Stellen weitergeleitet haben. Für die Bereitschaft zur Auskunft und für die interessanten Einblicke gilt mein besonderer Dank Herrn Volker Conradt vom Bibliotheksservice-Zentrum Baden-Württemberg, Herrn Hansueli Locher von der Schweizerischen Nationalbibliothek und Herrn Simon Allemann von der Universität Zürich.

Ein herzlicher Dank gilt meinem privaten Umfeld für die Kraft und Unterstützung während meines Studiums und während der Diplomarbeitszeit.

1 Einleitung

Edmund Burke (1729 - 1797), Schriftsteller und irisch-englischer Politiker, stellte bereits vor mehr als zwei Jahrhunderten fest, was auch heute noch in vielen Bereichen gilt:

> *„Rechtzeitige und vorsorgliche Angst ist die Mutter der Sicherheit."*

Bezogen auf die vorliegende Ausarbeitung möchte ich dieses Zitat auf die Sicherung und Sicherheit von Daten abbilden. Denn gerade was den Umgang mit Daten betrifft, darf die Angst vor einer möglichen Beschädigung oder gar einem Verlust der Daten nie verloren gehen. In der Bibliothekslandschaft stellt sich somit die Frage, welche Gefahren für die Datensicherung von Benutzerdaten und bibliographischen Daten bestehen und welche Massnahmen sowohl vorsorglich als auch reaktiv auf ein eingetretenes Risiko ergriffen werden können.

1.1 Ausgangslange und Problemstellung

Immer mehr Schweizer Bibliotheken schliessen sich den verschiedenen Bibliotheksverbünden an, so dass diese immer grössere Mengen an Datenmaterial verwalten. Da bislang noch keine Bestandsaufnahme der Sicherheitsmassnahmen in den Verbundzentren und den einzelnen Partnerbibliotheken existiert, können auch keine Aussagen über die Sicherheit der verwalteten und gespeicherten Daten getroffen werden. Schutzmassnahmen zur Gewährleistung der Datensicherheit betreffen die folgenden Bereiche:

- Räumlichkeiten (Hardware, Leitungen)
- Verwendete Software
- Datensicherung (Backup und Firewall)
- Datenschutz

Diese Arbeit legt den Fokus auf den Bereich der Datensicherung in den Bibliotheksverbundszentren. Da die übrigen Aspekte die Datensicherung unterstützen, können diese nicht vollständig ausgeblendet werden und fliessen in entsprechendem Umfang in die Arbeit ein. Zu den zu sichernden Daten in Bibliotheksverbünden gehören sowohl die Benutzerdaten der Bibliothekskundinnen und Bibliothekskunden als auch die Daten der Bestände der Bibliotheken (bibliographische Daten).

Bibliotheksverbünde werden als zentrale Dienststellen für Bibliotheken verstanden, die den teilnehmenden Institutionen zentrale Informatik-Dienstleistungen anbieten. Zur Verfügung gestellt werden beispielsweise ein gemeinsamer Server für die Daten und eine zentrale Datenbank mit den Daten der Bestände, so dass mit nur einer Suchmaske gleichzeitig in allen Katalogen der einzelnen Bibliotheken nach Dokumenten gesucht werden kann.

1.2 Zielsetzung

Im Folgenden wird untersucht, ob in Schweizer Bibliotheksverbünden schriftlich dokumentierte Sicherheitskonzepte für die Datensicherung existieren und über welche inhaltlichen Schwerpunkte diese verfügen. Es wird aufgezeigt, welche sicherungsrelevanten Massnahmen für die Sicherung von Benutzerdaten und bibliographischen Daten ergriffen werden. Gleichzeitig werden die wichtigsten Aspekte für die Datensicherung in Bibliotheksverbünden identifiziert. Zu diesem Zweck werden die Bibliotheksorganisationen

- des Informationsverbundes Deutschschweiz (IDS) Universität Zürich und
- der Schweizer Nationalbibliothek

bezüglich ihrer Sicherheitspolitik befragt. Um den Blickwinkel etwas zu erweitern, wird zusätzlich ein grosser Bibliotheksverbund aus Deutschland,

- der Südwestdeutsche Bibliotheksverbund (SWB),

in die Untersuchung miteinbezogen.

Basierend auf der Analyse der Sicherheitskonzepte dieser ausgewählten wissenschaftlichen Institutionen sowie einer Vergleichsanalyse der gewonnenen Informationen sollen Ähnlichkeiten und Differenzen in der Sicherung von Daten in Bibliotheksverbünden festgestellt werden, so dass anschliessend Empfehlungen für die Datensicherung in den Schweizer Bibliotheksverbünden erarbeitet werden können. Für die Entwicklung der Empfehlungen fliessen neben den Erfahrungen aus den Sicherheitsmassnahmen der untersuchten Bibliotheksverbundorganisationen weitere Erkenntnisse aus der spezifischen Literatur zur Datensicherung ein.

Die Betrachtung der bestehenden Sicherheitsmassnahmen der analysierten Institutionen führt zu einem breiten Überblick über die Möglichkeiten, Daten in einem Bibliotheksverbund zu sichern. Die jeweiligen Sicherheitskonzepte werden allerdings nicht miteinander verglichen, um das „beste“ Konzept zu küren, sondern um den IST-Zustand darzustellen, anhand welchem Empfehlungen zur Vorgehensweise bezüglich der Datensicherung zusammengestellt und formuliert werden.

1.3 Methodik

Die genannten Ziele werden erreicht, indem Methoden der Literaturanalyse, der Befragung und der Vergleichsanalyse angewandt werden. Mit einer Literaturanalyse werden Massnahmen für die Sicherung von Daten identifiziert, anhand derer ein Fragebogen zur Evaluation des aktuellen Standes der Datensicherung in Bibliotheksverbünden entwickelt wird. Auf Grund der Verwendung eines Fragebogens ist die vorliegende Diplomarbeit somit dem wissenschaftlichen Bereich der empirischen Studien zuzuordnen.

1.3.1 Untersuchungsmethode Fragebogen

Für die Erhebung der Informationen zum Stand des Einsatzes von Sicherheitskonzepten in Bibliotheksverbünden wurde der Fragebogen als Untersuchungsform der Befragung gewählt. Diese Methode wurde dem Interview vorgezogen, da der zeitliche Rahmen der ursprünglichen Diplomarbeit die Organisation und Durchführung mehrerer Interviews nur schwer zuliess. Bei der angewandten Form der schriftlichen Befragung handelt es sich um eine Expertenbefragung, da eine wichtige Voraussetzung für die Gewinnung von relevantem Datenmaterial darin liegt, dass die Befragten über Fachkenntnisse im Bereich der Informationssicherheit und der Datensicherung verfügen. Der Fragebogen wurde aus diesem Grund den für die Datensicherung zuständigen IT-Verantwortlichen der jeweiligen Verbundorganisationen per E-Mail zugestellt.

Formal enthält der Fragebogen sowohl offene Fragen, die es den Befragten ermöglichen, ihre Antworten selbstständig zu formulieren (Atteslander, 2003, S.161), als auch geschlossene Fragen, bei denen entweder alle oder zumindest alle relevanten Antworten vorgegeben werden (Atteslander, 2003, S.162). Zusätzlich wurden den Befragten genügend Möglichkeiten gegeben, weitere Bemerkungen zu den einzelnen Fragen oder Themenbereichen anzubringen.

Für das Ausfüllen des Fragebogens standen den Befragten ein Worddokument und eine Onlineversion des Fragebogens zur Verfügung. Der Onlinefragebogen wurde mit 2ask, einem Internetdienst für Online-Umfragen (amundis communications GmbH, 2007), realisiert.

Da für die empirische Untersuchung nicht alle Bibliotheksverbünde der Schweiz analysiert werden konnten, was einer Vollerhebung (Atteslander, 2003, S.304) entspräche, handelt es sich um eine Stichprobe. Im Fall einer Stichprobe werden die Daten nicht von der Gesamtheit einer Zielgruppe erhoben, sondern nur von einem Teil dieser Gesamtheit (Atteslander, 2003, S.304). Für die vorliegende Stichprobe wurde eine Auswahl getroffen, die einen grossen Schweizer Bibliotheksverbund (IDS Universität Zürich), die Schweizer Nationalbibliothek auf Grund ihres spezifischen Auftrages, und, zur Erweiterung des Blickwinkels, einen grossen Deutschen Bibliotheksverbund (SWB) umfasst.

1.3.2 Aufbau des Fragebogens

Basierend auf der vorhergehenden Literaturanalyse zur Thematik der Datensicherung, der IT-Sicherheit und der Informationssicherheit wurde ein Fragebogen konzipiert, der nicht nur das Sicherheitskonzept an sich fokussiert, sondern auch präventive und reaktive Massnahmen zur Datensicherung und Datenrekonstruktion betrachtet.

Somit gibt der Fragebogen Aufschluss über folgende Aspekte:

- **Grundlegendes**
  - Bedeutung des Themas „Sicherheit“ in Strategie / Leitbild / Vision / Mission
  - Vorhandensein eines Sicherheitskonzepts für die Datensicherung der Benutzer- und Bestandsdaten
- **Sicherheitskonzept**[1]
  - Beeinflussung durch Gesetze, Vorschriften, Normen und Standards
  - Bedeutung der Themen Sicherheit und/oder Datensicherung im Sicherheitskonzept
  - Bedeutung der Sicherheitskriterien Verfügbarkeit, Vertraulichkeit, Integrität u. w.
  - Bereitschaft des Managements für die Bereitstellung der erforderlichen Mittel und Ressourcen
  - Ziele und Vorgaben zur Datensicherung
  - Beteiligte, Aufgaben, Verantwortlichkeiten
  - Sensibilisierung, Schulung und Übung der Beteiligten
  - Prüfung, Aktualisierung, Pflege und Weiterentwicklung des Sicherheits-Managements
  - Verpflichtung des Managements und der Mitarbeitenden zur Sicherheit
  - Regelung der Vergabe und Verwaltung von Zugriffsrechten
  - Richtlinien zum Aufbau und Wechsel von Passwörtern
- **Datensicherung / Backup-Management**
  - Art der Datensicherung (komplett, differenziell, inkrementell, selektiv)
  - Rhythmus der Datensicherung (zeitversetzt, zeitnah, Echtzeit)
  - Räumliche Trennung der Server
  - Backup nach dem RAID-Konzept
  - Manuelle oder automatische Datensicherung
  - Verantwortlichkeiten

[1] Die Begriffe Sicherheitspolitik, Sicherheitskonzept und Security Policy werden in der Literatur gleichbedeutend aufgefasst. Um Missverständnissen vorzubeugen, wird im Fragebogen der Begriff Security Policy verwendet. In der vorliegenden Arbeit werden die Begriffe Sicherheitskonzept und Security Policy abwechselnd gebraucht.

  - Prüfung der Backups auf Wiederherstellbarkeit
  - Sicherungssoftware
  - Arten der eingesetzten Speichermedien
  - Aufbewahrungsort der Backups
  - Dauer der Aufbewahrung

- **Firewall**
  - Verwendete Soft-/Hardware
  - Installation mit Standardeinstellung oder Anpassung an die Sicherheitsziele
  - Eingesetzte Firewall-Komponenten
  - Rhythmus der Aktualisierung der Firewall-Software

- **Risikoanalyse**
  - Regelmässige Durchführung von Risikoanalysen
  - Bekannte Risiken in der Datensicherung
  - Massnahmen zur Vermeidung dieser Risiken
  - Massnahmen bei Eintritt der bekannten Gefahren

- **Katastrophenplan / Notfallplan**
  - Existenz eines Katastrophen- oder Notfallplans
  - Existenz eines Wiederanlaufplans (Notfall Recovery)
  - Durchführung von Notfallübungen
  - Verantwortlichkeiten
  - Existenz eines Alarmierungsplans für Not- und Störfälle
  - Regelmässige Überprüfung der Funktionsfähigkeit des Notfallplans
  - Dokumentation von Notfällen

1.3.3 Pretest

Im Vorfeld der Erhebung wurde das Untersuchungsinstrument getestet, um unklare Begriffe und Fragen sowie weitere mögliche Missverständlichkeiten aufzudecken und vor dem Einsatz des Fragebogens zu klären. Für die Durchführung des Pretests wurde der Fragebogen zwei Personen, die im Arbeitsfeld der Informationstechnik (IT) sowie der Elektrotechnik tätig sind, vorgelegt. Auf Grund des Feedbacks wurden einige wenige Anpassungen in der Formulierung der Fragen vorgenommen.

1.4 Begriffsdefinitionen

Bevor nun mit der Untersuchung des Standes der Datensicherung in Bibliotheksverbünden begonnen werden kann, müssen zunächst einige wichtige Begriffe bestimmt und voneinander abgegrenzt werden. Auf diese Weise wird klar definiert, was unter den einzelnen Begrifflichkeiten zu verstehen ist, so dass Missdeutungen vorgebeugt wird. Der folgende Abschnitt behandelt die Begriffe „Bibliotheksverbund“ und „Datenschutz“, da diese für das Verständnis der Arbeit von Bedeutung sind. Weitere Begriffe wie „Datensicherheit“, „Datensicherung“ und „Sicherheitskonzept“ werden in den jeweiligen Kapiteln vertieft dargestellt und erläutert.

1.4.1 Bibliotheksverbund

Sowohl auf regionaler als auch auf nationaler Ebene schliessen sich seit Jahren immer häufiger Bibliotheken zu so genannten Bibliotheksverbünden, auch Bibliothekenverbünde genannt, zusammen. Eine einfache und allgemeingültige Erläuterung des Begriffs „Bibliotheksverbund“ beschreibt diesen deshalb als *„Zusammenschluss verschiedener Bibliotheken einer Region“* (Schalwat, 1995). Allerdings ist diese Definition verhältnismässig ungenau, da sie wichtige Aspekte und Voraussetzungen für einen Bibliotheksverbund nicht umfasst. Welche wesentlichen Aufgaben ein Bibliotheksverbund erfüllt, macht das St.Galler Bibliotheksnetz deutlich, wenn es sich darstellt als

> *„Bibliothekenverbund von 43 Bibliotheken, die gemeinsam mit dem Bibliothekssystem ALEPH eine Verbunddatenbank verwalten und dem Publikum einen Online-Katalog für bibliographische Recherchen und eine Dokumenten- und Buchbestellung anbieten.“*
> (St.Galler Bibliotheksnetz, 2007)

Ein Bibliotheksverbund ist nur unter der Voraussetzung funktionsfähig, dass alle am Verbund teilnehmenden Bibliotheken ihre Medien in einem einheitlichen Format elektronisch erfassen (Bauer, 1995). Grundsätzlich koordinieren Bibliotheksverbünde die Zusammenarbeit der Bibliotheken untereinander (Rasch, 2000), so dass bibliothekarische Aufgaben wie Katalogisierung und Fernleihe einheitlich geregelt werden. Verbundzentralen leisten somit Planungs- und Entwicklungsarbeit für die Vereinheitlichung der bibliothekarischen Datenverarbeitung (Hacker, 2000, S.54), was schlussendlich dazu führt, dass Aufträge effektiver und effizienter abgewickelt werden können.

Wie bereits unter 1.1 erwähnt, werden Bibliotheksverbünde im Folgenden als zentrale Dienststellen für Bibliotheken verstanden, die den teilnehmenden Institutionen zentrale Informatik-Dienstleistungen anbieten. So wird den Bibliotheken bspw. ein gemeinsamer Server sowie eine zentrale Datenbank mit den Daten der Bestände aller teilnehmenden Bibliotheken zur Verfügung gestellt.

1.4.2 Datenschutz

Die vorliegende Arbeit befasst sich nicht ausführlich mit dem Thema Datenschutz. Da dieser jedoch eng verbunden mit der Informationssicherheit und der Datensicherung ist, wird der Begriff an dieser Stelle kurz erläutert und von den Begriffen der Datensicherheit und der Datensicherung abgegrenzt.

In der Schweiz gilt das Bundesgesetz über den Datenschutz (DSG), welches den *"Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden"* (DSG, 2006, S.1) bezweckt.

Nach dem DSG dürfen Daten nicht beliebig *"beschafft, aufbewahrt, verwendet, umgearbeitet, bekannt gegeben, archiviert oder vernichtet"* (DSG, 2006, S.2) werden, weshalb das DSG und weitere kantonale Datenschutzgesetze regeln, wie mit Personendaten umzugehen ist (Datenschutzbeauftragter Kanton Zürich, 2005). Neben den nationalen existieren europaweit und international geltende Richtlinien, die ebenfalls der Verhinderung möglicher Missbräuche von personenbezogenen Daten dienen (Datacom, 2007). Vordergründig handelt es sich beim Datenschutz demnach um den Schutz der Persönlichkeit und der Privatsphäre, und betrifft weniger die Daten an sich (Datenschutzbeauftragter Kanton Zürich, 2005). Neben den rechtlichen Grundlagen zum Schutz von Persönlichkeit und Privatsphäre gewinnt auch der Aspekt der Sicherheit von Informationstechnologien an Bedeutung (Baeriswyl/Rudin, 2002, S.14). Die Entwicklung der Technologien schreitet unentwegt fort und bringt nicht nur Vorteile in der Sicherung von Daten mit sich, sondern forciert ebenso neue Gefahren wie bspw. durch Störungen der Informationsinfrastruktur. Dies führt dazu, dass Aspekte der Privatsphäre und der Sicherheit nicht mehr getrennt voneinander betrachtet werden, da sie häufig ineinander verwoben sind. So wirkt sich z.B. ein Zugriffsschutz auf Daten gleichzeitig auch auf die Privatsphäre der betroffenen Personen aus. (Baeriswyl/Rudin, 2002, S.14) In diesem Punkt schliesst sich der Kreis der gegenseitigen Beeinflussung von Datensicherheit, Datensicherung und Datenschutz, wie er für das Verständnis der Diplomarbeit nötig ist. Die Begriffe der Datensicherheit und der Datensicherung werden in Kapitel 2.1 ausführlich definiert.

1.5 Analysierte Institutionen

Nachfolgend sollen nun die Bibliotheksverbund-Institutionen kurz vorgestellt werden, deren Sicherheitsvorkehrungen bezüglich der Datensicherung im Rahmen der vorliegenden Ausarbeitung untersucht wurden, so dass ein kleiner Einblick in die Organisation und die Aufgabengebiete der Institutionen gegeben wird.

1.5.1 IDS Universität Zürich

Mehr als 100 Bibliotheken aus den Fakultäten der Universität Zürich sowie weiteren Hochschulen sind im Informationsverbund der Universität Zürich zusammen geschlossen und betreiben den gemeinsamen Bibliothekskatalog IDS Universität Zürich[2] (Dickenmann, 2007). Zu den Hochschulen, deren Bibliotheken am IDS der Universität Zürich teilnehmen, gehören die Pädagogische Hochschule Zürich, die Hochschule für Musik und Theater Zürich, die Hochschule für Angewandte Psychologie, die Interkantonale Hochschule für Heilpädagogik sowie das Staatsarchiv des Kantons Zürich, das Stadtarchiv Zürich, das Zentrum für Ausbildung im Gesundheitswesen Kanton Zürich und das Tibet-Institut Rikon. Eine Ausnahme bilden die Bibliotheken der Juristischen Fakultät, des Englischen Seminars und des Slavischen Seminars, da deren Bestände sowie der Bestand der Zentralbibliothek Zürich in einem anderen Verbund, dem NEBIS, nachgewiesen sind. Allerdings können beide Verbundkataloge über die IDS Zürich Recherche[3] gleichzeitig konsultiert werden. (Dickenmann, 2007)

Der Bibliothekskatalog des IDS Universität Zürich ermöglicht eine übergreifende Suche in allen Katalogen der am IDS Universität Zürich beteiligten Bibliotheken mit nur einer einzigen Suchanfrage. Ende des Jahres 2006 verzeichnete der Bibliothekskatalog bereits über 2,2 Millionen Einträge bibliographisch erschlossener Medien und weiterhin wird jährlich mit einem durchschnittlichen Zuwachs von 100'000 Dokumenten gerechnet (Dickenmann, 2007). Koordiniert wird der Informationsverbundes von der Abteilung IT/Verbund der Hauptbibliothek der Universität Zürich (HBZ), zu deren wichtigsten Aufgaben die folgenden gehören (Dickenmann, 2005):

- Koordination des Informationsverbundes der Universität Zürich
- Konfiguration des Bibliothekssystems ALEPH
- Erweiterung des Informationsverbundes
- Redaktion des Verbundkataloges
- Schulung und Betreuung der Bibliothekarinnen im Informationsverbund der Universität Zürich

[2] Der IDS-Katalog findet sich im Internet unter: http://biblio.uzh.ch/F/ [23.08.2007].

[3] Zur IDS Zürich Recherche gelangt man über den IDS-Katalog http://biblio.uzh.ch/F/, welcher oben rechts die Weiterleitung ermöglicht.

1.5.2 Schweizerische Nationalbibliothek

Das Bundesgesetz über die Schweizerische Nationalbibliothek (NB) legt den Auftrag der 1895 gegründeten NB (Bundesbehörden der Schweizerischen Eidgenossenschaft, 2006a) fest, nach welchem diese zur Aufgabe hat,

> *„gedruckte oder auf anderen Informationsträgern gespeicherte Informationen, die einen Bezug zur Schweiz haben, zu sammeln, zu erschliessen, zu erhalten und zu vermitteln.“* (Nationalbibliotheksgesetz, 1992)

Zusammengefasst werden all diese Informationen mit dem Fachbegriff „Helvetica“ bezeichnet, worunter Publikationen zu verstehen sind, die

- in der Schweiz erscheinen
- sich auf die Schweiz oder auf Personen mit schweizerischem Bürgerrecht oder Wohnsitz beziehen oder
- von schweizerischen oder mit der Schweiz verbundenen Autoren oder Autorinnen geschaffen oder mitgestaltet wurden.

(Bundesbehörden der Schweizerischen Eidgenossenschaft, 2006b)

Mittlerweile umfasst die Sammlung der Schweizerischen Nationalbibliothek mehr als drei Millionen Dokumente, die allen Interessierten zur Verfügung gestellt werden (Bundesbehörden der Schweizerischen Eidgenossenschaft, 2006a). Neben der Sammlung der
Helvetica schliesst die NB auch mehrere Spezialsammlungen und Spezialinstitutionen ein, zu deren wichtigsten das Schweizerische Literaturarchiv, die Graphische Sammlung und das Centre Dürrenmatt Neuchâtel gehören (Bundesbehörden der Schweizerischen Eidgenossenschaft, 2006a). Trotz dieser Angliederung externer Institutionen kann die NB nicht als eigentlicher Bibliotheksverbund bezeichnet werden. Auf Grund des besonderen Sammelauftrags zur Aufbewahrung und Vermittlung der Schweizer Literatur wird die Schweizerische Nationalbibliothek im Rahmen dieser Untersuchung dennoch berücksichtigt, um zu ermitteln, welche Massnahmen zur Sicherung der für die Schweizerische Geschichte bedeutenden Daten unternommen werden.

1.5.3 SWB – Südwestdeutscher Bibliotheksverbund

Ein besonders grosser Bibliotheksverbund ist der Südwestdeutsche Bibliotheksverbund, der die Medienbestände von mehr als 1'200 wissenschaftlichen Bibliotheken aus den Bundesländern Baden-Württemberg, Saarland und Sachsen sowie die Bestände weiterer Spezialbibliotheken in anderen Bundesländern verzeichnet (BSZ, 2007a). Im Online-Katalog des SWB sind mehr als 47,5 Millionen Bestandsnachweise zu über 12 Millionen

Titeln recherchierbar, wobei die Titelaufnahmen und Bestandsnachweise mehr als 1,2 Millionen Besitznachweise zu gut 350'000 Zeitschriftentiteln enthalten (BSZ, 2007b). Seit seiner Gründung im Jahr 1983 unterhält das Bibliotheksservice-Zentrum Baden-Württemberg den SWB und bietet damit die Möglichkeit, Bücher, Zeitschriften, Aufsätze, andere Medien und vermehrt auch elektronische Ressourcen (BSZ, 2007c) über einen Katalog in vielen Bibliotheken gleichzeitig zu suchen. Das BSZ übernimmt dabei eine bedeutende Rolle in der Koordination und Unterstützung der Bibliotheken und darüber hinaus der Archive und Museen der Region (BSZ, 2007d). Zu den wichtigsten Dienstleistungen, die das BSZ den Institutionen anbietet, zählen die Beratung, Betreuung und Unterstützung beim Einsatz und Betrieb von EDV-Systemen, dem Gesamtnachweis der Medienbestände und elektronischen Ressourcen aller am SWB beteiligten Bibliotheken und dem Betrieb und Unterhalt der bibliographischen Verbunddatenbank, welche zur kooperativen Katalogisierung, zur Literaturrecherche, zur Fernleihe und zur Dokumentenlieferung genutzt wird. Im Weiteren unterstützt das BSZ wissenschaftliche Bibliotheken bei der Beschaffung, Einrichtung und dem Betrieb der lokalen Bibliothekssysteme, entwickelt gemeinsam mit den wissenschaftlichen Bibliotheken die Digitale Bibliothek Baden-Württemberg und organisiert den Leihverkehr zwischen den Bibliotheken. (BSZ, 2007d)

Auf Grund der Grösse des Südwestdeutschen Bibliotheksverbunds ergibt sich die Wichtigkeit einer Auseinandersetzung mit der Frage nach der Datensicherung, um die Sicherheit der in der bibliographischen Verbunddatenbank verwalteten Daten zu gewährleisten.

Bevor nun die Sicherheitsvorkehrungen der vorgestellten Verbundorganisationen aufgezeigt werden, werden zunächst die nötigen Grundlagen zu den Themenbereichen Datensicherheit und Datensicherung, Sicherheits-Management, Sicherheitsprozess und Sicherheitskonzept behandelt.

2 Datensicherheit und Datensicherung

Im Bereich der Informationssicherheit nehmen die Datensicherheit und die Datensicherung zwei wichtige Positionen ein und sollen deshalb im folgenden Kapitel vertieft betrachtet und erläutert werden. Nach den begrifflichen Bestimmungen werden die unterschiedlichen Verfahren zur Datensicherung sowie mögliche Datensicherungsstrategien dargestellt. Abschliessend wird ein kurzer Exkurs zur technischen Datensicherungsmassnahme der Firewall unternommen.

2.1 Definition

Sowohl in der Literatur als auch im täglichen Sprachgebrauch wird Datensicherung auch als „Backup" (Hoppe/Priess, 2001, S.180) bzw. „Back-up" bezeichnet. Im Fachwesen der Informatik wird für die Datensicherheit ebenfalls häufig der englische Begriff „data security" verwendet. Die beiden Bereiche der Datensicherheit und der Datensicherung sind aber nicht nur eng miteinander verbunden sondern greifen gleichzeitig ineinander über. Dies zeigt sich in den Definitionen der Begriffe, die den Schluss nahe legen, dass es sich bei der Datensicherung um einen äusserst wichtigen Aspekt zum Erhalt der Datensicherheit handelt: Hansen und Neumann bezeichnen Datensicherheit als

> *„Verhinderung von Datenverlust, Datendiebstahl und Datenverfälschung. Durch vorbeugende Massnahmen soll die jederzeitige Vollständigkeit und Korrektheit der Daten gewährleistet werden."* (Hansen/Neumann, 2001, S.173)

Die Massnahmen, die zur Sicherheit der Daten führt, gehören zur Datensicherung, da diese

> *„das Anlegen von Sicherungskopien aller relevanten Datenbestände und deren Verwahrung an einem sicheren Ort beinhaltet."* (Hansen/Neumann, 2001, S.235)

Im Fall eines Störfalles, der einen Datenverlust oder eine Datenbeschädigung verursacht, dient die Datensicherung somit der schnellen und zuverlässigen Rekonstruktion der betroffenen Daten (Hansen/Neumann, 2001, S.235).

2.2 Verfahren

Um eine rasche Wiederherstellung der Daten zu erreichen, werden von den zu sichernden Datenbeständen in regelmässigen Zeitintervallen Sicherungskopien erstellt, die es ermöglichen, die Daten redundant zu halten (Hoppe/Priess, 2003, S.221). Für die Anfertigung von Sicherheitskopien stehen verschiedene Speichermedien zur Verfügung, auf denen die Daten gesichert werden können. Die Auswahl des geeigneten Datenträgers erfolgt nach Kriterien wie der Speicherkapazität, der Datenübertragungsrate von der

Festplatte auf das Speichermedium sowie den Kosten für die Datenträger und die benötigten Gerätschaften (Hansen/Neumann, 2001, S.235). Mögliche Speichermedien für die Datensicherung sind (Müller, 2003, S.96):

- Mikrofilme
- Optische Speichermedien: CD-ROM, WORM, DVD
- Magnetische Speichermedien: Disketten, Festplatten, Bänder/Tapes
- RAM: Random Access Memory (Halbleiterspeicher)

Allerdings eignen sich nicht alle Speichermedien gleich gut für die unterschiedlichen Anwendungsbereiche von Datenbeständen. Für einen Grossteil der privaten Computer-Nutzer sowie für Betriebe mit einem kleinen Datenbestand von wenigen Megabytes reichen Disketten bzw. CD-ROMs und DVDs auf Grund des angebotenen Speicherplatzes und der vergleichsweise niedrigen Kosten vollends aus. Anders verhält es sich in Institutionen, die über grosse Datenbestände verfügen, deren redundante Speicherung ausserordentlich wichtig ist. Diese Umgebungen erfordern möglichst ausfallsichere Speichermedien mit hoher Speicherkapazität.

2.2.1 Klassische Datensicherung

Das klassische Datensicherungsverfahren beruht auf dem Kopieren der Daten, die sich auf einem schnellen Speichermedium wie bspw. der Festplatte befinden, auf ein langsameres Speichermedium (z.B. Magnetband) mit grossem Speicherplatz (Schmidt, 2006, S.165). Zugegriffen und gearbeitet wird grundsätzlich nur auf dem schnellen Medium, so dass das Sicherungsmedium nur dann verwendet wird, wenn die Daten auf der Festplatte beschädigt wurden oder verloren gegangen sind. Für den Vorgang der Sicherung wird eine Datensicherungssoftware eingesetzt, die ebenfalls das Zurückspielen der Daten abwickelt. (Schmidt, 2006, S.165)

Datensicherungen können manuell durchgeführt werden, wobei Personen für die Auswahl des Sicherungsmediums und das Auswechseln der Datenträger verantwortlich sind (Hoppe/Priess, 2003, S.180). Um sich der Abhängigkeit der Datensicherung von bestimmten Personen oder Stellen zu entziehen, kann die Datensicherung automatisiert erfolgen. In diesem Fall läuft die Sicherung der Datenbestände nach definierten Sicherungsroutinen programmgesteuert ab (Hoppe/Priess, 2003, S.180). Durch den Einsatz von automatischen Datensicherungsrobotern, so genannten Autoloadern, die bspw. den Wechsel der verwendeten Sicherungsdatenträger durchführen, können zahlreiche Fehlerquellen vermieden werden, die auf menschlichem Handeln basieren (Hoppe/Priess, 2003, S.180).

2.2.2 Datensicherungsstrategien

Für die klassische Datensicherung existieren folgende Datensicherungsstrategien (Schmidt, 2006, S.166):

Vollständiges Backup (Full Backup)

Für ein vollständiges Backup werden bei jedem Sicherungsvorgang alle Daten komplett auf das Sicherungsmedium kopiert. Auf diese Weise steht beim Zurückspielen der Daten nach einem Störfall der gesamte Datenbestand im ursprünglichen Zustand zur Verfügung. Nachteilig wirken sich der grosse Zeitbedarf für die Datensicherung sowie die hohe benötigte Speicherkapazität des Sicherungsmediums aus.

Selektives Backup / Datenbackup (Partial Backup)

Im Gegensatz zum vollständigen Backup, welches alle Daten kopiert, werden bei einem partiellen Backup nur die Daten gesichert, die als sicherungswürdig eingestuft sind. Das zu sichernde Datenvolumen wird reduziert, da z.B. temporäre Dateien nicht gesichert werden, was dazu führt, dass auf dem Sicherungsmedium eine deutliche Ersparnis an Speicherplatz erzielt werden kann.

Differenzielles Backup

Sowohl beim vollständigen Backup als auch beim selektiven Backup wird ein Grossteil der Daten immer wieder gesichert, obwohl sich an diesem Teil des Datenbestandes nichts geändert hat. Um diese Vergeudung der Zeit- und Speicherplatzressourcen zu verhindern, werden bei einem differenziellen Backup nach einer einmaligen Sicherung des Datenbestandes nur noch die Daten gesichert, die Änderungen gegenüber der Anfangssicherung erfahren haben (Müller, 2003, S.113). Der Vorteil dieser Sicherungsmethode liegt darin, dass der Zeitbedarf für die Datensicherungen nach dem vollständigen Backup erheblich verringert wird und zugleich weniger Speichermedien erforderlich sind (Müller, 2003, S.113). Im Fall einer Rücksicherung (Zurückspielen des Datenbestandes) wird im Vergleich zu einem vollständigen Backup allerdings deutlich mehr Zeit benötigt, da nach dem Zurückspielen der vollständigen Datensicherung die danach veränderten Dateien vom differenziellen Backup zurückgespielt werden müssen (Müller, 2003, S.113).

Inkrementelles Backup (Incremental Backup)

Eine weitere Methode zur effektiven Ressourcennutzung besteht in der inkrementellen Datensicherung, bei welcher ebenfalls zunächst ein vollständiges Backup durchgeführt wird, auf welches weitere Datensicherungen folgen, die nur noch diejenigen Daten und Dateien sichern, welche sich gegenüber dem vorhergegangenen Sicherungslauf verändert haben (Müller, 2003, S.113).

Auch mit diesem Verfahren wird wie beim differenziellen Backup das zu sichernde Datenvolumen verringert, so dass die aufeinander folgenden Datensicherungen beschleunigt werden (Schmidt, 2006, S.166). Der Schwachpunkt dieser Datensicherungsstrategie liegt darin, dass bei einem Zurückspielen die einzelnen inkrementellen Datensicherung nach und nach in der richtigen Reihenfolge eingespielt werden müssen, was nicht nur kompliziert sondern auch zeitaufwändig ist (Müller, 2003, S.113).

Sicherungszyklus (Backup Rotation)

Im Bereich des Datensicherungs-Managements hat sich gezeigt, dass nicht nur eine Datensicherungsstrategie allein angewendet werden kann, sondern dass rotierende Sicherungsstrategien durchaus sinnvoll sind. Um Daten in einem Sicherungszyklus zu sichern, wird in einem ersten Schritt die Länge des Zyklus, bspw. eine Woche, im Rahmen eines Zeitraums festgesetzt. Zu Beginn des Zyklus, also z.B. zu Wochenbeginn, wird ein vollständiges Backup des zu sichernden Datenbestandes durchgeführt. Anschliessend erfolgen während des Zyklus in regelmässigen oder unregelmässigen Abständen inkrementelle Datensicherungen, bspw. täglich. Nach Abschluss des Zyklus beginnt der nächste Zyklus erneut mit einem vollständigen Backup.

Zusammenfassend ergeben sich folgende Vorteile und Nachteile der verschiedenen Datensicherungsstrategien (Müller, 2003, S.114):

Tabelle 1: Vor- und Nachteile der Datensicherungsstrategien

Sicherungsumfang	Zeitbedarf		Medien-verbrauch	Komplexität
	Sicherung	Rücksicherung		
Vollständig	Hoch	Gering	Hoch	Niedrig
Differenziell	Mittel	Mittel	Mittel	Mittel
Inkrementell	Gering	Hoch	Niedrig	Hoch

Was das partielle Backup anbelangt, können keine verallgemeinernden Angaben gemacht werden, da der Aufwand an Zeit und Speichermedien davon abhängt, wie gross die zu sichernden Teildatenbestände sind. Ebenso verhält es sich bei einem Sicherungszyklus, bei welchem die benötigten Ressourcen und die Komplexität von der Wahl der eingesetzten Datensicherungsstrategien beeinflusst werden.

2.2.3 Datenspiegelung

Steigende Produktionskapazitäten und sinkende Preise von schnellen Speichermedien (Schmidt, 2006, S.167) ermöglichen weitere interessante Verfahren zur Datensicherung, wobei vermehrt auf langsame Sicherungsmedien wie Bänder oder Disketten verzichtet werden kann. Die Datenspiegelung gehört zu diesen Ansätzen und basiert auf dem Prinzip, dass der gesamte zu sichernde Datenbestand auf zwei gleichartigen Speichermedien (z.B. Festplatten, Server) vorhanden ist. Im Fall eines Störvorfalls, der dazu führt, dass ein Speichermedium ausfällt, kann ohne Zeitverlust mit den redundanten Daten des zweiten Speichermediums weitergearbeitet werden. (Schmidt, 2006, S.167) Damit beide Medien über den exakt gleichen Datenbestand verfügen, wird eine Hardware- oder Softwarelösung eingesetzt, die für die Synchronisation zuständig ist. Zunächst wird definiert, auf welchem Medium gearbeitet wird, welches also als „Primärmedium“ bezeichnet wird. Durch die Synchronisierung werden alle Änderungen zeitnah auf dem zweiten Speichermedium festgehalten. (Schmidt, 2006, S.167)

Abbildung 1 zeigt eine derartige asynchrone Datenspiegelung (Müller, 2003, S.115), bei welcher zwischen dem Schreibvorgang auf dem Primärmedium und der Synchronisation auf dem Sekundärmedium immer eine gewissen Zeitspanne besteht, in der die Datenbestände beider Medien nicht genau übereinstimmen (Schmidt, 2006, S.168).

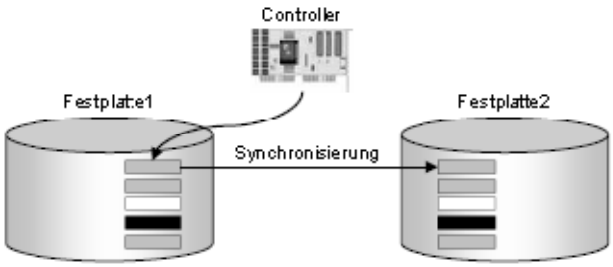

Abbildung 1: Asynchrone Datenspiegelung (Schmidt, 2006, S.168)

Um das Risiko eines Fehlers bei der asynchronen Datenspiegelung zu vermeiden, kann die Datenspiegelung in Echtzeit durchgeführt werden, so dass die Schreibvorgänge erst dann bestätigt werden, wenn die Daten auf beiden Speichermedien erfolgreich synchronisiert worden sind (Müller, 2003, S.115). Zur Unterstützung des parallelen Schreibens auf beiden Medien wird ein spezieller Controller benötigt, weshalb dieses Verfahren der Datensicherung kostenintensiver ist (Schmidt, 2006, S.168). Abbildung 2 zeigt eine synchrone Datenspiegelung in Echtzeit.

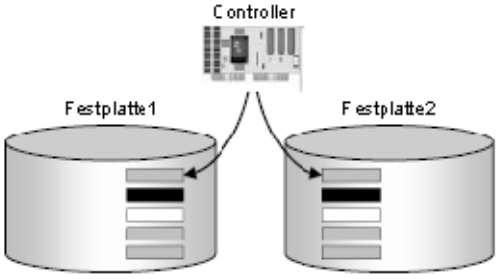

Abbildung 2: Synchrone Datenspiegelung mit parallelem Schreibzugriff (Schmidt, 2006, S.168)

Sowohl die zeitnahe (asynchrone) als auch die zeitgleiche (synchrone) Datenspiegelung bieten eine hohe Ausfalltoleranz, da auf Grund der Redundanz alle Daten auch bei einem Störvorfall weiterhin verfügbar sind (Schmidt, 2006, S.168). Allerdings können semantische Fehler auch mit diesen Verfahren nicht ausgeschlossen werden, da Schreibaktionen, die zu semantisch nicht mehr einwandfreien Daten führen, diese Aktionen auf dem zweiten Medium genau gleich durchgeführt werden, so dass die Daten dort ebenfalls nicht mehr korrekt sind. Wird auf den beiden Speichermedien mit unterschiedlichen Betriebssystemen wie bspw. Windows und UNIX oder unterschiedlichen Softwareanwendungen gearbeitet, kann die Spiegelung semantischer Fehler verhindert werden. (Schmidt, 2006, S.168)

2.2.4 RAID – Redundant Array of Inexpensive/Independent Disks

Ein weiterer, etwas komplexerer Ansatz zur nachhaltigen Sicherung von Daten durch Datenspiegelung auf Servern bzw. Festplatten existiert in Form von RAID-Systemen. Dieses Verfahren stützt sich auf die Idee, durch die logische Verbindung von mehreren kleinen und billigen physischen Festplatten eine grosse logische Festplatte zu simulieren (Schmidt, 2006, S.169). Forscher der Universität von Kalifornien in Berkeley entwickelten dieses Konzept der redundanten Datensicherung Ende der Achtzigerjahre des letzten Jahrhunderts (Müller, 2003, S.99). Auf Grund der bereits damals niedrigen Kosten für Festplatten wurde das System ursprünglich „Redundant Array of Inexpensive Disks“ genannt (Müller, 2003, S.99). Da die Kosten für Festplatten allerdings weiterhin gesunken sind und somit für RAID-Systeme nicht mehr gezwungenermassen billige und damit nicht sehr zuverlässige Festplatten eingesetzt werden mussten, wurde der Begriff später in „Redundant Array of Independent Disks“ (Schmidt, 2006, S.169) geändert. In der Literatur wird vereinzelt auch der Doppelbegriff „Redundant Array of Inexpensive/Independent Disks“ verwendet (z.B. Plötner/Wendzel, 2005, S.321).

Die Vorteile von RAID-Systemen liegen darin, dass durch die Verwendung mehrerer günstiger Festplatten nicht nur die Kosten gesenkt, sondern gleichzeitig auch die Datentransferrate und die Ausfalltoleranz erhöht werden können (Hoppe/Priess, 2003, S.183). Die

besonderen Charakteristiken von RAID-Systemen liegen in der Aufteilung des Datenbestandes und der Ausfalltoleranz:

Aufteilung des Datenbestandes

Für die Sicherung des Datenbestandes werden mehrere einzelne Platten verwendet, die gemeinsam als eine grosse Festplatte erscheinen. Der Datenbestand wird auf den einzelnen Festplatten verteilt, wobei jeweils keine kompletten Dateien auf die Festplatten geschrieben werden. Jede Datei wird auf mehrere Festplatten verteilt, so dass auf keiner Platte des RAID-Systems vollständige Dateien gesichert sind. (Schmidt, 2006, S.170)

Ausfalltoleranz

Auf Grund der Datenspiegelung werden alle Daten des gesamten Datenbestandes redundant gespeichert und können somit rekonstruiert und wiederhergestellt werden (Schmidt, 2006, S.170).

RAID-Systeme werden, basierend auf den jeweils angewandten Verfahren, in die RAID-Level 0-7 (Hansen/Neumann, 2001, S.753) eingeteilt, wobei der Begriff „Level“ missverständlich ist, da die RAID-Level nicht aufeinander aufbauen (Hoppe/Priess, 2003, S.183). Bei den am Häufigsten eingesetzten Levels handelt es sich um die RAID-Level 0, 1, 3, 4 und 5, welche nachfolgend kurz dargestellt werden. Weiter bestehen Mischformen, wie bspw. RAID-10 als Kombination aus RAID-1 und RAID-0 (Müller, 2003, S.99).

Auf eine Erläuterung des RAID-Levels 2 wird verzichtet, da dieses auf Grund des eingesetzten Verfahrens für die Datensicherung nicht mehr relevant ist (Müller, 2003, S.99).

Tabelle 2 zeigt in der Übersicht die Level RAID-0, RAID-1, RAID-3, RAID-4 und RAID-5 mit den jeweils angewandten Verfahren und den dadurch entstehenden Vor- und Nachteilen.

Tabelle 2: Übersicht über die RAID-Level 0, 1, 3, 4 und 5

RAID-Level	Verfahren	Vorteil	Nachteil
RAID-0	Beim RAID-0-Verfahren werden die zu sichernden Daten in Blöcke aufgeteilt und parallel auf zwei oder mehrere Platten verteilt (Hoppe/Priess, 2003, S.183), was als so genanntes „Data Striping“ bezeichnet wird (Müller, 2003, S.99). Die Ein-/Ausgabelast wird auf mehrere Kanäle und Laufwerke aufgeteilt, so dass die Leistung erhöht wird; allerdings entsteht keine Datenredundanz (Hansen/Neumann, 2001, S.753). Definitionsgemäss ist RAID-0 demnach keine RAID-Technik (Hoppe/Priess, 2003, S.183).	• Steigerung der Performance (Datendurchsatz) (Müller, 2003, S.99) • Geringe Kosten (Hansen/Neumann, 2001, S.753)	• Keine Datenredundanz! Bei einem Ausfall gehen alle Daten verloren. (Müller, 2003, S.99)
RAID-1	Bei RAID-1-Systemen, die auf dem Prinzip der Spiegelung (Mirroring) basieren, werden die Daten gleichzeitig auf verschiedene Laufwerke geschrieben (Hoppe/Priess, 2003, S.183). Auf Grund des Spiegelungs-Verfahrens besteht eine 100%ige Redundanz der Daten (Müller, 2003, S.99).	• 100%ige Datenredundanz	• Hohe Kosten (Hansen/Neumann, 2001, S.754)

RAID-Level	Verfahren	Vorteil	Nachteil
RAID-3	Für das RAID-3-System werden Datenblöcke byteweise aufgeteilt und parallel auf mehreren Laufwerken gespeichert. Auf ein einzelnes separates Laufwerk werden zusätzlich Paritätsinformationen geschrieben. (Hoppe/Priess, 2003, S.184) Bei einem Ausfall eines Laufwerks werden die fehlenden Daten an Hand der Paritätsinformationen und der Daten auf den verbleibenden Laufwerken rekonstruiert. Der Ausfall des Paritätslaufwerks beeinträchtigt den Datenzugriff nicht. (Hansen/Neumann, 2001, S.754)	• Hohe Performance (Datendurchsatz) (Hansen/Neumann, 2001, S.754)	• Jede Lese-/Schreibaktion erfordert den Zugriff auf alle Laufwerke. Da deshalb nur jeweils ein Lese-/ oder Schreibzugriff gleichzeitig möglich ist, eignet sich RAID-3 vorwiegend für Anwendungen mit wenigen grossen Dateien (z.B. Bildverarbeitung). (Hansen/Neumann, 2001, S.754)
RAID-4	Das Verfahren für RAID-4 entspricht analog demjenigen des RAID-3-Systems. Im Gegensatz zur byteweisen Aufteilung der Daten bei RAID-3 werden die Daten bei RAID-4 in Blöcken von 8, 16, 64 oder 128 Kilobyte auf verschiedenen Laufwerken gespeichert. Paritätsinformationen existieren auch bei RAID-4 und werden ebenfalls blockweise berechnet. (Hoppe/Priess, 2003, S.184)	• Schnelle Lesezugriffe bei grossen Datenblöcken auf Grund der Möglichkeit, alle Laufwerke parallel und gleichzeitig auszulesen (Singhuber, 2000)	• Die maximal mögliche Datenübertragungsgeschwindigkeit wird durch die Datenübertragungsgeschwindigkeit des Paritätslaufwerks begrenzt, da das Paritätslaufwerk bei allen Lese- und Schreibaktionen beteiligt ist (BC Industrieservice, 2007).

RAID-Level	Verfahren	Vorteil	Nachteil
RAID-5	RAID-5-Systeme verzichten auf ein separates Paritätslaufwerk. Daten und Paritätsinformationen (Prüfsummen), die für eine Rekonstruktion benötigt werden, werden quer über alle Laufwerke geschrieben (Hansen/Neumann, 2001, S.754). Somit besteht die Möglichkeit, mehrfach und gleichzeitig auf die verschiedenen Laufwerke zuzugreifen (Hansen/Neumann, 2001, S.754). RAID-5-Systeme eignen sich besonders für Anwendungen mit einer Vielzahl von Dateien und werden häufig bei grossen Datenbanken eingesetzt (Hoppe/Priess, 2003, S.184).	• Hoher Durchsatz in der Transaktionsverarbeitung auf Grund des mehrfachen gleichzeitigen Zugriffs auf die Laufwerke (Hoppe/Priess, 2003, S.184).	Die Schreib-Performance wird verlangsamt, da die Parität zunächst ermittelt, neu berechnet und dann wieder geschrieben werden muss (Microsoft TechNet, 2006).

Die Mindestanzahl der verwendeten Festplatten für die redundante Datensicherung mit dem RAID-System entspricht bei RAID-0 und RAID-1 jeweils zwei Festplatten, für Systeme der Level RAID-3, RAID-4 und RAID-5 werden im Minimum drei Festplatten benötigt (Nedrik, 2004).

Auf die Darstellung weiterer RAID-Level und RAID-Level-Kombinationen wird an dieser Stelle verzichtet, da diese für die vorliegende Ausarbeitung nicht relevant sind.

2.3 Exkurs: Firewall

Grundsätzlich können alle Massnahmen, die der Sicherung von Daten und Systemen sowie der Informationssicherheit an sich dienen, nach ihrer Wirkungsweise in präventive, detektive und reaktive Massnahmen unterschieden werden (vgl. Aebi, 2004, S.19; Weber/Willi, 2006, S.29). Die vorliegende Diplomarbeit fokussiert die bestehenden Regelungen zur Sicherung der Benutzer- und Bestandsdaten in Bibliotheksverbünden, wobei der Schwerpunkt klar auf den präventiven und weniger auf den reaktiven Vorkehrungen liegt. Ein wichtiger Bestandteil der Datensicherung mit präventiver Wirkung ist der Einsatz von Firewalls, weshalb dieser Aspekt nachfolgend in seiner Funktions- und Wirkungsweise etwas näher betrachtet wird.

2.3.1 Definition und Aufgaben

Durch die Anbindung von Rechnern oder Netzsegmenten an ein öffentliches Netz wie das Internet ergeben sich unterschiedliche Bedrohungen für die Sicherheit (Eckert, 2005, S.329). Eine Möglichkeit zum Schutz vor diesen Gefahren und zur Kontrolle der Zugriffe auf die internen Rechner und Netzsegmente bietet der Einsatz von Firewall-Systemen, kurz Firewalls genannt. Ursprünglich stammt der Begriff Firewall aus dem Feuerwehrjargon, wo Brandschutzmauern zwischen Gebäuden dazu dienten, eine Ausbreitung von Bränden von einem Gebäude auf das nächste zu verhindern (Eckert, 2005, S.329). Übertragen auf die Kommunikation von offenen Rechnernetzen bedeutet dies, dass Firewalls verschiedene Netze voneinander trennen, wobei gezielte und kontrollierte Übergänge zwischen den Netzen weiterhin zugelassen werden. Bestandteile eines Firewall-Systems sind eine oder mehrere soft- und/oder hardwarebasierte Netzwerkkomponenten, die gewährleisten, dass der Verkehr zwischen zwei Netzwerken mit unterschiedlichem Sicherheitsbedarf durch die Firewall geleitet wird (Aebi, 2004, S.70). Zugriffe auf die Netzwerke werden nur erlaubt, wenn sie den zuvor festgelegten und konfigurierten Anforderungen entsprechen (Aebi, 2004, S.70). Abbildung 4 zeigt in vereinfachter Weise das Funktionsprinzip einer Firewall.

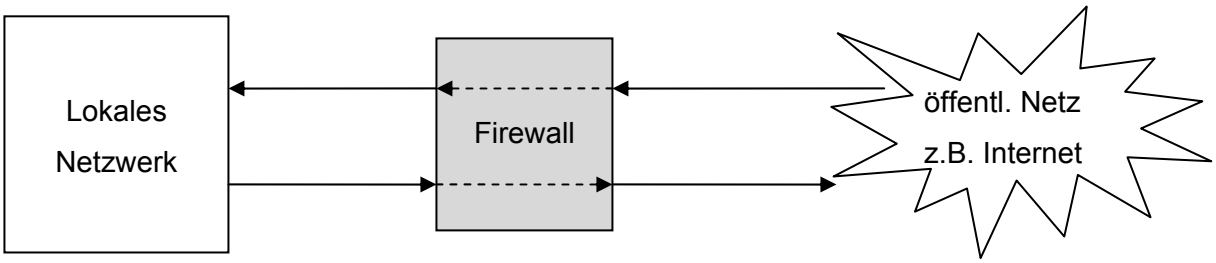

Abbildung 3: Funktionsprinzip einer Firewall (Vgl. Aebi, 2004, S.70; Eckert, 2005, S.330)

Neben dieser Funktion der Trennung zweier unterschiedlicher Netzwerke (lokal und öffentlich) kann eine Firewall auch eingesetzt werden, um unternehmensintern zwei Netzbereiche mit ungleichem Sicherheitsbedarf zu trennen (Hoppe/Priess, 2003, S.135).

Grundsätzlich nimmt eine Firewall folgende Aufgaben wahr (vgl. Aebi, 2004, S.71; Hoppe/Priess, 2003, S.134; Kruth, 2004, S.231f.):

- Kontrolle des Datenstroms, der zwischen Netzen, Netzsegmenten oder Teilnetzen stattfindet (Zugriffskontrolle)
- Unterbindung von nicht erlaubter Kommunikation
- Festlegung, welche Protokolle und Dienste zu welchen Zeiten für die Kommunikation eingesetzt werden (Rechteverwaltung)
- Protokollierung der Kommunikation zur Beweissammlung und –sicherung
- Alarmierung bei sicherheitsrelevanten Vorfällen
- Verbergen der internen Netzstruktur, damit aus dem unsicheren Netz nicht sichtbar ist, wie viele Rechnersysteme das zu schützende Netz umfasst.

Bezüglich des technischen Ablaufs der Kommunikation zwischen zwei Systemen liegt der Firewall das ISO/OSI-Referenzmodell zugrunde (Hoppe/Priess, 2003, S.135).

Das ISO/OSI-Referenzmodell bezeichnet ein abstraktes Schichtenmodell, welches die wichtigsten Eigenschaften und Funktionen von offenen Kommunikationssystemen auf einfache Art und Weise veranschaulicht (Hansen/Neumann, 2002, S.1146f.). Die vorliegende Diplomarbeit verzichtet auf eine ausführliche Erklärung des ISO/OSI-Referenzmodells[4], allerdings soll eine graphische Darstellung des Schichtenmodells das Verständnis der nachfolgenden Erläuterungen zur Wirkungsweise von Firewall-Systemen erleichtern.

[4] Für detaillierte Beschreibungen des ISO/OSI-Referenzmodells siehe bspw. Hansen/Neumann, 2002, S. 1146ff.; Hoppe/Priess, 2003, S.135ff.; Kruth, 2004, S.159f.

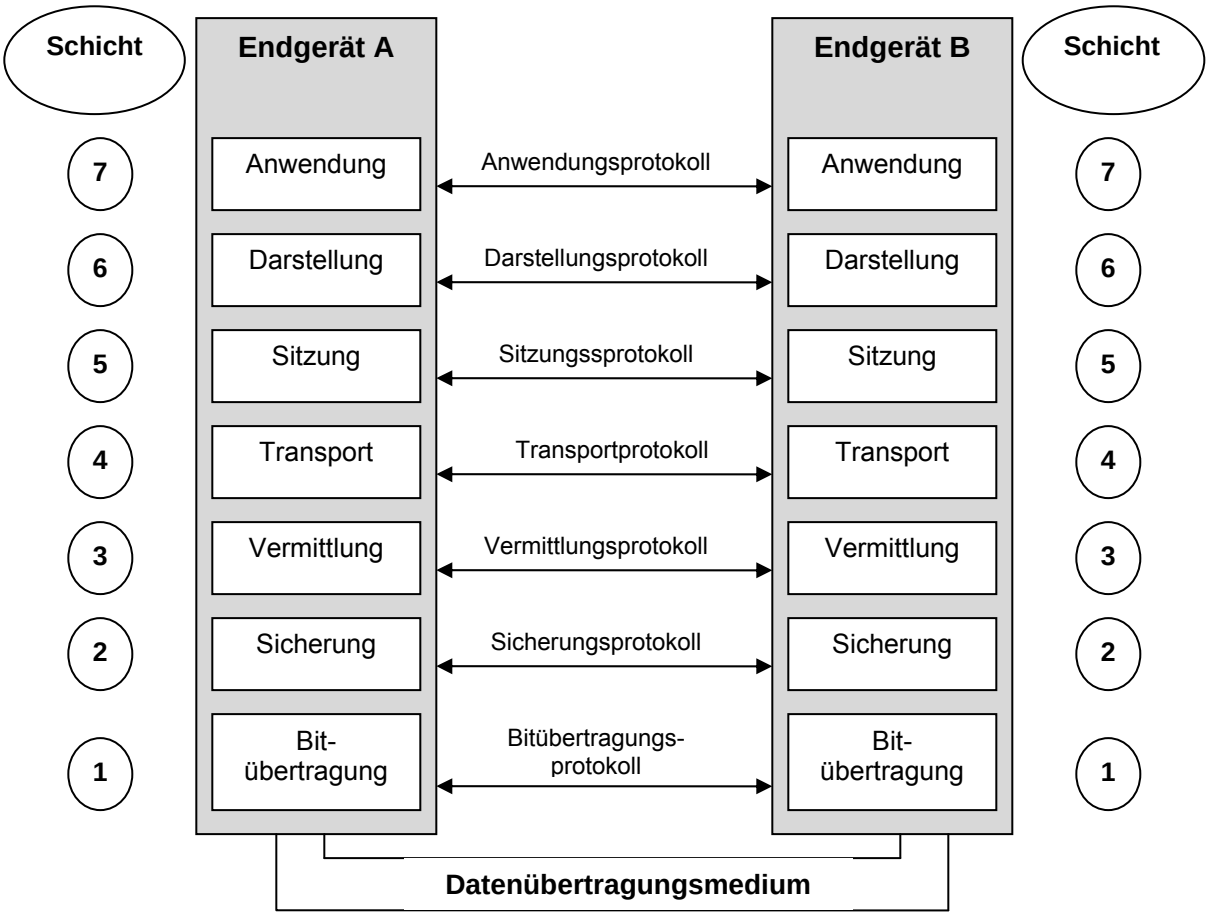

Abbildung 4: ISO/OSI-Referenzmodell (in Anlehnung an Hansen/Neumann, 2002, S.1147)

2.3.2 Komponenten einer Firewall

Für den Aufbau eines Firewall-Systems bestehen mehrere Architekturmöglichkeiten, die sich auf Grund des Einsatzes und der Kombination von Firewall-Komponenten unterscheiden. Zunächst werden deshalb die Komponenten einer Firewall, Paketfilter und Application Gateways bzw. Proxy-Server, kurz erklärt, bevor die Funktionsweise der einstufigen, zweistufigen und dreistufigen Architekturvarianten aufgezeigt wird.

Paketfilter

Paketfilter setzen zur Erfüllung ihrer Aufgaben auf den Schichten 3 und 4 des ISO/OSI-Referenzmodells, der Vermittlungs- (3) und der Transportschicht (4), auf (Eckert, 2005, S.332). Im Bereich der Vermittlungs- und Transportprotokolle übernehmen Paketfilter

- die Kontrolle aller Datenpakete, die die Firewall passieren wollen, und
- die Entscheidung, ob die Weiterleitung der Datenpakete zulässig ist (Hoppe/Priess, 2003, S.139).

Bei den betreffenden Protokollen der ISO/OSI-Schichten 3 und 4 handelt es sich meist um TCP/IP bzw. UDP/IP, da Paketfilter als Firewall-Komponente, wie Abbildung 3 zeigt, in der Regel zwischen einem lokalen Netz und einem öffentlichen Netz wie dem Internet eingesetzt werden (Eckert, 2005, S.332).

Für die Bewältigung der Aufgaben müssen entsprechende Filterregeln definiert werden, nach denen die Paketfilter entscheiden, welche Datenpakete weitergeleitet werden dürfen und welche nicht (Hoppe/Priess, 2003, S.139). Um eine möglichst hohe Sicherheit zu garantieren, sollten die Filterregeln so konstruiert werden, dass grundsätzlich *„alles verboten ist, was nicht explizit erlaubt ist“* (Hoppe/Priess, 2003, S.139). Paketfilter können Datenpakete also entweder durchlassen (allow), verwerfen (deny) oder zusammen mit einer Fehlermeldung zurückweisen (reject) (Hoppe/Priess, 2003, S.139). Neben diesen möglichen Reaktionen eines Paketfilters auf ein Datenpaket kann der Filter bei Ablehnung eines Pakets auch einen Eintrag in eine Logdatei schreiben oder bei spezifizierten Datenpaketen den Administrator durch einen gezielten Alarm informieren (Eckert, 2005, S.333).

Application Gateways / Proxy-Server

Im Gegensatz zu Paketfiltern, die keine Filterung der Datenpakete auf Anwendungsebene durchführen können, verwenden Application Gateways, auch als Proxy-Server bekannt, zur Kontrolle und Protokollierung der Kommunikation zwischen den Netzen Informationen von Schicht 7 des ISO/OSI-Referenzmodells (Hoppe/Priess, 2003, S.141). Als Firewall-Komponente stellen Application Gateways für jedes auf der Anwendungsebene zu protokollierende Programm einen spezifischen Filter zur Verfügung. Da diese speziellen, als Programme realisierten Filter auf einem Proxy-Server laufen, werden sie häufig als Proxies bezeichnet, wobei zwischen Application-Level-Proxies und generischen, so genannten Circuit-Level-Proxies zu unterscheiden ist: Application-Level-Proxies sind genau auf bestimmte Programme oder Protokolle zugeschnitten, während Circuit-Level-Proxies für Programme oder Protokolle definiert werden, für die kein spezieller Application-Level-Proxy existiert. (Hoppe/ Priess, 2003, S.141)

Zu den Aufgaben von Application Gateways gehören das Entgegennehmen, Prüfen und Protokollieren der Verbindungsanfragen von Anwendungen, sowie deren Weiterleitung bei erfolgreicher Prüfung (Hoppe/Priess, 2003, S.141). Circuit-Level-Proxies können die

Verbindungen nur protokollieren sowie einfache Prüfungen durchführen, während Application-Level-Proxies auf Grund ihrer spezifischen Konfiguration Verbindungsanfragen detaillierter prüfen können, bspw. durch eine Benutzerauthentifizierung. Weitere Möglichkeiten bestehen in der Analyse der Protokolle sowie dem Unterbinden bestimmter Anwendungsfunktionen, die von den entsprechenden Systemadministratoren als nicht zulässig eingestuft worden sind (Hoppe/Priess, 2003, S.141).

Da bei einem Einsatz eines Application Gateways mit nur einer Netzwerkkarte für die Kommunikation nach innen und nach aussen dieselbe Netzwerkkarte genutzt wird, kann der Proxy theoretisch umgangen werden (Hoppe/Priess, 2003, S.142). Um dies zu verhindern, können mehrere Netzwerkkarten eingesetzt werden, so dass die Netzbereiche innerhalb des Application Gateways „räumlich“ getrennt werden. Dieses Vorgehen bedingt beim späteren Einrichten neuer Anwendungen bzw. Dienste die Konfiguration eines entsprechenden Proxies (Hoppe/Priess, 2003, S.142), was zur Steigerung des Schutzes beiträgt. Durch eine Regelung, die festlegt, dass nur die Proxies auf die interne Netzwerkkarte, welche die einzige Verbindung zum externen Netz darstellt, zugreifen dürfen, kann der Schutz des internen Netzes zusätzlich erhöht werden (Hoppe/Priess, 2003, S.142).

Somit können Application Gateways differenziert werden in (Hoppe/Priess, 2003, S.142):

- **single-homed** Application Gateways mit einer Netzwerkkarte,
- **dual-homed** Application Gateways mit zwei Netzwerkkarten, sowie
- **multi-homed** Application Gateways mit mehr als zwei Netzwerkkarten

Tabelle 3 zeigt in einem Überblick die Vor- und Nachteile der beiden Firewall-Komponenten Paketfilter und Application Gateway auf (vgl. Hoppe/Priess, 2003, S.142f.):

Tabelle 3: Vor- und Nachteile von Paketfiltern und Application Gateways

	Vorteile	Nachteile
Paketfilter	• Hohe Flexibilität im Einsatz • Keine Geschwindigkeits-einbussen, keine erhöhten Rechenleistungen erforderlich	• Aufwändige Administration auf Grund der komplizierten Filter-regeln
Application Gateway	• Einfache Administration auf Grund modularer Struktur (Proxies) • Hoher Schutz des internen/ lokalen Netzes möglich (bei entsprechender Konfiguration der Proxies sowie dem Einsatz mehrerer Netzwerkkarten)	• Geringe Flexibilität im Einsatz: Jedes einzelne Programm erfor-dert eine entsprechende Proxy-Anwendung. • Ohne den Einsatz einer speziel-len Protokollierungs-Software werden Anfragen, für die kein Proxy existiert, ohne Protokollie-rung verworfen. • Geschwindigkeitseinbussen durch die Proxy-Prozesse auf der Anwendungsebene → Hohe Rechenleistungen sind erforderlich.

2.3.3 Architekturen

Firewall-Architekturen basieren meist auf Kombinationen von Paketfiltern und Application Gateways (Eckert, 2005, S.347). Möglich sind aber auch einstufige Firewall-Architekturen, bei denen nur Paketfilter oder Application Gateways zur Sicherung des internen Netzes eingesetzt werden. Im Folgenden sollen die verschiedenen Architekturvarianten kurz erläutert werden.

Einstufige Architekturen

Bei der einfachsten einstufigen Firewall-Architekturvariante wird zum Schutz des bezüglich des Sicherheitsbedarfs höher eingestuften Netzes ein Paketfilter zwischen diesem internen und dem externen Netz platziert (Hoppe/Priess, 2003, S.144). Die beiden Netze werden auf diese Weise allerdings nur physisch, nicht aber logisch voneinander getrennt:

Die ein- und ausgehenden Datenpakete werden anhand der Adress- und Portinformationen des Quell- und Zielrechners kontrolliert (Hoppe/Priess, 2003, S.145). Abbildung 5 zeigt ein Beispiel einer einstufigen Firewall-Architektur, bei der das zu schützende Netz (Intranet) durch den Einsatz eines Paketfilters gesichert wird.

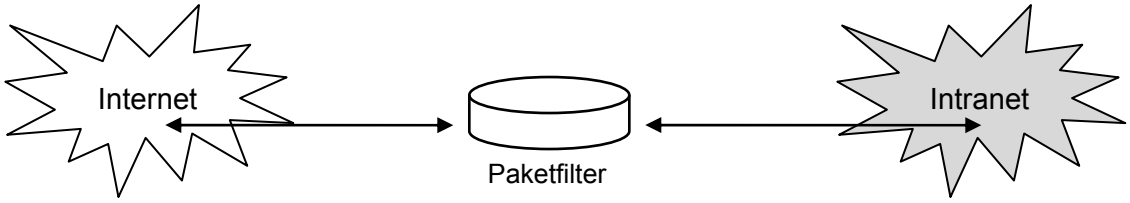

Abbildung 5: Einstufige Firewall-Architektur mit Paketfilter (Hoppe/Priess, 2003, S.145)

Diese Form der einstufigen Architektur kann entweder als Netzwerkrouter realisiert werden, der die entsprechenden Filterfunktionen bereitstellt, oder mit einem Rechner, auf dem eine Paketfilter-Anwendung läuft (Hoppe/Priess, 2003, S.145). Eine Firewall-Komponente, die auf einem Rechner umgesetzt wird, über den sämtliche eingehenden und ausgehenden Verbindungen zwischen einem internen und einem externen Netz geleitet werden (Eckert, 2005, S.340) bzw. der als erster oder einziger Rechner aus dem externen Netz erreicht werden kann (Hoppe/Priess, 2003, S.145), wird als „Bastion Host“ bezeichnet.

Zur Sicherung eines internen Netzes kann in einer einstufigen Firewall-Architektur statt eines Paketfilters auch ein Application Gateway zwischen die voneinander zu trennenden Netze geschaltet werden. Abbildung 6 zeigt die Funktionsweise einer Firewall mit einem singlehomed Application Gateway. Beim Einsatz eines Application Gateways mit nur einer Netzwerkkarte werden alle Kommunikationsverbindungen, für die Proxies konfiguriert wurden, über den Application Gateway geleitet (Hoppe/Priess, 2003, S.146). Anfragen, für die keine Proxies vorliegen, werden allerdings direkt an das interne Netz weitergeleitet (Hoppe/Priess, 2003, S.146), was dazu führt, dass das zu schützende Netz unter Umständen nicht ausreichend gesichert ist.

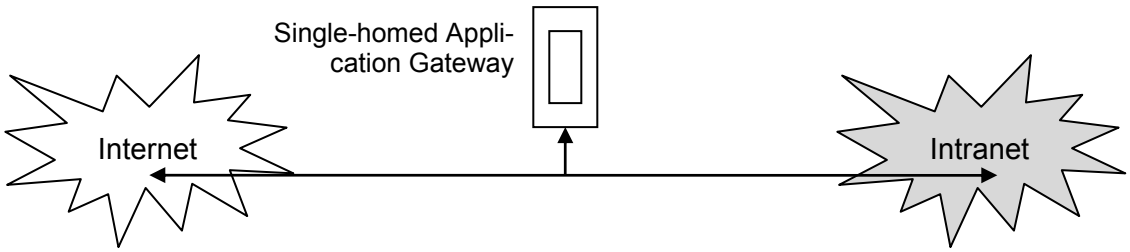

Abbildung 6: Einstufige Firewall-Architektur mit single-homed Application Gateway (Hoppe/Priess, 2003, S.145)

Um zu erzwingen, dass alle eingehenden und ausgehenden Verbindungen über das Application Gateway laufen müssen, kann alternativ ein dual-homed Application Gateway mit zwei Netzwerkkarten eingesetzt werden (Hoppe/Priess, 2003, S.146). Die wesentliche Eigenschaft eines dual-homed Application Gateways liegt darin, dass die beiden Netze vollständig voneinander isoliert werden, da kein IP-Routing und auch kein IP-Forwarding möglich ist, so dass die Datenpakete nicht direkt weitergeleitet werden können, sondern vorerst analysiert werden müssen (Eckert, 2005, S.347).

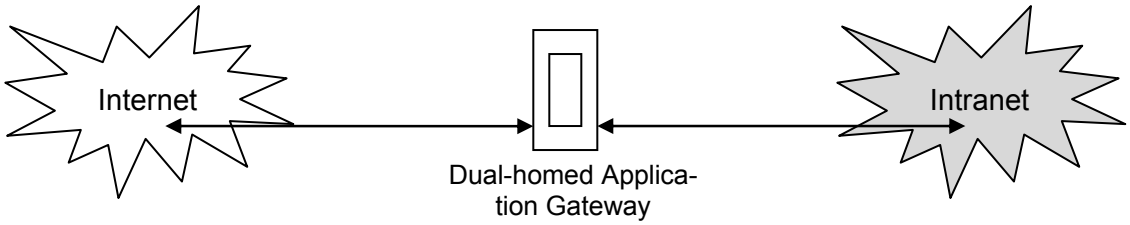

Abbildung 7: Einstufige Firewall-Architektur mit dual-homed Application Gateway (Hoppe/Priess, 2003, S.146)

Im Gegensatz zu Firewall-Architekturen, die Paketfilter verwenden und somit das interne und das externe Netz nur physisch voneinander trennen, können Firewall-Architekturen mit Application Gateways die Netze sowohl physisch als auch logisch gegeneinander absichern (Hoppe/Priess, 2003, S.146).

Zweistufige Architekturen

Um einen höheren Schutz des internen Netzes zu erreichen, kann das Firewall-System zweistufig aufgebaut werden, indem eine Kombination aus Paketfilter(n) und Application Gateway eingesetzt wird. Sinnvolle Kombinationen entstehen aus dem Einsatz eines single oder dual-homed Application Gateways, welchem ein Paketfilter vorgelagert wird (Hoppe/Priess, 2003, S.146). In diesem Fall dient der Paketfilter als erste Hürde bzw. Stufe, da die festgelegten Filterregeln eine erste Kontrolle der Datenpakete anhand der

mitgelieferten Adressen und Dienste durchführen. Anfragen, die auf Grund der Filterregeln nicht zulässig sind, werden demnach nicht angenommen. Hingegen werden Datenpakete, die erlaubt sind, vom Paketfilter an die zweite Sicherheitsstufe, den Application Gateway weitergeleitet, welches die Anfrage auf der Anwendungsebene prüft und/oder protokolliert (Hoppe/Priess, 2003, S.147). Allerdings werden auch bei einer zweistufigen Architekturvariante mit einem single-homed Application Gateway Verbindungen für Dienste, für die kein Proxy eingerichtet ist, am Application Gateway vorbei direkt in das interne Netz geleitet, wie Abbildung 8 zeigt (Hoppe/Priess, 2003, S.146).

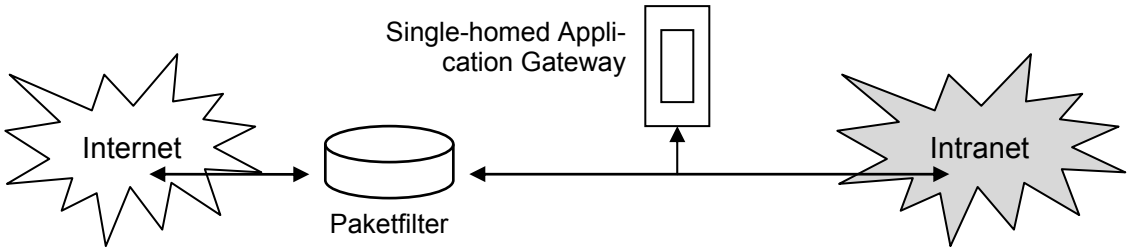

Abbildung 8: Zweistufige Firewall-Architektur mit single-homed Application Gateway

Wird hingegen statt eines single-homed ein dual-homed Application Gateway mit zwei Netzwerkkarten verwendet, werden die beiden Netze vollständig physisch getrennt, so dass direkte Verbindungen vom Paketfilter in das interne Netz nicht möglich sind. Der Netzbereich, der durch den Einsatz eines dual-homed Application Gateway zwischen diesem und dem vorgelagerten Paketfilter entsteht und zwei Netze mit unterschiedlich eingestuftem Sicherheitsbedarf voneinander trennt, wird demilitarisierte Zone (DMZ) oder auch Screened Subnet genannt. (Hoppe/Priess, 2003, S.147) Abbildung 9 zeigt eine vereinfachte Darstellung einer zweistufigen Architektur mit dual-homed Application Gateway und DMZ.

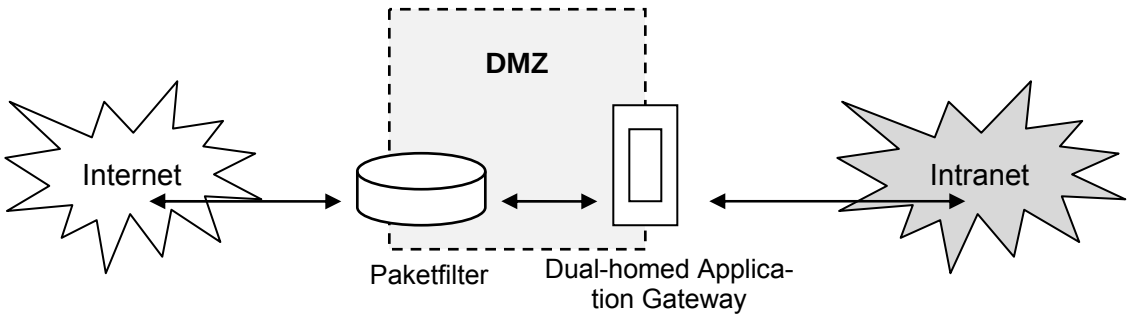

Abbildung 9: Zweistufige Firewall-Architektur mit dual-homed Application Gateway und DMZ (Hoppe/Priess, 2003, S.147)

Beim Aufbau eines Firewall-Systems sollte darauf geachtet werden, dass die verwendeten Firewall-Komponenten sinnvoll kombiniert und angeordnet werden. So macht es wenig Sinn, ein Application Gateway einem Paketfilter vorzulagern, da das Application Gateway über ein höheres Gefährdungspotenzial verfügt und durch die umgekehrte Anordnung einer wesentlich grösseren Gefahr ausgesetzt ist (Hoppe/Priess, 2003, S.147). Die Eroberung eines Application Gateways kann durchaus dazu führen, dass der Paketfilter seine Aufgabe nicht mehr sinngemäss ausführt, da die Filterregeln festlegen, dass Datenpakete vom Application Gateway an das interne Netzt geleitet werden (Hoppe/Priess, 2003, S.147). Der Schutz des internen Netzes ist in diesem Fall hochgradig gefährdet.

Dreistufige Architekturen

Sicherheitsarchitektonisch betrachtet gehen dreistufige Firewall-Architekturen noch einen Schritt weiter als die ein- und zweistufigen Architekturvarianten. Dreistufige Firewalls verfügen über ein Application Gateway, welches von allen Seiten durch Paketfilter geschützt wird. Werden hierbei zwei Paketfilter eingesetzt, so werden diese je nachdem, ob sie sich beim internen oder beim externen Netz befinden, als interner bzw. externer Paketfilter bezeichnet. (Hoppe/Priess, 2003, S.148)

Der Einsatz eines Application Gateways mit nur einer Netzwerkkarte (single-homed) und die Anordnung der Paketfilter führt dazu, dass eine einzige DMZ entsteht, da alle Datenpakete, die von den Paketfiltern auf Grund der Filterregeln durchgelassen werden, für die aber kein Proxy auf dem Application Gateway abgelegt ist, an diesem vorbei geleitet werden (Hoppe/Priess, 2003, S.148).

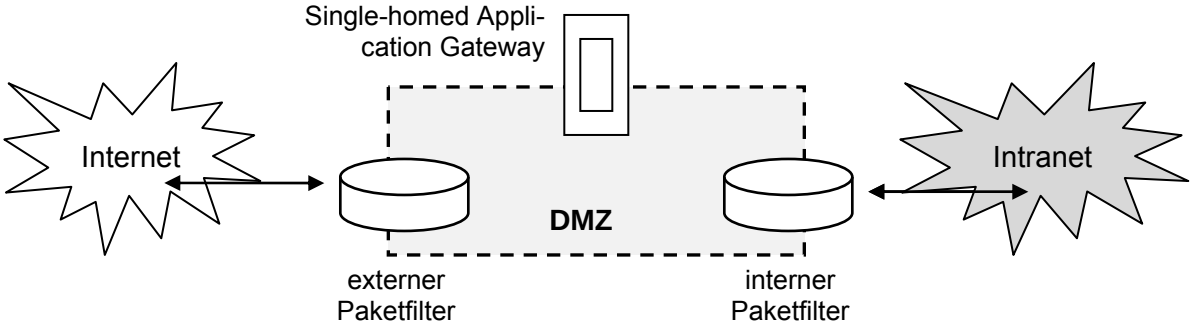

Abbildung 10: Dreistufige Firewall-Architektur mit single-homed Application Gateway und DMZ (Hoppe/Priess, 2003, S.148)

Im Gegensatz dazu entstehen zwei demilitarisierte Zonen, wenn die dreistufige Firewall-Architektur über ein dual-homed Application Gateway mit zwei Netzwerkkarten

verfügt (Hoppe/Priess, 2003, S.149). Der Schutz des internen Netzes ist bei dieser Architekturvariante besonders hoch, da erzwungen wird, dass sämtlich Anfragen über den Application Gateway laufen müssen und keine direkte Verbindung zwischen den Paketfiltern möglich ist.

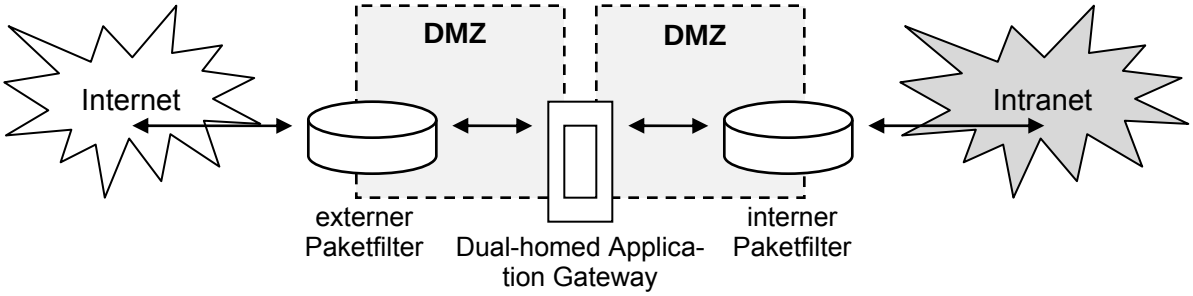

Abbildung 11: Dreistufige Firewall-Architektur mit dual-homed Application Gateway und DMZ (Hoppe/Priess, 2003, S.149)

Diese Darstellung möglicher Architekturvarianten für den Aufbau eines Firewall-Systems beschliessen den kleinen Exkurs zum Aspekt der Firewall als präventive technische Sicherheitsmassnahme zur Datensicherung. Auf detailliertere Ausführungen wird verzichtet, da weitere Erläuterungen zu Firewalls für die vorliegende Ausarbeitung nicht relevant sind.

3 Sicherheitskonzept

Nachdem nun die Grundlagen, Verfahren, Massnahmen und Strategien der Datensicherung dargestellt sind, folgt deren Umsetzung. Auch wenn höchst strukturierte Datensicherungsstrategien existieren, bedeutet dies nicht zwingend, dass die betreffenden Daten entsprechend ihrer Aufgabe genug gesichert sind. Eine zweckgemässe Sicherung von Daten erfordert eine Auseinandersetzung mit den Daten selbst, auf Grund derer die Datensicherung organisiert und schriftlich festgehalten werden kann. Dies erfolgt meist in Form eines Sicherheitskonzepts oder einer so genannten Security Policy. Nach Hoppe und Priess bezeichnet Sicherheit im Kontext von Informationen, Informationssystemen, Informationsverarbeitung und Daten

> *„den Zustand des Sicherseins vor Gefahr oder Schaden bzw. einen Zustand, in dem Schutz vor Gefährdungen besteht.“* (Hoppe/Priess, 2003, S.23)

Weiter wird die Sicherheit zu einem bestimmten Zeitpunkt als „Ist-Sicherheit“ verstanden, welche klar von einem geplanten Ausmass an Sicherheit als der so genannten „Soll-Sicherheit“ unterschieden werden muss (Hoppe/Priess, 2003, S.23).

Die folgenden Ausführungen zeigen auf, in welchem Rahmen Sicherheitskonzepte entstehen, in welche Unternehmensbereiche diese eingebunden werden müssen und über welche Inhalte sie verfügen. Damit wird der Grundstein für eine ausführliche Betrachtung der Sicherheitskonzepte der analysierten Institutionen gelegt.

3.1 Sicherheitskriterien

Einen Zustand absoluter Gefahren- bzw. Risikofreiheit gibt es nicht, woraus folgt, dass Sicherheit nur bezogen auf eine Situation, einen gewissen Zeitraum und bestimmte Rahmenbedingungen betrachtet werden kann (Schmidt, 2006, S.14f.). Auf Grund dieser Tatsache muss im Informationssicherheits-Management und besonders im Teilbereich der Datensicherung evaluiert und definiert werden, welche Form der Sicherheit für die unterschiedlichen Unternehmensbereiche und Datenbestände benötigt wird (Schmidt, 2006, S.15). Zur Unterstützung in der Beantwortung dieser Frage dienen Sicherheitskriterien, die Bestandteil diverser Kriterienmodelle sind (Schmidt, 2006, S.15).

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) betrachtet die Aspekte

- Vertraulichkeit
- Verfügbarkeit
- Integrität

als Grundwerte der IT-Sicherheit (BSI, 2005a). Zu den weiteren, je nach Institution wichtigen Sicherheitskriterien gehören (BSI, 2005a):

- Authentizität
- Zuverlässigkeit
- Verbindlichkeit
- Nichtabstreitbarkeit

Die Wahl der zu beachtenden Sicherheitskriterien obliegt der jeweiligen Institution, so dass die Kriterien selten standardisiert sind. Einen ähnlichen Ansatz wie das BSI verfolgt Schmidt, der neben den drei wichtigsten Grundwerten der IT-Sicherheit die folgenden Sicherheitskriterien nennt (Schmidt, 2006, S.17f):

- Authentizität
- Konformität
- Nachvollziehbarkeit
- Verbindlichkeit

Im Kontext der Informationstechnik wird Sicherheit verstanden als (ITSEC, 1991, S.1):

- Verfügbarkeit: Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln
- Vertraulichkeit: Schutz vor unbefugter Preisgabe von Informationen
- Integrität: Schutz vor unbefugter Veränderung von Informationen

Zum besseren Verständnis sollen diese drei wichtigen Sicherheitskriterien etwas genauer erläutert werden.

3.1.1 Verfügbarkeit

Prozesse in Institutionen sind meist nur funktions- und ablauffähig durch die Unterstützung von IT-Diensten, die von der Informationstechnik zur Verfügung gestellt werden (Schmidt, 2006, S.15). Demnach verlangt die Sicherheit dieser Prozesse, dass die benötigten IT-Dienste zu jeder Zeit nutzbar sind (Schmidt, 2006, S.15). Die Verfügbarkeit eines Informationssystems (IS) ist nach Hoppe und Priess dann gewährleistet, wenn

> *„keine Beeinträchtigungen der Funktionalität eines IS vorliegen und das System einschliesslich der Daten autorisierten Nutzern uneingeschränkt zur Verfügung steht.“*
> (Hoppe/Priess, 2003, S.24)

Gemessen und angegeben wird die Verfügbarkeit in Prozentwerten, womit dargestellt wird, wie häufig das System funktioniert bzw. ausfällt (Schmidt, 2006, S.15). 0% Verfügbarkeit bedeuten somit, dass das System nie funktioniert; bei einer 50%igen Verfügbarkeit läuft das System zur Hälfte ohne Probleme und fällt zur Hälfte aus, und ein 100%ig verfügbares System

würde nie ausfallen und wäre zu jedem Zeitpunkt nutzbar (Schmidt, 2006, S.15). In der Informationssicherheit werden zwar oft hohe Verfügbarkeits-Werte für Informationssysteme vorgegeben, die meist sogar mehr als 99% betragen, dennoch ergeben diese Prozentzahlen ausgerechnet als Ausfallzeiten pro Jahr durchaus akzeptable und tolerante bzw. sogar relativ hohe Werte für die Ausfallzeit des Systems (Schmidt, 2006, S.15). Dies veranschaulicht die folgende, von Schmidt übernommene Tabelle:

Tabelle 4: Verfügbarkeit von Informationssystemen (Schmidt, 2006, S.16)

Verfügbarkeit	Ausfall pro Jahr
90%	36,5 Tage
95%	8,25 Tage
99%	3,65 Tage
99,9%	8,76 Stunden
99,99%	52,56 Minuten
99,999%	5,26 Minuten

Grundlage für die in der Tabelle dargestellten Werte bildet ein kontinuierlich arbeitender, sich im so genannten „24x7-Dauerbetrieb“ befindlicher IT-Dienst, der entsprechend 24 Stunden pro Tag und sieben Tage die Woche in Betrieb ist. Die Werte wurden gerundet. (Schmidt, 2006, S.16)

3.1.2 Vertraulichkeit

Das Sicherheitskriterium der Verfügbarkeit spricht in seiner Definition bereits einen weiteren wichtigen Aspekt an, indem darauf hingewiesen wird, dass das System und die Daten ausschliesslich *autorisierten* Nutzern zugänglich sein dürfen (Hoppe/Priess, 2003, S.24). Die Vertraulichkeit ist somit ein Zeichen dafür, dass sichergestellt wird, dass *„eine vertrauliche Information nur denjenigen Personen zugänglich gemacht wird, für die sie vorgesehen ist“* (Schmidt, 2006, S.16).

Um die Sicherheit des Datenbestandes des Unternehmens oder der Institution zu gewährleisten, können die Daten zur Wahrung der Vertraulichkeit in so genannte Sicherheitsstufen, auch als Vertraulichkeitsstufen (Schmidt, 2006, S.17) bezeichnet, eingeteilt werden (Hoppe/Priess, 2003, S.24). Mögliche Einstufungen hierfür sind „gering – mittel – hoch – sehr

hoch“ oder „öffentlich – intern – vertraulich – streng vertraulich“ (Schmidt, 2006, S.17) oder „nicht vertraulich – vertraulich – geheim – streng geheim“ (Hoppe/Priess, 2003, S.24).

3.1.3 Integrität

Neben der Vertraulichkeit und Verfügbarkeit von Daten und Informationssystemen ist natürlich auch deren Integrität von äusserst hoher Bedeutung, da eine unbemerkte und unbefugte Manipulation der Daten, wie bspw. Änderungen oder gar Löschvorgänge, grossen Schaden anrichten können. In einem Informationssystem ist die Integrität der Daten gewährleistet, wenn *„Daten korrekt, aktuell, vollständig und widerspruchsfrei bzw. konsistent sind.“* (Hoppe/Priess, 2003, S.24)

Die Integrität sollte zu jedem Zeitpunkt geprüft und nachvollzogen werden können, so dass beabsichtigte oder unabsichtliche Änderungen an Daten oder Informationssystemen, die zu falschen oder unvollständigen Informationen bzw. im Bereich der Informationssysteme zu nur vorgetäuschten Operationen und Abläufen führen, verhindert werden können (Hoppe/Priess, 2003, S.24). Daten und technische Systeme werden als *integer* bezeichnet, wenn deren Integrität sichergestellt ist (Hoppe/Priess, 2003, S.24).

Als besonders wichtig erweist sich der Aspekt der referenziellen Integrität von Daten, welcher fordert, dass voneinander abhängige Datensätze nur vollständig, d.h. gemeinsam, gelöscht werden dürfen (Hoppe/Priess, 2003, S.24), so dass die Datenintegrität weiterhin gewährleistet ist.

3.2 Sicherheits-Management

Die Erarbeitung, Durchsetzung und Kontrolle eines Sicherheitskonzepts fällt in den Aufgabenbereich des Sicherheitsmanagements, welches als spezifisches Teilgebiet des Informationsmanagements (Hoppe/Priess, 2003, S.269) fungiert. Zu den Kernfunktionen des Sicherheitsmanagements zählen die Untersuchung des benötigten Schutzes, bspw. durch eine Risikoanalyse, sowie die anschliessende Definition der geeigneten Sicherheitsmassnahmen (Hoppe/Priess, 2003, S.69) in Form eines Sicherheitskonzeptes oder einer Security Policy. Nach Heinrich besteht das übergeordnete Ziel des Sicherheitsmanagements darin,

> *„einen kontinuierlichen und störungsfreien Betrieb der Informationsinfrastruktur sowie die Sicherheit der gespeicherten und verarbeiteten Daten zu gewährleisten.“*
>
> (Heinrich, 2002, S.279)

Auf diese Weise kann die Wahrscheinlichkeit, dass bestimmte Gefahren eintreten, von vornherein reduziert werden. Tritt dennoch ein Gefahrenvorfall ein, so dient das

Sicherheitsmanagement dazu, den Störfall aufzudecken und den dadurch verursachten Schaden möglichst gering zu halten. (Hoppe/Priess, 2003, S.270)

Der Komplexität des Informationssystems entsprechend müssen Massnahmen für die Gewährleistung sämtlicher Sicherheitsaspekte festgelegt werden, da Einzellösungen für die Sicherheit von Teilbereichen der Informationssysteminfrastruktur nicht ausreichen (Hoppe/Priess, 2003, S.270). Somit erscheint es sinnvoll, aus dem übergeordneten Ziel des Sicherheitsmanagements differenzierte Teilziele abzuleiten (Hoppe/Priess, 2003, S.270):

- Mögliche Gefährdungen, wie Risiken und Schwachstellen, werden identifiziert und analysiert.
- Der Eintritt von Gefahren wird möglichst verhindert bzw. die Wahrscheinlichkeit eines Eintritts minimiert.
- Eingetretene Gefahren werden entdeckt und ausgeschaltet.
- Die Folgen eingetretener Gefahren werden minimiert und beseitigt.

Sowohl das übergeordnete Ziel als auch die Teilziele des Sicherheitsmanagements können in strategische und operative Ziele unterschieden werden (Hoppe/Priess, 2003, S.271). Für die Definition von strategischen Sicherheitszielen und deren schriftliche Dokumentation in der Sicherheitspolitik des Unternehmens zeigt sich die Unternehmensleitung verantwortlich. Die in der Sicherheitspolitik verankerten Sicherheitsziele werden auf operativer Ebene in einem Sicherheitskonzept mittels der Festlegung konkreter Massnahmen zur Gewährleistung der Informationssicherheit präzisiert. (Hoppe/Priess, 2003, S.271)

Damit die von der Institution angestrebte Informationssicherheit und die Sicherheit der Daten nach den Sicherheitskriterien der Verfügbarkeit, Vertraulichkeit und Integrität erreicht und umgesetzt werden können, besteht eine weitere wichtige Aufgabe des Sicherheitsmanagements darin, so genannte Sicherheitsrichtlinien zu formulieren (Mühlenbrock, 2003, S.27) und dem Personal mitzuteilen bzw. schriftlich auszuhändigen (Hoppe/Priess, 2003, S.203). Sicherheitsrichtlinien sind von der Unternehmensleitung erarbeitete verbindliche Anleitungen (Mühlenbrock, 2003, S.27), die *„konkrete, nachvollziehbare und vor allem umsetzbare Verfahrensanweisungen enthalten“* (Hoppe/Priess, 2003, S.203). Als Präventivmassnahme dient die Vermittlung von unternehmensinternen Sicherheitsrichtlinien der Sensibilisierung des Personals in Bezug auf die Informations- und die Datensicherheit.

3.3 Der Sicherheitsprozess

Bevor der Aufbau und die nötigen und möglichen inhaltlichen Aspekte eines Sicherheitskonzepts vertieft behandelt werden, sollen die bisherigen Erkenntnisse aus den Bereichen des Sicherheitsmanagements und der Datensicherheit zusammenfassend dargestellt werden. Da Sicherheit und auch die Aufgaben des Sicherheitsmanagements nicht als einmalige Aktion verstanden werden dürfen, sondern als *„flexibler, dynamischer und kontinuierlicher Prozess“* (Hoppe/Priess, 2003, S.275) betrachtet werden müssen (Aebi, 2004, S.23), eignet sich der Sicherheitsprozess für die Darstellung besonders gut.

Der prozesshafte Charakter des Sicherheits-Managements wird bedingt durch sich stetig ändernde Anforderungen an die Informations- und Datensicherheit auf Grund ebenso kontinuierlicher Entwicklungen der Informationstechnologien (Hoppe/Priess, 2003, S.275). Wachsende und sich verändernde Ansprüche an die zu gewährleistende Sicherheit erfordern regelmässige Überprüfungen, Aktualisierungen und Ergänzungen der Sicherheitskonzepte, Sicherheitsmassnahmen und Sicherheitsrichtlinien im Unternehmen (Hoppe/Priess, 2003, S.275). Somit dient der iterative Sicherheitsprozess der sinnvollen Umsetzung und der Erfolgskontrolle der im Sicherheitskonzept festgelegten Sicherheitsmassnahmen.

Die fachspezifische Literatur behandelt verschiedene Ansätze zur Darstellung des Sicherheitsprozesses, die oft nur in wenigen Teilaspekten differieren. Zu den grundlegenden Phasen des Sicherheitsprozesses zählen (vgl. Aebi, 2004, S.23; Hoppe/Priess, 2003, S.276):

- Erstellung einer Sicherheitspolitik
- Analyse und Bewertung von Risiken
- Erstellung und Anpassung eines Sicherheitskonzepts
- Planung und Umsetzung von Sicherheitsmassnahmen
- Überwachung, Überprüfung und Reaktion bzw. kontinuierliche Verbesserung

Aebi macht darauf aufmerksam, dass eine weitere, durchaus wichtige Phase im Sicherheitsprozess oft unterschätzt und ausser Acht gelassen wird. Deshalb stellt er den genannten Phasen die Phase der Bewusstseinsbildung voran, die impliziert, dass entsprechendes Verhalten zur Wahrung der Sicherheit nur gewährleistet ist, wenn sich das Personal aller Unternehmensebenen sowohl der möglichen Gefahren und Risiken als auch der Abwehrmöglichkeiten bewusst ist (Aebi, 2004, S.23f.).

Der Sicherheitsprozess dient ebenso wie das Sicherheitskonzept und das Sicherheitsmanagement der Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität des Informationssystems sowie der gespeicherten und verarbeiteten Daten (Eggel, 2000, S.1072). Abbildung 12 veranschaulicht das Zusammenwirken der einzelnen Phasen des Sicherheitsprozesses und zeigt dessen kontinuierlichen Ablauf.

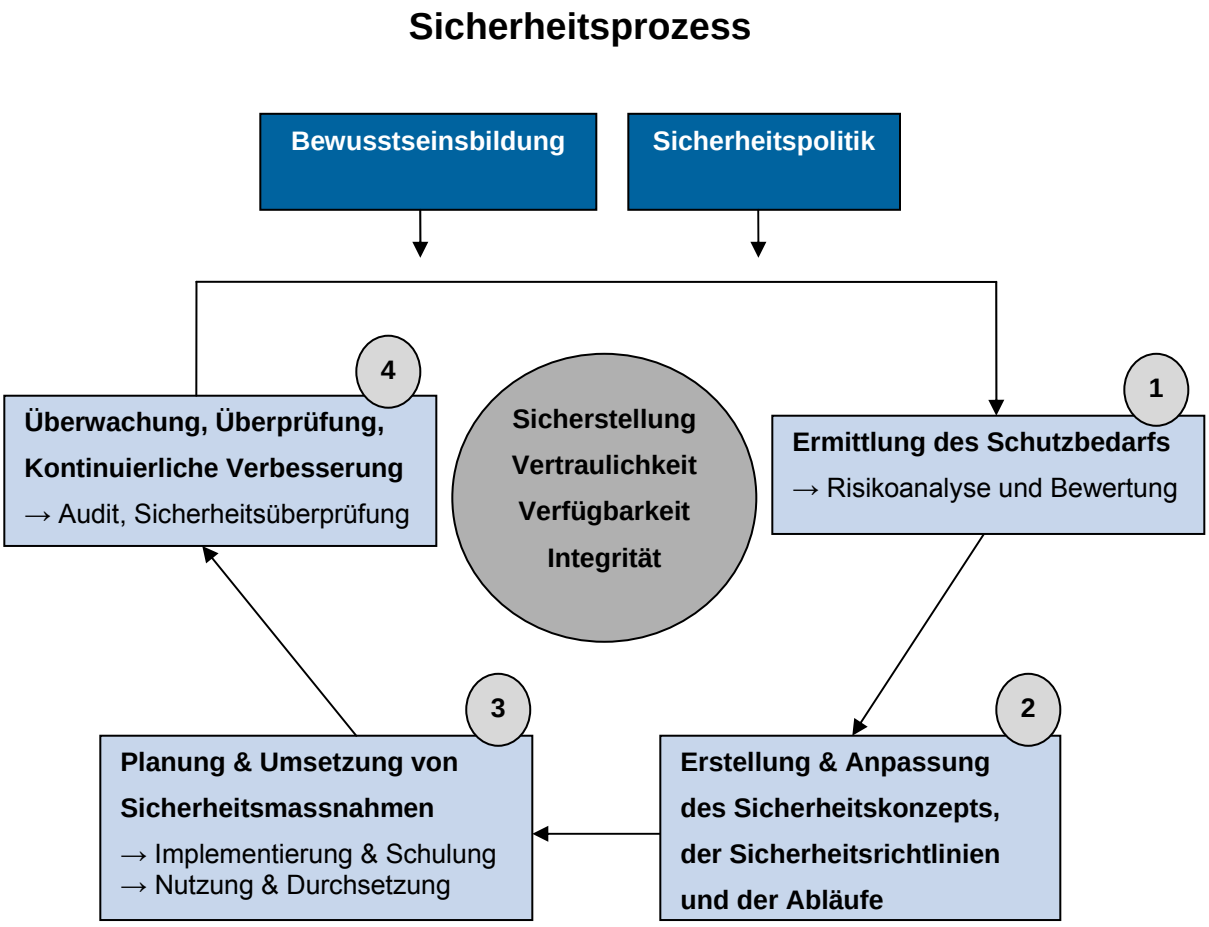

Abbildung 12: Sicherheitsprozess (in Anlehnung an Aebi, 2004, S.24 und Eggel, 2000, S.1072)

Basis und Voraussetzung für einen funktionierenden Sicherheitsprozess bilden die Phasen der Bewusstseinsbildung und der Erarbeitung einer Sicherheitspolitik, die auf den zuvor von der Unternehmensleitung aufgesetzten Sicherheitszielen basiert. Inhaltlich legt die Sicherheitspolitik Unternehmensstrukturen, Richtlinien, Regeln und Vorgaben fest, die zur Erreichung der definierten Sicherheitsziele benötigt werden (Hoppe/Priess, 2003, S.275). Ein weiterer wichtiger Faktor, der zur Gewährleistung der Sicherheit von Daten und Informationssystemen beiträgt, ist die schriftliche Dokumentation von Verantwortlichkeiten und

Kompetenzen in der Sicherheitspolitik (Hoppe/Priess, 2003, S.275) und in allen weiteren sicherheitsspezifischen Unterlagen.

Der nun folgende Abschnitt beschäftigt sich vertieft mit der Erarbeitung eines Sicherheitskonzepts und zeigt auf, welche Überlegungen zu Aufbau und Inhalt in die Entwicklung einfliessen sollten.

3.4 Aufbau eines Sicherheitskonzepts

Sowohl der Inhalt als auch der Aufbau von Sicherheitskonzepten ist nicht standardisiert (Schmidt, 2006, S.93), da beide Aspekte an die spezifischen Gegebenheiten der Institution angepasst werden müssen, damit die Sicherheit der eingesetzten Informationssysteme sowie der verarbeiteten und gespeicherten Daten garantiert werden kann. Die Fachliteratur zur Thematik der Netzwerksicherheit und der so genannten IT-Sicherheit behandelt unterschiedliche Ansätze zur Erstellung von Sicherheitskonzepten bzw. Security Policies. Die Spanne reicht dabei von einfachen Massnahmenkatalogen (vgl. Aebi, 2004, S.19) bis hin zu komplexen Sicherheitskonzepten, die nicht nur formelle Aspekte sondern auch spezifische Inhalte zur Datensicherung umfassen (vgl. Junk, 2003, S.14; Hoppe/Priess, 2003, S.221ff.). Nachfolgend werden die in der Literatur dargestellten Komponenten von Sicherheitskonzepten sinnvoll miteinander kombiniert, um einen möglichst ausführlichen und breiten Überblick über die Möglichkeiten zum Aufbau von Sicherheitskonzepten zu erhalten.

3.4.1 Allgemeines

Zwei Punkte sind von zentraler Bedeutung, wenn es darum geht, eine Security Policy aufzusetzen: Die Gesamtverantwortung für die Informationssicherheit obliegt der Unternehmensleitung, auch wenn diese auf Grund des fehlenden Fachwissens die entsprechenden Experten mit der Erarbeitung des Sicherheitskonzepts beauftragen muss (Schmidt, 2006, S.92). Ebenso wichtig wie die klare Verantwortlichkeit der Unternehmensleitung ist das Bewusstsein des Personals (Junk, 2003, S.14) für die Informations- und Datensicherheit im Unternehmen, wie dies bereits der Sicherheitsprozess aufgezeigt hat. Die Gewährleistung der Sicherheit steht und fällt mit der Umsetzung der vorgeschriebenen Massnahmen und Richtlinien durch die betroffenen und beteiligten Mitarbeitenden, weshalb die Regeln so formuliert werden müssen, dass sich das Personal nicht nur mit den Regelungen identifizieren kann, sondern diese auch einhält (Junk, 2003, S.14).

Zu den grundlegenden Komponenten eines Sicherheitskonzeptes gehören (vgl. Junk, 2003, S.14; Schmidt, 2006, S.93f):

- Abgrenzung des Gültigkeitsbereiches des Sicherheitskonzepts
- Definition der Verantwortlichkeiten und Kompetenzen im Kontext des Sicherheits-Managements
- Begriffe und Definitionen
- Dokumentation der Bedeutung der Informations- und Datensicherheit für das Unternehmen
- Nennung der sicherheitskritischen Prozesse, der schutzbedürftigen Werte und der grundsätzlichen Sicherheitsziele
- Integriertes Datensicherungskonzept mit den Richtlinien, Regeln und Massnahmen zur Umsetzung und Gewährleistung der Informationssystem- und Datensicherheit
- Definition der Verantwortlichkeiten und Konsequenzen bei Nichteinhalten des Sicherheitskonzepts
- Regelungen und Massnahmen zur Kontrolle und Überprüfung des Sicherheitskonzepts

Diese einzelnen Teilaspekte sollten grundsätzlich Bestandteil eines jeden Sicherheitskonzepts sein, wobei die Gewichtung und die Ausführlichkeit je nach Branche der Institution, nach Vorschriften von Aufsichtsbehörden oder von Gesetzes wegen oder auf Grund weiterer Rahmenbedingungen variieren kann (Schmidt, 2006, S.93). Zum besseren Verständnis werden die genannten Komponenten eines Sicherheitskonzepts bzw. einer Security Policy genauer betrachtet und erläutert. Da das Regelwerk zur Datensicherung einen besonderen Stellenwert in der vorliegenden Diplomarbeit einnimmt, wird es gesondert behandelt und in einem weiteren Unterkapitel ausführlich dargestellt.

Abgrenzung des Gültigkeitsbereiches des Sicherheitskonzepts

Mit der Definition des Gültigkeitsbereiches wird festgelegt, über welche Unternehmensbereiche sich die Vorgaben erstrecken und für welche Personengruppen das Sicherheitskonzept verbindlich ist. In Anbetracht der Tatsache, dass die vorgegebenen Richtlinien und Massnahmen in der Praxis umgesetzt und auch kontrolliert werden müssen, sollte die Reichweite des Gültigkeitsbereiches wohl überlegt und nicht zu gross gewählt werden. Wenn externe Partner und Instanzen Bestandteil des Gültigkeitsbereiches sind, muss die Vereinbarkeit von Durchsetzung und Kontrolle der Anwendung des Sicherheitskonzeptes genau überprüft werden. (Schmidt, 2006, S.93)

Definition der Verantwortlichkeiten und Kompetenzen im Kontext des Sicherheits-Managements

In jedem Sicherheitskonzept muss klar geregelt werden, welche Rollen im Sicherheits-Management existieren und wer über welche Verantwortlichkeiten und Kompetenzen verfügt. Die Kompetenzen sollten eindeutig verteilt sein und sich personell nicht überschneiden, um Konfliktsituationen durch Kompetenzgerangel zu vermeiden. (Schmidt, 2006, S.94)

Die Beschreibung des Aufbaus der Sicherheitsorganisation schafft für alle Beteiligten nicht nur einen Überblick über die Rollen, die sich mit sicherheitsrelevanten Themen im Unternehmen beschäftigen, über die Funktionen und Aufgaben, die von diesen Rollen wahrgenommen werden und über die Positionen im Organigramm, die sicherheitsrelevante Aufgaben übernehmen, sondern zeigt gleichzeitig auf, in welcher Form diese Positionen kooperieren und wie sie sich voneinander abgrenzen (Schmidt, 2006, S.33). So muss bspw. festgelegt werden, ob es eine zentrale Rolle des Sicherheitsmanagers gibt, der für alle sicherheitsrelevanten Aspekte verantwortlich und zuständig ist, oder ob das Sicherheits-Management weitere Rollen wie diejenige des Risikomanagers, des IT- Sicherheitsbeauftragten, des Datensicherungsverantwortlichen oder des Datenschutzverantwortlichen umfasst.

Begriffe und Definitionen

Alle für die Informations- und Datensicherheit des Unternehmens relevanten Begriffe müssen im Sicherheitskonzept eindeutig definiert und erläutert werden, um den Interpretationsspielraum des verwendeten Vokabulars möglichst gering zu halten. Die Arbeit und der unternehmensweite Umgang mit den unterschiedlichen Aspekten der Sicherheit werden durch einen einheitlichen Sprachgebrauch und ein gemeinsames Verständnis der Begriffe erheblich erleichtert. (Schmidt, 2006, S.93)

Dokumentation der Bedeutung der Informations- und Datensicherheit für das Unternehmen

Wie bereits einleitend erwähnt, können die Wichtigkeit und die Bedeutung der Informationssicherheit und der Datensicherheit von Unternehmen zu Unternehmen auf Grund unterschiedlicher Einflüsse variieren. Zu den Einflussfaktoren von Aussen zählen unter anderem die Branche, der die Institution angehört, die Risikobereitschaft der Institution, Vorschriften von Aufsichtsbehörden oder gesetzliche Vorgaben (Schmidt, 2006, S.93). Umso wichtiger ist es demnach, den Stellenwert der Sicherheit bezüglich Informationen, Informationssystemen und Daten explizit darzustellen und schriftlich festzuhalten. Dies dient der Orientierung aller Mitarbeitenden über den Status der Sicherheit und gibt dem verantwortlichen Sicherheits-Team

durch die Unterschrift der Unternehmensleitung den nötigen Rückhalt bei Budgetverhandlungen und Zielkonflikten mit anderen Unternehmensbereichen oder Abteilungen (Schmidt, 2006, S.93).

Nennung der sicherheitskritischen Prozesse, der schutzbedürftigen Werte und der grundsätzlichen Sicherheitsziele

Um die Beteiligten des Gültigkeitsbereiches des Sicherheitskonzepts für die Informations- und Datensicherheit zu sensibilisieren, müssen alle schutzbedürftigen Unternehmenswerte, Prozesse und Sicherheitsziele im Sicherheitskonzept detailliert aufgelistet und beschrieben werden. Die Sicherheitsziele zeigen dabei auf, mit welchen Mitteln, Vorgehensweisen und Massnahmen die Werte und Prozesse geschützt werden sollen. (Schmidt, 2006, S.94)

Integriertes Datensicherungskonzept mit den Richtlinien, Regeln und Massnahmen zur Umsetzung und Gewährleistung der Informationssystem- und Datensicherheit

In Kapitel 3.4.2 werden die einzelnen Komponenten der Datensicherung sowie deren Zusammenwirken in Form eines Datensicherungskonzepts ausführlich betrachtet.

Definition der Verantwortlichkeiten und Konsequenzen bei Nichteinhalten des Sicherheitskonzepts

Der Sinn von Regelungen zur Informations- und Datensicherheit liegt darin, dass diese den Beteiligten nicht nur bekannt sind, sondern von diesen auch befolgt werden (Junk, 2003, S.16). Basierend auf dieser Überlegung sollte das Sicherheitskonzept Massnahmen enthalten, die beschreiben, wie die Einhaltung kontrolliert wird und mit welchen Sanktionen bei Nichteinhalten des Sicherheitskonzepts gerechnet werden muss (Schmidt, 2006, S.94).

Regelungen und Massnahmen zur Kontrolle und Überprüfung des Sicherheitskonzepts

Abschliessend sollten im Sicherheitskonzept geeignete Regeln und Massnahmen festgelegt werden, die die Kontrolle des Sicherheitskonzepts auf dessen Durchführbarkeit und Aktualität betreffen. Grundsätzlich sollte ein Sicherheitskonzept möglichst stabil formuliert werden, damit es nur selten verändert werden muss. Dennoch bedingen Entwicklungen wie bspw. ein Wechsel der Unternehmensleitung, Fusionen, Umstrukturierungen oder technologische Fortschritte eine Anpassung der Inhalte des Sicherheitskonzepts an die neuen Gegebenheiten. (Schmidt, 2006, S.93)

Die Formulierung all dieser Aspekte eines Sicherheitskonzepts sollte nicht übermässig viel Platz beanspruchen, so dass das Sicherheitskonzept einen Umfang von gut fünf bis zehn Seiten aufweist (Schmidt, 2006, S.94).

3.4.2 Aufbau eines Datensicherungskonzepts

Im Gegensatz zu Sicherheitskonzepten, zu deren typischen Inhalten Regelungen zur Nutzung des Internets und zum sachgemässen Umgang mit E-Mails gehören (Junk, 2003, S.17), beschäftigen sich Datensicherungskonzepte ausführlicher mit der Sicherung von Daten. Dies beruht auf dem Grundprinzip der Datensicherung, welches die regelmässige Erstellung von Sicherungskopien vorsieht (Hoppe/Priess, 2003, S.221), um im Störfall auf die redundanten Daten zurückgreifen zu können und somit einem Datenverlust oder einem Unterbruch der betrieblichen Abläufe vorzubeugen.

Damit die Sicherung und Rekonstruierung aller Daten und Informationssysteme zu jeder Zeit gewährleistet sind, sollte neben dem Sicherheitskonzept ein spezifisches Datensicherungskonzept entwickelt werden, welches bei Änderungen der Systemkonfiguration aktualisiert und an die neuen Rahmenbedingungen angepasst wird (Hoppe/Priess, 2003, S.221).

Vom Aufbau her enthalten sowohl das Sicherheitskonzept als auch das Datensicherungskonzept einige recht ähnliche Punkte, was sich besonders im Bereich der organisatorischen Massnahmen zeigt. Grundsätzlich umfasst das Datensicherungskonzept Regelungen zu folgenden Aspekten (vlg. Hoppe/Priess, 2003, S.221; BSI, 2006, S.3423):

- Verantwortlichkeiten für die Durchführung bzw. Überwachung der Sicherung
- Zeitintervall zwischen den Sicherungsvorgängen
- Zeitpunkt der Sicherung
- Art der Datensicherung
- Anzahl der aufzubewahrenden Sicherungsvorgänge
- Verwendete Datenträger
- Dokumentation bzw. Protokollierung der Sicherungsvorgänge
- Archivierung der Sicherungsdaten
- Rekonstruktionsplan

Da die Archivierung und die Massnahmen zur Wiederherstellung der Daten einen besonders hohen Stellenwert im Bereich der Datensicherung einnehmen, kann es durchaus sinnvoll sein, zusätzlich zum Datensicherungskonzept ein separates Archivierungskonzept und einen separaten Rekonstruktionsplan zu erarbeiten (Hoppe/Priess, 2003, S.221).
Für die Erstellung eines Datensicherungskonzepts darf der Einfluss bestimmter Modalitäten auf das einzusetzende Datensicherungsverfahren nicht ausser Acht gelassen werden, da die

Datensicherung durch folgende Faktoren wesentlich beeinflusst (vgl. Hoppe/Priess, 2003, S.222; BSI, 2006, S.3424ff.) wird:

- Wiederverfügbarkeit der Daten
- Datenmenge
- Änderungshäufigkeit und Änderungszeitpunkt der Daten
- Möglichkeit zur Durchführung der Datensicherung während des laufenden Systembetriebs
- Verfügbares Budget
- Wissensstand der Systemnutzer

Die zuvor genannten Bestandteile eines Datensicherungskonzepts sollen an dieser Stelle genauer erläutert werden, um die einzelnen Aspekte verstehen und nachvollziehen zu können.

Verantwortlichkeiten für die Durchführung bzw. Überwachung der Sicherung

Wie bereits im Sicherheitskonzept muss auch im Datensicherungskonzept klar festgelegt werden, welche Stelle bzw. welche Person oder welcher Personenkreis für die Datensicherung verantwortlich ist. Zu den möglichen Verantwortlichen zählen der IT-Benutzer selbst, der Systemverwalter oder ein speziell für die Datensicherung ausgebildeter Administrator (BSI, 2006, S.3432).

Je nachdem, ob die Sicherung manuell oder automatisch durchgeführt wird, muss der Sicherungsvorgang regelmässig ausgelöst bzw. bei einem automatisierten Verfahren zunächst konfiguriert werden (Hoppe/Priess, 2003, S.222). Zu den weiteren Aufgaben der zuständigen Stelle gehören, wenn nötig, das Einlegen und Wechseln der Speichermedien, sowie bei der automatischen Datensicherung die Überwachung des Sicherungsvorgangs, um auf auftretende Fehlermeldungen in einem angemessenen Zeitrahmen reagieren zu können (Hoppe/Priess, 2003, S.222).

Neben der Klärung der Zuständigkeiten für die Datensicherung muss ebenfalls definiert werden, wer über die Berechtigung eines Zugriffs auf die Datensicherungsträger verfügt und wer befugt ist, Entscheidungen bezüglich einer Daten-Rekonstruktion zu treffen bzw. erforderliche Massnahmen zu veranlassen (BSI, 2006, S.3432). Die für die Datensicherung verantwortliche Stelle muss jederzeit erreichbar sein, weshalb zusätzlich ein Vertreter benannt

werden muss, der entsprechend in das Arbeitsfeld der Datensicherung eingearbeitet ist (BSI, 2006, S.3432).

Zeitintervall zwischen den Sicherungsvorgängen und Zeitpunkt der Sicherung

Nach einem Datenverlust oder einer Datenbeschädigung müssen für die Wiederherstellung des Ursprungszustandes sämtliche Änderungen, denen die Daten seit der letzten Datensicherung unterlegen sind, erneut vorgenommen werden (BSI, 2006, S.3426). Demnach entsteht bedeutend weniger Aufwand für eine Rekonstruktion der Daten, wenn der zeitliche Abstand zwischen den einzelnen Datensicherungsvorgängen kurz gewählt wird (Hoppe/Priess, 2003, S.222). Gerade bei Daten, die häufig geändert werden, sollten die Zeitintervalle möglichst gering sein (Hoppe/Priess, 2003, S.222).

Bezüglich der Wahl des geeigneten Zeitpunktes für die Datensicherung gilt zu beachten, dass der Datenbestand nicht nur periodisch (täglich, wöchentlich, monatlich o. ä.) gesichert werden kann, sondern dass eine Datensicherungen auch nach einem besonderen Ereignis, wie bspw. nach dem Ausführen einer bestimmten Anwendung oder nach einer Systemkonfiguration, erforderlich sein kann (BSI, 2006, S.3426).

Art der Datensicherung

Das Datensicherungskonzept sollte Angaben zur eingesetzten Datensicherungsstrategie enthalten. Zu den verschiedenen Möglichkeiten der Datensicherung gehören die Datenspiegelung, vollständige, inkrementelle, differenzielle und selektive Datensicherungen und die redundante Datenspeicherung mittels RAID-Systemen. Kapitel 2 befasst sich ausführlich mit der Darstellung von Verfahren zur Datensicherung und mit möglichen Datensicherungsstrategien.

Anzahl der aufzubewahrenden Sicherungsvorgänge

Auch Datensicherungen sind vor Fehlern nicht geschützt, weshalb gewährleistet sein muss, dass die Sicherungskopien möglichst lange aufbewahrt werden (BSI, 2006, S.3426). Die Sicherungsdaten dienen als so genannte Ankerpunkte (Hoppe/Priess, 2003, S.223), bei denen im Falle einer Rekonstruktion von Daten angesetzt werden kann. In der Praxis wird im Bereich der Datensicherung häufig nach dem Mehr-Generationen-Prinzip verfahren, welches auch als „Grossvater-Vater-Sohn-Prinzip“ bezeichnet wird, wobei unter einer Generation eine vollständige Datensicherung verstanden wird (Hoppe/Priess, 2003, S.223).

Im Datensicherungskonzept muss nicht nur die Anzahl der aufzubewahrenden Generationen festgehalten werden, sondern auch der Zeitabstand, der zwischen den einzelnen Generationen liegen muss (BSI, 2006, S.3426). Dieser zeitliche Abstand darf ein Mindestmass nicht unterschreiten und wird deshalb als Mindestalter bezeichnet (BSI, 2006, S.3427). Das Bundesamt für Sicherheit in der Informationstechnik macht dies an folgendem Beispiel deutlich:

> *„In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrüchen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.“* (BSI, 2006, S.3427)

Je höher das Mindestalter angesetzt wird, desto grösser ist die Wahrscheinlichkeit, dass zu einer beschädigten oder gelöschten Datei noch eine Vorgängerversion zur Verfügung steht und je mehr Generationen vorhanden sind, desto aktueller ist die benötigte Vorgängerversion (BSI, 2006, S.3427).

Ausgehend von der Anforderung, für jede Generation eigene Datenträger zu verwenden, ergibt sich ein enger Zusammenhang mit den Kosten für die Datensicherung (Hoppe/Priess, 2003, S.223). Nach wirtschaftlichen Überlegungen sollte die Anzahl der Generationen demnach auf ein sinnvolles Mass beschränkt werden (BSI, 2006, S.3427).

Verwendete Datenträger

Erst nachdem die Parameter „Art der Datensicherung“, „Häufigkeit“ und „Anzahl der aufzubewahrenden Generationen“ festgelegt worden ist, kann die Wahl des geeigneten Datenträgers bzw. Speichermediums getroffen werden (BSI, 2006, S.3428). Bei der Entscheidung zum Einsatz des angemessenen Speichermediums sollte beachtet werden, dass sich diese bezüglich gewisser Eigenschaften wie der Zugriffszeiten, der Transferrate, der Handhabbarkeit, der Speicherkapazität und der Kosten unterscheiden (Hoppe/Priess, 2003, S.224). Ebenso muss in Betracht gezogen werden, dass die einzelnen Datenträger auch entsprechende Lese- und Schreibgeräte erfordern (Hoppe/Priess, 2003, S.224), die weitere Kosten verursachen und Platz beanspruchen.

Mögliche Datenträger für die Datensicherung sind Mikrofilme, optische Speichermedien (CDROM, WORM, DVD), magnetische Speichermedien (Disketten, Festplatten, Bänder) und Halbleiterspeicher, so genannte RAM (Random Access Memory) (Müller, 2003, S.96).

Das Datensicherungskonzept sollte beschreiben, welche Datenträger verwendet werden und in welcher Kombination bzw. mit welchen weiteren Apparaten diese eingesetzt werden.

Dokumentation bzw. Protokollierung der Sicherungsvorgänge

Sämtliche durchgeführten Sicherungsvorgänge sollten in einem Sicherungsprotokoll dokumentiert werden. Bestandteil des Protokolls sind mindestens eine eindeutige Bezeichnung des Datenträgers, das Datum der Sicherung und die für die Durchführung verantwortliche Stelle oder Person. (Hoppe/Priess, 2003, S.224)

Archivierung der Sicherungsdaten

Eine wichtige Rolle bezüglich der Archivierung der gesicherten Daten spielt der Aspekt des Aufbewahrungsortes. Grundsätzlich sollten die Originaldatenträger und die Datenträger mit den gespeicherten Daten an unterschiedlichen Orten aufbewahrt werden (BSI, 2006, S.3433). Die Wahrscheinlichkeit, dass die Sicherungskopien in einem Katastrophenfall (Brand, Wasser, Stromunterbruch o. ä.) beschädigt werden, kann gesenkt werden, indem die Datenträger mit den Sicherungskopien in einem anderen Gebäudeteil oder sogar an einem anderen Standort verwahrt werden (BSI, 2006, S.3433). Allerdings entstehen durch die Auslagerung der Datenträger auch dementsprechend längere Transportwege und Transportzeiten (BSI, 2006, S.3433), was sich im Fall einer Rekonstruktion hinderlich oder sogar negativ auswirken kann. Demnach sollten bei der Wahl des Aufbewahrungsortes die Anforderungen an die Verfügbarkeit der Sicherungsdatenträger miteinbezogen werden.

Rekonstruktionsplan

Datensicherungen dienen der zeitnahen Rekonstruktion von Daten und Programmen. Bei der Durchführung einer Rekonstruktion müssen die gesicherten Daten zunächst eine Sicherheitsprüfung durchlaufen, um sicherzustellen, dass die Daten konsistent sind und keine Malware vorhanden ist (Hoppe/Priess, 2003, S.226). Bei einer vollständigen Rekonstruktion eines Datenbestandes wird zuerst die letzte Generation zurückgespielt und anschliessend, je nach Datensicherungsstrategie (differenziell, inkrementell), werden die benötigten Teilsicherungen zurückgespielt. Sind nur ein oder mehrere Teile des Datenbestandes von der Rekonstruktion betroffen, so werden diese aus den betreffenden Datensicherungen seit der letzten Generation extrahiert. (Hoppe/Priess, 2003, S.226)

Mit regelmässigen Simulationen von Rekonstruktionen sollte die Funktionsfähigkeit des eingesetzten Verfahrens kontrolliert und überprüft werden.

Das Datensicherungskonzept sollte einen Rekonstruktionsplan enthalten, in welchem folgende Punkte festgelegt werden (vgl. BSI, 2006, S.3387; Hoppe/Priess, 2003, S.227):

- Speicherort von Programmen und Daten im Normalbetrieb
- Bestand der gesicherten Daten (Bestandsverzeichnis)
- Zeitpunkte der Datensicherung
- Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten
- Aufbewahrungsort der gesicherten Programme und Daten und ggf. erforderliche Zutrittsmittel

Ein Rekonstruktionsplan mit diesen Angaben unterstützt im Notfall einen sachverständigen Dritten bei der Beschaffung und Installation der Programme und Daten, die für einen Wiederanlauf des Informationssystems benötigt werden (Hoppe/Priess, 2006, S.226f.).

Sowohl für die Entwicklung eines Sicherheitskonzepts als auch für die Konzeption eines Datensicherungskonzepts lohnt es sich, diverse Listen anzulegen. Zu diesen Listen zählen (vgl. Kersten/Klett, 2005, S. 90):

- Liste der Objekte (Prozesse, Systeme, Daten)
- Liste der Subjekte (Personal)
- Liste der Bedrohungen/Risiken (auf Grund der Risikoanalyse)
- Liste der Massnahmen

Die Listen schaffen einen klaren Überblick und erleichtern den kontinuierlichen Verbesserungsprozess der sicherheitsspezifischen Dokumente, da sie mit wenig Aufwand geändert, angepasst und erweitert werden können.

4 Sicherheitskonzepte und Massnahmen zur Datensicherung in Bibliotheksverbünden

Auf der Basis der vorhergehenden theoretischen Grundlagen zu den Aspekten der Datensicherheit, Datensicherung sowie zu Sicherheits- und Datensicherungskonzepten folgt nun die Darstellung der konkret umgesetzten Massnahmen zur Sicherung der Benutzerdaten und der bibliographischen Daten im IDS Universität Zürich, in der Schweizerischen Nationalbibliothek und im Südwestdeutschen Bibliotheksverbund. Sämtliche Aussagen entstammen den retournierten Fragebögen, wobei zwei Institutionen den Fragebogen im Word-Format beantwortet haben und eine Organisation die Online-Version des Fragebogens zur Beantwortung gewählt hat. Auf Grund der Vertraulichkeit gewisser Daten begrenzt sich der Umfang der Informationen zu den Sicherheitsmassnahmen der Universität Zürich. Im Weiteren unterliegen die Daten des IDS Universität Zürich keiner eigenen Security Policy, sondern werden von den Informatikdiensten der Universität Zürich entsprechend der allgemeinen Regelungen behandelt. Zu diesen Regelungen gehören das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) und die „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006). Ansonsten standen für die vorliegende Ausarbeitung keine weiteren Dokumente wie IT-Sicherheitsleitlinien, IT-Sicherheitsrichtlinien oder Sicherheitskonzepte zur Verfügung, so dass hauptsächlich die beantworteten Fragebögen ausgewertet werden konnten.

Die Antworten werden in Anlehnung an den in Kapitel 1.3.2 erläuterten Aufbau des Fragebogens thematisch gegliedert und anhand des jeweiligen Themenbereichs aufgeführt. Für das Verständnis einzelner Begriffe, Verfahren oder Strategien wird auf die jeweiligen Kapitel verwiesen, in denen diese ausführlich erklärt sind.

4.1 Grundlegendes

Bedeutung des Themas „Sicherheit“ in Strategie / Leitbild / Vision / Mission	
IDS	In der Informatikstrategie (Bachmann, 2005, S.20) der Informatikdienste der Universität Zürich wird die Bedeutung der IT-Sicherheit dargestellt und aufgezeigt, in welcher Form die Informatikdienste zur Gewährleistung der Sicherheit beitragen.
NB	Der Aspekt der Sicherheit ist mit der Zielformulierung „Datensicherheit garantieren“ schriftlich festgehalten.

SWB	Das Bibliotheksservice-Zentrum Baden-Württemberg (BSZ) verfügt über eine offizielle IT-Sicherheitsleitlinie mit Stand vom 10.03.2007, womit dem hohen Stellenwert der Sicherheit der Informationssysteme und der Daten Rechnung getragen wird.

Vorhandensein eines Sicherheitskonzepts für die Datensicherung der Benutzer- und Bestandsdaten	
IDS	Für die Datensicherung im IDS Universität Zürich besteht kein eigenes Sicherheitskonzept, da die Daten nach den allgemeinen Regelungen der Informatikdienste der Universität Zürich gesichert werden. Dokumente, die Bezug zum Umgang mit den Daten und deren Sicherung nehmen, sind das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) und die „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006). Diese Vorschriften sind den Mitarbeitenden bekannt.
NB	Die Bundesverwaltung, zu der die Schweizerische Nationalbibliothek gehört, erlässt auf verschiedenen Stufen Richtlinien, die den Umgang mit Daten und deren Sicherung regeln. Diese Richtlinien sind den sie betreffenden Mitarbeitenden bekannt.
SWB	Ein Sicherheitskonzept für die Datensicherung der Benutzer- und Bestandsdaten des SWB existiert momentan nur im E-Mail-Format. Ein offizielles Dokument wird derzeit nach den IT-Grundschutz-Katalogen des BSI[5] erstellt. Die vorhandenen Regelungen zur Gewährleistung der Datensicherheit sind den sie betreffenden Mitarbeitenden bekannt.

4.2 Sicherheitskonzept

Im Fragebogen bezogen sich die folgenden Aspekte auf ein bereits vorhandenes Sicherheitskonzept bzw. Security Policy Dokument.

[5] IT-Grundschutz-Kataloge des BSI: http://www.bsi.bund.de/gshb/deutsch/index.htm [27.08.2007].

Beeinflussung durch Gesetze, Vorschriften, Normen und Standards	
IDS	Die Datensicherheit im IDS Universität Zürich wird durch das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) und die „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006) geregelt und erhält weitere Einflüsse durch das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BüPF), die Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VüPF) sowie weitere Kantonale Datenschutzgesetze.
NB	Die Sicherheitsrichtlinien der NB enthalten Hinweise auf die „Weisung des IRB[6] über die Informatiksicherheit in der Bundesverwaltung“, auf das „Informatik-sicherheitsleitbild“ und auf die „Weisung über die Nutzung von Informations- und Kommunikationsmitteln“.
SWB	Die bestehenden Regelungen zur Datensicherung im E-Mail-Format werden nicht durch Gesetze, Vorschriften, Normen oder Standards beeinflusst. Das Dokument, welches momentan erarbeitet wird, wird nach den Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI)[7] erstellt.

Bedeutung der Themen Sicherheit und/oder Datensicherung im Sicherheitskonzept	
IDS	Die Bedeutung des Sicherheits- und des Datensicherungsaspekts werden im „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) und in den „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006) nicht explizit erläutert. Die Wichtigkeit der Gewährleistung der Sicherheit ergibt sich aber aus den strengen Sicherheitsvorschriften (vgl. Universität Zürich, Universitätsleitung, 2006, S.5) und den Normen, die in den beiden Dokumenten festgelegt sind.
NB	Die Bedeutung der Themen Sicherheit und Datensicherung wird im Informatik-sicherheitsleitbild mit folgendem Wortlaut dargestellt:

[6] Der Informatikrat Bund (IRB) trägt die Gesamtverantwortung für die IKT der Bundesverwaltung und erlässt Vorgaben wie Strategien, Architekturen und Sicherheitsweisungen (ISB, 2007).

[7] IT-Grundschutz-Kataloge des BSI: http://www.bsi.bund.de/gshb/deutsch/index.htm [27.08.2007].

	„Die Informatik ist für das Eidgenössische Departement des Innern (EDI) bei der täglichen Arbeit zu einem unverzichtbaren Bestandteil geworden und gilt als ein Gut, welches einen hohen Schutzbedarf geniesst. Das Ziel dieses Leitbildes ist der umfassende Schutz der Informatiksysteme und der Daten in Bezug auf deren Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit. Dieses Leitbild bildet die Basis für die Entwicklung und die Umsetzung einer risikogerechten und wirtschaftlich angemessenen Informatiksicherheit innerhalb des EDI. Das Leitbild definiert Schutzziele, Grundregeln und bestimmt die für die Organisation der Informatiksicherheit zuständigen Verantwortlichkeiten.“
SWB	Die hohe Bedeutung des Sicherheitsaspektes spiegelt sich in der Erstellung eines Dokuments "IT-Sicherheits-Management" wider, welches einen Unterpunkt "Datensicherungskonzept" enthält. Aufbau und Inhalt des Datensicherungskonzepts lehnen sich an die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) an, das unter der Annahme der typischen Gefährdungslage eines Verlustes gespeicherter Daten zur Konzeption eines solchen Datensicherungskonzepts rät (BSI, 2007a). Das BSI schlägt ein Datensicherungskonzept mit folgendem Aufbau vor (BSI, 2007a): **Planung und Konzeption** • Entwicklung eines Datensicherungskonzepts • Erhebung der Einflussfaktoren der Datensicherung • Festlegung der Verfahrensweise für die Datensicherung • Festlegung des Minimaldatensicherungskonzepts **Beschaffung** • Beschaffung eines geeigneten Datensicherungssystems **Umsetzung** • Verpflichtung der Mitarbeiter zur Datensicherung • Sicherungskopie der eingesetzten Software • Dokumentation der Datensicherung

	Betrieb • Geeignete Aufbewahrung der Backup-Datenträger • Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen • Regelmässige Datensicherung **Notfallvorsorge** • Übungen zur Datenrekonstruktion

Bedeutung der Sicherheitskriterien Verfügbarkeit, Vertraulichkeit, Integrität u.w. (siehe Kapitel 3.1)	
IDS	Das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ schreibt vor, dass *„für jeden Computer […] die Sicherheitsanforderungen bezüglich* • *Vertraulichkeit und Zugangsschutz,* • *Datensicherheit und* • *Verfügbarkeit* *festzulegen und mit geeigneten Massnahmen sicherzustellen [sind].“* (Universität Zürich, Universitätsleitung, 2006) Die „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006) umfassen die konkreten Massnahmen zur Gewährleistung der genannten Sicherheitskriterien.
NB	Die Sicherheitskriterien werden im Leitbild genannt, aber nicht genauer definiert: „Das Ziel dieses Leitbildes ist der umfassende Schutz der Informatiksysteme und der Daten in Bezug auf deren Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit.“
SWB	In der offiziellen IT-Sicherheitsleitlinie wird auf die Bedeutung der Sicherheitskriterien hingewiesen.

Bereitschaft des Managements für die Bereitstellung der erforderlichen Mittel und Ressourcen	
IDS	Die für die Gewährleistung der Sicherheit der Systeme und Daten notwendigen Ressourcen und Mittel stehen zur Verfügung, wofür sich das Management bereit erklärt.
NB	Das Management erklärt sich im Leitbild schriftlich dazu bereit, die für die Sicherheit und Datensicherung notwendigen Mittel und Ressourcen zur Verfügung zu stellen.
SWB	Im Rahmen der offiziellen IT-Sicherheitsleitlinie erklärt sich das Management schriftlich dazu bereit, die benötigten Mittel und Ressourcen zur Gewährleistung der Datensicherung zur Verfügung zu stellen.

Ziele und Vorgaben zur Datensicherung	
IDS	Übergreifende Sicherheitsziele werden im „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ nicht speziell erwähnt, allerdings wird festgehalten, dass *„die Systeme […] so zu pflegen [sind], dass sie vor Missbrauch durch Dritte bestmöglich geschützt sind. Insbesondere ist dafür Sorge zu tragen, dass ein Angriff auf weitere Computer im Netzwerk und die Ausbreitung von schädlichen Programmcodes möglichst wirksam verhindert wird.“* (Universität Zürich, Universitätsleitung, 2006) Vorgaben und Massnahmen, mit denen die Sicherheitskriterien der Vertraulichkeit und des Zugangsschutzes, der Datensicherheit und der Verfügbarkeit erfüllt werden, werden in den „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006) konkretisiert.
NB	Das Informatiksicherheitsleitbild enthält grobe Ziele zur Datensicherung: „Eine absolute Sicherheit kann nie garantiert werden. Jedoch ist das Ziel aller Massnahmen, in allen Bereichen der täglichen Arbeit ein angemessenes Sicherheitsniveau einzuführen. Auch werden die Sicherheitsmassnahmen darauf hin ausgerichtet, die Häufigkeit und die Auswirkungen schädigender Ereignisse zu minimieren.“

SWB	Die offizielle IT-Sicherheitsleitlinie und deren Anhänge weisen auf übergreifende Ziele und Vorgaben zur Datensicherung hin. Der konkrete Wortlaut ist nicht bekannt.

Beteiligte, Aufgaben, Verantwortlichkeiten	
IDS	Rollen, Aufgaben und Verantwortlichkeiten werden in verschiedenen Dokumenten geregelt, wie bspw. den Leistungsvereinbarungen, die vertraulich eingestuft sind. Das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) beschreibt die Aufgabenbereiche der Endbenutzenden und Systemadministratoren, der Benutzereinheiten, der Informatikdienste und der IT-Sicherheitsstelle der Universität Zürich.
NB	Das Leitbild enthält eine Beschreibung der Zuständigkeiten der einzelnen Rollen vom Führungsorgan bis zum Applikationsverantwortlichen.
SWB	Die Verantwortlichkeiten für die Datensicherung sind in der offiziellen IT-Sicherheitsleitlinie ausführlich dargestellt und schriftlich festgehalten.

Sensibilisierung, Schulung und Übung der Beteiligten	
IDS	Massnahmen für die Sensibilisierung der Mitarbeitenden für die Datensicherung sind nach dem aktuellen Wissensstand in keinem Dokument schriftlich definiert.
NB	Im Leitbild wird mit folgendem Wortlaut auf die Schulung eingegangen: „Die Schulung aller Mitarbeitenden im korrekten Umgang mit Daten und IKT-Mitteln wird als wichtig erachtet und wird gefördert.“
SWB	Auf die Sensibilisierung und Schulung der Mitarbeitenden bezüglich der Datensicherung wird grosser Wert gelegt. Konkrete Massnahmen werden derzeit auf der Ebene des Managements, auf der Anwendungsebene und auf der Systemadministrationsebene erarbeitet.

Prüfung, Aktualisierung, Pflege und Weiterentwicklung des Sicherheits-Managements	
IDS	Es liegen keine Informationen bezüglich der Kontrolle und Weiterentwicklung der sicherheitsspezifischen Dokumente vor.
NB	Zur Kontrolle wird Folgendes festgehalten: „Die Einhaltung des Leitbildes wird in erster Linie durch die Informatiksicherheits-beauftragten oder bei Bedarf in Zusammenarbeit mit einer Revisionsstelle (z.B. ISB-SEC, externe Firma, EFK) regelmässig überprüft.“
SWB	Die Dokumente, die Vorgaben, Ziele und Massnahmen zur Datensicherung und Datensicherheit regeln, werden auf einem File-Server gehalten und über das IT-Grundschutz Tool GSTOOL[8], welches vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellt wird, verwaltet. Auf diese Weise werden die Sicherheits-Dokumente laufend überarbeitet, womit deren Aktualität gewährleistet wird.

Verpflichtung des Managements und der Mitarbeitenden zur Sicherheit	
IDS	Das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ weist auf die Einhaltung der Vorschriften und der „Normen für den Betrieb von Systemen an der Universität Zürich“ hin (Universität Zürich, Universitätsleitung, 2006, S.5).
NB	Das Informatiksicherheitsleitbild enthält eine Verpflichtung aller Mitarbeitenden und des Managements zur Einhaltung der im Informatiksicherheitsleitbild vorgegebenen Massnahmen.
SWB	Die offizielle IT-Sicherheitsleitlinie sieht eine Verpflichtung des Managements und der Mitarbeitenden zur Gewährleistung der Sicherheit durch Einhalten der IT-Sicherheitsleitlinie vor.

[8] Das GSTOOL ist eine vom BSI zur Verfügung gestellt Software, die die Anwender bei der Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend den IT-Grundschutzkatalogen unterstützt (BSI, 2007b).

Regelung der Vergabe und Verwaltung von Zugriffsrechten	
IDS	Im „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ (Universität Zürich, Universitätsleitung, 2006) und in den „Normen für den Betrieb von Systemen an der Universität Zürich“ (Universität Zürich, Informatikdienste, 2006) wird die Vergabe und Verwaltung der Zugriffsrechte nicht geregelt. Dies erfolgt an anderer Stelle.
NB	Wie und von wem Zugriffsrechte vergeben und verwaltet werden, wird nicht in der Policy sondern in einem Rollenmodell und dem Prozessbeschrieb festgelegt.
SWB	Die Vergabe von Zugriffsrechten wird klar geregelt. Die Dokumente werden auf einem File-Server gehalten und über das GSTOOL vom BSI verwaltet. Die Aktualität der Dokumente wird durch die laufende Bearbeitung durch das BSI gesichert.

Richtlinien zum Aufbau und Wechsel von Passwörtern	
IDS	Das „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ hält fest: *„Starke Passwörter sind mindestens 8 Zeichen lang, haben aus jeder der vier Buchstabengruppen Grossbuchstaben, Kleinbuchstaben, Ziffern und Sonder-zeichen (wie Satzzeichen u.ä.) mindestens ein Element und dürfen keine erkennbare Konstruktionsregel aufweisen.“* (Universität Zürich, Universitätsleitung, 2006, S.2) Hinweise, in welchem Rhythmus Passwörter geändert werden müssen, sind keine vorhanden, da dies IDS-spezifisch geregelt wird.
NB	Regeln zum Aufbau von Passwörtern werden nicht in der Policy festgehalten, sondern separat vom Bundesamt für Informatik und Telekommunikation definiert. Passwörter müssen alle 42 Tage geändert werden.
SWB	Die offizielle IT-Sicherheitsleitlinie enthält zurzeit keine Vorgaben zum Aufbau und Wechsel von Passwörtern. Für Passwörter des Bibliotheksservice-Zentrums Baden-Württemberg (BSZ) ist dies zukünftig geplant. Was die Passwörter der am SWB teilnehmenden Bibliotheken anbelangt, so sind Regelungen zum Aufbau und vor allem zum Wechsel organisatorisch schwer durchsetzbar, weshalb keine Regeln festgelegt sind.

4.3 Datensicherung / Backup-Management

Art der Datensicherung (komplett, differenziell, inkrementell, selektiv; siehe Kapitel 2.2.2) und Rhythmus der Datensicherung (zeitversetzt, zeitnah, Echtzeit; siehe Kapitel 2.2.3)	
IDS	Die Daten der Systeme der Universität Zürich werden einmal täglich, mit drei Versionen in die Vergangenheit, gesichert. Dies bedeutet, dass bei einem täglichen Backup auf drei Tage zurück und bei einem wöchentlichen Backup auf drei Wochen zurück gesichert wird. Die Oracle Datenbanken werden einmal wöchentlich mit zwei Versionen zurück gesichert. Für die Datensicherung werden komplette, differenzielle, inkrementelle und selektive Sicherungsverfahren angewendet. Neben diesen zeitversetzten Datensicherungen werden die Daten zusätzlich über RAID und SAN[9]-Systeme gesichert, so dass teilweise asynchrone (zeitnahe) und synchrone (Echtzeit) Sicherungen das klassische Backup ergänzen.
NB	Die NB verfolgt den Ansatz der inkrementellen Datensicherung: Zu Beginn wird eine komplette Datensicherung durchgeführt, mit anschliessenden Folgedatensicherungen der Dateien, die sich gegenüber dem vorherigen Sicherungslauf verändert haben. Die Komplettsicherung erfolgt dabei in festen Zeiträumen, die inkrementelle Sicherung täglich in der Zwischenzeit. Die Datensicherung erfolgt demnach zeitversetzt, da die Daten zu bestimmten Zeiten gesichert werden und nicht in Echtzeit gespiegelt oder zeitnah mit einem Abstand von wenigen Sekunden bis Minuten gespeichert werden.
SWB	Der Südwestdeutsche Bibliotheksverbund sichert die Benutzer- und Bestandsdaten durch komplette und inkrementelle Datensicherungen, die im Wechsel durchgeführt werden. Über Logfiles erfolgt alle zwei Stunden eine inkrementelle Sicherung der Daten. Zeitversetzt wird jede Nacht eine inkrementelle Bandsicherung und einmal pro Woche eine Komplettbandsicherung ausgeführt. Zusätzlich besteht eine zeitgleiche Datensicherung auf einen zweiten Rechner, um bei einem technischen Problem den Betrieb aufrechterhalten zu können.

[9] Mit dem Einsatz eines so genannten Storage Area Network, kurz SAN, können Server als Engpässe der Datensicherung umgangen werden, indem die zu sichernden Daten direkt auf das Speichermedium geschrieben werden (Hoppe/Priess, 2003, S.181).

Backup nach dem RAID-Konzept (siehe Kapitel 2.2.4)	
IDS	Für die Datensicherung an der Universität Zürich werden verschiedenste RAID-Level eingesetzt, u.a. die Level 0, 1 und 5.
NB	Die Datensicherungen basieren auf dem RAID-Level 5.
SWB	Für die zeitgleiche Datensicherung werden die Server nach dem RAID-Konzept gespiegelt, wobei das RAID-Level 5 verwendet wird.

Räumliche Trennung der Server	
IDS	Die Spiegelserver befinden sich an einem anderen, ca. fünf Kilometer entfernten Standort.
NB	Die eingesetzten Server sind räumlich nicht getrennt.
SWB	Die Server sind auf zwei Stockwerke verteilt, die verschiedenen Brandschutz-zonen angehören.

Manuelle oder automatische Datensicherung	
IDS	Die Datensicherung wird kombiniert durchgeführt, das heisst, sie wird sowohl manuell als auch automatisch durchgeführt.
NB	Die Datensicherung erfolgt programmgesteuert, also automatisch.
SWB	Die Datensicherung wird automatisch durchgeführt.

Verantwortlichkeiten	
IDS	Verantwortlich für die Backups an der Universität Zürich ist die Systemgruppe.
NB	Für die Backups verantwortlich, und damit auch zuständig für die Kontrolle auf Erfolg und Misserfolg der Datensicherung, ist übergeordnet das Personal für die Datenserver. Für das Bibliothekssystem übernimmt die Stelle des/der Applika-tionsverantwortlichen die Verantwortung für die Datensicherung.
SWB	Im SWB sind die Systemadministratoren für die Backups verantwortlich.

Prüfung der Backups auf Wiederherstellbarkeit	
IDS	Regelmässige Test stellen die Wiederherstellbarkeit der Backups sicher. Die Datensicherung wird *„nach jeder Verfahrensänderung sowie mindestens alle drei Monate geprüft.“* (Universität Zürich, Informatikdienste, 2006, S.1)
NB	Die Datensicherungen werden in unregelmässigen Abständen mittels Restore (Zurückspielen) auf ihre Wiederherstellbarkeit geprüft.
SWB	Die Systembackups werden wöchentlich auf einen separaten Rechner eingespielt und auf einer Schulungsdatenbank getestet.

Sicherungssoftware	
IDS	Die Datensicherung wird durch den Einsatz der Sicherungssoftware Tivoli Storage Manager (IBM) unterstützt.
NB	Zur Unterstützung der Datensicherung wird im Bundesamt für Informatik und Telekommunikation eine spezielle Sicherungssoftware eingesetzt. Das Bibliothekssystem wird vorläufig noch ohne Spezialsoftware betrieben (bis Ende des Jahres 2007).
SWB	Für die Datensicherung wird die Sicherungssoftware Sun Networker verwendet.

Arten der eingesetzten Speichermedien	
IDS	Die Daten der Universität Zürich werden auf verschiedenen Speichermedien gesichert. Eingesetzt werden Spiegelserver, Festplatten, Wechselplatten und Bänder. Disketten, DVDs, CD-ROMs bzw. WORM werden nur in seltenen Fällen für die Datensicherung genutzt.
NB	Für die Datensicherung der Benutzer- und Bestandsdaten der Schweizerischen Nationalbibliothek werden Tapes/Bänder verwendet.
SWB	Auch der SWB nutzt Bänder als Speichermedium für die Datensicherung.

Aufbewahrungsort der Backups und Dauer der Aufbewahrung	
IDS	Die synchronen und asynchronen Spiegelungen werden an einem anderen Standort aufbewahrt und die Bänder werden in feuerfesten, gesicherten Bunkern/ Tresoren verwahrt.
NB	Die Backup-Tapes werden in einem feuer- und wasserfesten Tresor in einem separaten Raum aufbewahrt, wobei die vollständige Sicherung ca. ein Jahr und die inkrementellen Sicherungen weniger lang aufgehoben werden.
SWB	Die Sicherungsbänder werden in einem separaten, ca. fünf Kilometer entfernten Gebäude aufbewahrt. Die Aufbewahrungsdauer beträgt ein Jahr.

4.4 Firewall

Verwendete Soft-/Hardware	
IDS	Zu der in der Universität Zürich eingesetzten Firewall- Soft- und Hardware liegen auf Grund der Vertraulichkeit keine Informationen vor.
NB	Als präventive, technische Massnahme für die Datensicherung stellt das Bundesamt für Informatik und Telekommunikation der NB die Firewall-Hardware Nokia IP350 zur Verfügung.
SWB	Im SWB wird zur Sicherung des internen Netzes eine Cisco PIX Firewall-Hardwarekomponente verwendet.

Installation mit Standardeinstellung oder Anpassung an die Sicherheitsziele	
IDS	Die eingesetzte Firewall ist an die Bedürfnisse der Umgebung der Universität Zürich angepasst.
NB	Für den Betrieb der Firewall werden modifizierte Einstellungen vorgenommen.
SWB	Die Freischaltung erfolgt IP-basiert. Die Firewall-Einstellungen sind damit zwar nicht direkt an die Sicherheitsziele und –richtlinien der IT-Sicherheitsleitlinie angepasst, die Firewall bietet aber dennoch Schutz vor Zugriffen von unbekannten Rechnern auf das interne Netz.

Eingesetzte Firewall-Komponenten (siehe Kapitel 2.3.2 und 2.3.3)	
IDS	Paketfilter, Application Gateways und Demilitarisierte Zonen werden in verschiedenen Kombinationen und Ausprägungen eingesetzt.
NB	Details zum Aufbau und zur Kombination der Firewall-Komponenten sind nicht bekannt, allerdings besteht eine demilitarisierte Zone (DMZ). Daraus ist zu schliessen, dass entweder eine zweistufige Firewall-Architektur mit einem Paketfilter und einem dual-homed Application Gateway mit zwei Netzwerkkarten oder sogar eine dreistufige Firewall-Architektur mit einem single-homed Application Gateway mit einer Netzwerkkarte und zwei Paketfiltern besteht.
SWB	Für die Sicherung des internen Netzes werden im SWB ebenfalls Paketfilter und Application Gateways sinnvoll miteinander kombiniert, so dass eine oder mehrere demilitarisierte Zonen (DMZ) entstehen.

Rhythmus der Aktualisierung der Firewall-Software	
IDS	Der Rhythmus, in welchem die Firewall-Software aktualisiert wird, ist nicht bekannt.
NB	Der Rhythmus, in welchem die Firewall-Software aktualisiert wird, ist nicht bekannt.
SWB	Die eingesetzte Firewall-Software wird über den Support-Vertrag dauernd aktualisiert.

4.5 Risikoanalyse

Auf Grund der Vertraulichkeit der Daten liegen vom IDS Universität Zürich keine Informationen bezüglich der Sicherheitsmassnahme „Risikoanalyse“ vor.

Regelmässige Durchführung von Risikoanalysen	
NB	Zuständig für die regelmässige Durchführung von Risikoanalysen zur Erkennung möglicher Gefahren der Datensicherung ist das Bundesamt für Informatik und Telekommunikation. Der Rhythmus ist nicht bekannt.

SWB	Risikoanalysen werden nach BSI Standard 100-2 „IT-Grundschutz Vorgehensweise“[10] und BSI Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“[11] regelmässig durchgeführt. Der Rhythmus ist nicht bekannt.

Bekannte Risiken in der Datensicherung	
NB	Möglich wäre der Verlust einer Tagesproduktion von Daten, da die Datensicherungen nur nachts durchgeführt werden.
SWB	Die Datensicherung der Benutzer- und Bestandsdaten des SWB unterliegt folgenden bekannten Risiken: • Technische Probleme (insbesondere Stromausfall) • Zerstörung durch Brand, Wassereinbruch etc. • Menschliches Versagen

Massnahmen zur Vermeidung dieser Risiken	
NB	Nach einer Kosten-Nutzen-Analyse wird das Risiko des Verlustes einer Tagesproduktion in Kauf genommen, weswegen vorderhand keine Massnahme zur Vermeidung festgelegt ist.
SWB	Um Zerstörung und menschliches Versagen in der Datensicherung zu verhindern, werden Brandmelder, Leitwarte und Zugangsbeschränkungen eingesetzt. Durch den Betrieb eines Diesel-Aggregators wird eine unterbrechungsfreie Stromversorgung (USV) erreicht, so dass kein Datenverlust infolge eines Stromausfalls entstehen kann.

[10] Der BSI Standard 100-2 „IT-Grundschutz Vorgehensweise“ ist online verfügbar unter: http://www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf [29.08.2007].

[11] Der BSI Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ ist online verfügbar unter: http://www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf [29.08.2007].

Massnahmen bei Eintritt der bekannten Gefahr	
NB	Tritt der genannte Störfall dennoch ein, so werden die Daten anhand des letzten verfügbaren Backups wiederhergestellt.
SWB	Im Fall eines Datenverlust oder einer Datenbeschädigung werden die Daten durch ein Recovery (Zurückspielen) der Sicherheitskopien wiederhergestellt.

Zusätzliche Bemerkung zur Risikoanalyse
Der Südwestdeutsche Bibliotheksverbund SWB plant derzeit den Aufbau eines vollständigen Backups mit Rechner, Anwendung und den aktuellen Daten an einem anderen Standort.

4.6 Katastrophenplan / Notfallplan

Existenz eines Katastrophen- oder Notfallplans	
IDS	Die Universität Zürich verfügt über einen Katastrophen- oder Notfallplan. Die Inhalte sind vertraulich.
NB	Übergeordnet besteht ein Katastrophen- oder Notfallplan, spezifisch für das Bibliothekssystem ist allerdings kein derartiges Dokument vorhanden.
SWB	Der SWB verfügt über eine Dienstvereinbarung, die eine Meldekette, die Rangfolge der Wiederherstellung und die Notfallnummern von Firmen umfasst.

Existenz eines Wiederanlaufplans (Notfall Recovery)	
IDS	Im IDS Universität Zürich existiert ein vertraulich klassifizierter Recovery Plan.
NB	Massnahmen, die Ausweichmöglichkeiten, Systemstartverfahren, Reihenfolge und Prioritäten für den Wiederanlauf nach einem Störfall festlegen, werden zurzeit nicht mehr aktualisiert, da der Betrieb der Bibliotheksumgebung auf Ende des Jahres 2007 an das Bundesamt für Informatik und Telekommunikation übergeht.
SWB	Ein Notfall Recovery Plan besteht momentan nicht, der Wiederanlaufplan befindet sich aber derzeit in Bearbeitung.

Durchführung von Notfallübungen	
IDS	Mögliche Störfälle werden derzeit nicht anhand von Notfallübungen geprobt.
NB	Momentan werden keine Notfallübungen durchgeführt, um den Ernstfall bestimmter Gefahren wie z.B. einen Serverausfall oder einen Betriebsunterbruch zu proben.
SWB	Notfallübungen befinden sich zurzeit in Planung. Der letzte vollständige Test wurde Ende des Jahres 2005 durchgeführt.

Verantwortlichkeiten	
IDS	Im Not- oder Störfall obliegt die Einleitung geeigneter Massnahmen dem Verantwortungsbereich des Chief Information Officers (CIO) und des Chief Security Officers (CSO).
NB	Bei Eintritt eines Notfalls oder Störfalls ist das Überwachungspersonal im Bundesamt für Informatik und Telekommunikation in Zusammenarbeit mit der Applikationsverantwortlichen und dem Leiter Informationstechnologien in der Schweizerischen Nationalbibliothek dafür verantwortlich, geeignete Massnahmen einzuleiten.
SWB	Beim SWB übernehmen das Management und die Systemadministratoren die Verantwortung, im Störfall die entsprechenden Massnahmen einzuleiten.

Existenz eines Alarmierungsplans für Not- und Störfälle	
IDS	In der Universität Zürich besteht ein Alarmierungsplan.
NB	Ein Alarmierungsplan, welcher das Vorgehen in einem Not- oder Störfall regelt, ist in der Schweizerischen Nationalbibliothek vorhanden.
SWB	Der Südwestdeutsche Bibliotheksverbund verfügt ebenfalls über einen Alarmierungsplan für Not- und Störfälle.

Regelmässige Überprüfung der Funktionsfähigkeit des Notfallplans	
IDS	Der Katastrophen- bzw. Notfallplan der Universität Zürich wird regelmässig auf seine Funktionsfähigkeit getestet.

NB	Der Notfallplan bzw. Wiederanlaufplan wird zurzeit nicht mehr auf seine Funktionsfähigkeit geprüft, da der Betrieb der Bibliotheksumgebung Ende des Jahres 2007 an das Bundesamt für Informatik und Telekommunikation übergeht.
SWB	Der Notfallplan wird regelmässig nach der Vorgehensweise des IT-Grundschutz (BSI, 2005b) überprüft, um eine effiziente und effektive Funktionsweise im Störfall zu gewährleisten.

Dokumentation von Notfällen	
IDS	Not- oder Störfälle, die aufgetreten sind, werden ausführlich dokumentiert.
NB	Eingetretene Notfälle werden in der NB momentan nicht ausführlich dokumentiert.
SWB	Notfälle werden derzeit nicht dokumentiert, sollen zukünftig aber nach den Vorgaben des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik ausführlich dokumentiert werden. Die konkreten Regeln sind zurzeit nicht bekannt.

5 Zusammenfassung der Erkenntnisse

Nach der Auswertung der Fragebögen sollen nun die wichtigsten, aus der Analyse gewonnenen Einsichten zusammenfassend dargestellt werden, um aufzuzeigen, welche präventiven und reaktiven Massnahmen für die Datensicherung in den untersuchten Bibliotheksinstitutionen vorgenommen werden.
Der Aufbau des Kapitels orientiert sich an den Themenbereichen des Fragebogens, wobei auf eine Wiederholung der einzelnen Fragestellungen verzichtet wird, da diese im vorhergehenden Kapitel genannt wurden.

Grundlegendes

Mit den wenigen grundlegenden Fragen sollte eruiert werden, ob die Sicherheit des Betriebs, der verwendeten Systeme und der verarbeiteten und gespeicherten Daten überhaupt ein Thema in den einzelnen Institutionen ist und welcher Stellenwert ihr zugeschrieben wird. Falls der Sicherheit nur wenig Bedeutung beigemessen würde, so dürfte davon ausgegangen werden, dass auch nur dementsprechend wenig unternommen wird, um die Sicherheit der Daten zu garantieren.

Die Auswertung hat allerdings ganz klar gezeigt, dass die Sicherheit ein äusserst wichtiger Faktor im Betrieb der beiden Bibliotheksverbünde und der Schweizerischen Nationalbibliothek ist. So wird die Bedeutung der Sicherheit in allen Institutionen in einem das Unternehmen betreffenden Dokument wie dem Informatikleitbild (NB), der Informatikstrategie (IDS Universität Zürich) oder der IT-Sicherheitsleitlinie (SWB) schriftlich festgehalten.

Neben der Erkenntnis der Wichtigkeit von Sicherheit verfügen die analysierten Institutionen über spezifische Dokumente, die den Umgang mit Daten und die Datensicherung regeln. Allerdings wird die Datensicherung derzeit von keiner Institution in einem eigenen Sicherheitskonzept oder Datensicherungskonzept geregelt, sondern jeweils in mehreren Dokumenten, die entsprechende Richtlinien vorgeben. Für die Datensicherung der Benutzer- und Bestandsdaten, die vom Südwestdeutschen Bibliotheksverbund SWB verwaltet werden, wird zurzeit ein offizielles Dokument erarbeitet, welches sich nach den Empfehlungen der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) richtet. Somit kann festgehalten werden, dass die untersuchten Institutionen bezüglich der Datensicherung und Sicherheit der Daten sensibilisiert sind. Durch Bekanntmachung der sicherheitsspezifischen Dokumente wird versucht, Sicherheit zu gewährleisten, da alle Personen, die dem Geltungsbereich der Dokumente angehören, zu einer sicherheitsorientierten Handlungs- und Arbeitsweise aufgefordert werden.

Sicherheitskonzept

Für die Entwicklung von Richtlinien zum Vorgehen der Datensicherung müssen Gesetze und Vorschriften miteinbezogen werden und es muss abgeklärt werden, ob auch Normen oder Standards die Datensicherung in der jeweiligen Institution tangieren. Zu den Gesetzen und Vorschriften gehören sowohl nationale Regelungen als auch regionale, z.B. kantonale Gesetze und Verordnungen. Ebenso müssen Richtlinien beachtet werden, die von einer übergeordneten Organisation erlassen werden. Wenn sicherheitsspezifische Dokumente von Gesetzen, Verordnungen und anderen Richtlinien beeinflusst werden, so sollten diese zur Absicherung und Verdeutlichung im betreffenden Dokument schriftlich erwähnt werden.

Die Bedeutung der Sicherheit und der Datensicherung wurde bereits angesprochen, in den sicherheitsrelevanten Dokumenten der betrachteten Institutionen finden diese beiden Aspekte allerdings keine besondere Erwähnung. Der hohe Stellenwert spiegelt sich mehr in der Existenz der einzelnen Dokumente und in den konkreten Vorschriften zur Gewährleistung der Sicherheit. Anders verhält es sich mit den in Kapitel 3.1 erläuterten Sicherheitskriterien, die in den Dokumenten aller Institutionen mindestens schriftlich festgehalten und teilweise näher ausgeführt werden. Zu den erwähnten Sicherheitskriterien zählen die Vertraulichkeit, Integrität, Verfügbarkeit, Datensicherheit und der Zugangsschutz.

Damit diese Kriterien, die angestrebte Sicherheit und die Vorschriften zur Datensicherung aber nicht nur Theorie bleiben, sondern ordnungsgemäss umgesetzt werden, erklärt sich das Management der untersuchten Institutionen bereit, die für die Umsetzung erforderlichen Mittel und Ressourcen zur Verfügung zu stellen.

In den sicherheitsspezifischen Dokumenten der Institutionen wird weniger Wert auf die Darstellung von Zielen zur Datensicherung gelegt, als auf die Dokumentation von Vorgaben bzw. Vorschriften zur Datensicherung. Diese sind hingegen sehr konkret formuliert.

Die unterschiedlichen Rollen, deren Aufgaben und die Verantwortlichkeiten in Bezug auf die Datensicherung werden in der IT-Sicherheitsleitlinie des SWB und im Leitbild der Schweizerischen Nationalbibliothek sowie im „Reglement über den Einsatz von Informatikmitteln an der Universität Zürich“ ausführlich dargestellt. Auf diese Weise ist für alle dem Gültigkeitsbereich der Sicherheitsdokumente Angehörigen klar ersichtlich, welche Stelle wofür verantwortlich ist. Auf die Schulung und Sensibilisierung der Beteiligten wird ebenfalls in allen drei Institutionen grosser Wert gelegt.

Da sich die Informationstechnologien in einem steten Wandel befinden, ist man sich an den untersuchten Institutionen durchaus bewusst, dass auch die Dokumente mit den Richtlinien

und Massnahmen zur Datensicherung kontinuierlich aktualisiert und verbessert werden müssen. Gleichzeitig enthalten die Dokumente eine Verpflichtung des Managements und der Mitarbeitenden zur Einhaltung der Vorschriften, da die Datensicherung schlussendlich nur so gut sein kann, wie die Umsetzung der entsprechenden Vorgaben durch das Personal aller Ebenen. Um den Zugangsschutz zu den Systemen und Daten abzusichern, werden in der Schweizerischen Nationalbibliothek und dem IDS Universität Zürich Regeln zum Aufbau und Wechsel von Passwörtern erlassen. Für die Gestaltung der Passwörter des Bibliotheks-service-Zentrums Baden-Württemberg sind zukünftig Richtlinien geplant. Für die Passwörter der an den Bibliotheksverbünden teilnehmenden Bibliotheken sind Regelungen zum Aufbau und Wechsel hingegen nur schwer realisierbar.

Datensicherung / Backup-Management

Mit einigen Fragen zur Vorgehensweise in der Datensicherung wurde untersucht, welche Methoden in den einzelnen Institutionen angewendet, welche Arten von Speichermedien eingesetzt und wo und wie lange die Backups aufbewahrt werden, um in einem Notfall beschädigte oder gar verloren gegangene Datenbestände wiederherzustellen.

Die Auswertung hat gezeigt, dass alle drei Bibliotheksorganisationen verschiedene Datensicherungsarten in einem Mix sinnvoll kombinieren und die Daten durch komplette, inkrementelle, differenzielle und teilweise selektive Sicherungen redundant halten. Ergänzend zu den zeitnahen und zeitversetzten Datensicherungsstrategien werden die Daten auch in Echtzeit gespiegelt, um bei technischen Problemen den Betrieb aufrechterhalten zu können. Die Daten werden nach dem Redundant-Array-of-Independent-Disks-Prinzip (RAID) gesichert, wobei die Schweizerische Nationalbibliothek und der Südwestdeutsche Bibliotheksverbund das Level RAID-5 verwenden. Der Informationsverbund Deutschschweiz Universität Zürich sichert nach RAID-0, RAID-1 und RAID-5. Eine weitere kleine Differenz zeigt sich in der Form der Datensicherung, da die Datensicherung bei der NB und dem SWB automatisch, also programmgesteuert erfolgt und der IDS Universität Zürich eine Kombination aus automatischer und manueller Datensicherung durchführt. Verantwortlich für die Kontrolle der Datensicherung auf deren Erfolg oder auch Misserfolg sind in allen Institutionen die Systemadministratoren. Um die Backups auf ihre Wiederherstellbarkeit zu prüfen, werden regelmässig Tests durchgeführt. Die Angaben zur Häufigkeit dieser Prüfungen variiert zwischen „wöchentlich“ (SWB) und „mindestens alle drei Monate“ (IDS Universität Zürich).

Zur Unterstützung der Datensicherung setzen alle drei analysierten Institutionen eine Sicherungssoftware bekannter Unternehmen wie IBM oder Sun Microsystems ein.

Für die Sicherungskopien der Daten werden unterschiedliche Speichermedien genutzt, hauptsächlich aber Bänder. Die Universität Zürich sichert ihre Daten zusätzlich auch auf Festplatten, Wechselplatten und in seltenen Fällen auf Disketten, DVDs und CD-ROMs. Die Bänder mit den gesicherten Datenbeständen werden im IDS Universität Zürich und in der NB in einem feuer- und wasserfesten Tresor, im SWB sogar an einem anderen, ca. fünf Kilometer entfernten Gebäude für ein Jahr aufbewahrt. Die Spiegelserver des IDS befinden sich ebenfalls an einem separaten, gut fünf Kilometer entfernten Standort. Die Server im SWB sind auf zwei Stockwerke verteilt, die verschiedenen Brandschutzzonen angehören. Die räumliche Trennung der Server und Speichermedien erhöht die Sicherheit, da die Wahrscheinlichkeit, dass bei einem Störfall, bspw. einem Feuer, sowohl die Originaldatenbestände als auch die Sicherungskopien beschädigt werden, verringert wird.

Firewall

Einige Fragen zu den in den Institutionen eingesetzten Firewall-Systemen geben Aufschluss darüber, mit welchen präventiven technischen Massnahmen das interne Netz vor Angriffen geschützt wird. So wurde festgestellt, dass die Firewalls nicht mit Standardeinstellungen installiert sind, sondern an die jeweiligen Sicherheitsziele angepasst sind, um einen optimalen Schutz zu bieten. Die Firewall-Architekturen basieren in allen drei Institutionen auf der Kombination von Paketfiltern und Application Gateways zur Entwicklung demilitarisierter Zonen, so dass das interne Netz möglichst effektiv vor Zugriffen von unbekannten Rechnern geschützt ist.

Risikoanalyse

Ein wichtiger Aspekt der Datensicherung ist die Risikoanalyse, anhand derer zu einem frühen Zeitpunkt mögliche Gefahren entdeckt und gegebenenfalls sogar bereits entschärft werden können. Aus Gründen der Vertraulichkeit stehen von der Universität Zürich keine Informationen bezüglich Risikoanalysen vor. Die Schweizerische Nationalbibliothek und der Südwestdeutsche Bibliotheksverbund führen regelmässig Gefahrenanalysen durch, die zum Ergebnis führen, dass für die Datenbestände Risiken durch technische Probleme, Zerstörung durch Brände oder Wassereinbrüche und durch menschliches Versagen entstehen können. Die NB stellt fest, dass auf Grund der nachts durchgeführten Datensicherungen die Möglichkeit des Verlustes einer Tagesproduktion von Daten besteht. Basierend auf einer Kosten-Nutzen-Analyse wird dieses Risiko von der NB in Kauf genommen. Um die weiteren bekannten Gefahren zu vermeiden, werden in der NB und im SWB Brandmelder, USV und Zugangsbeschränkungen eingesetzt. Falls einer dieser Störfälle trotz aller Prävention dennoch

eintritt, werden die beschädigten oder verloren gegangenen Daten anhand der ausgelagerten Backups wiedehergestellt (Recovery).

Zusätzlich zu den bereits bestehenden Datensicherungsmassnahmen plant der SWB derzeit den Aufbau eines vollständigen Backups mit Rechner, Anwendung und den aktuellen Daten an einem separaten Standort.

Katastrophenplan / Notfallplan

Um die Untersuchung der Vorgehensweise zur Datensicherung in der Schweizerischen Nationalbibliothek, dem IDS Universität Zürich und dem Südwestdeutschen Bibliotheksverbund abzuschliessen, geben einige Fragen Auskunft zu den Bestimmungen bezüglich der Reaktion in Notfällen.

Die Auswertung hat ergeben, dass alle Institutionen über einen Katastrophen- oder Notfallplan verfügen, welcher das Vorgehen in einem Störfall regelt. Ein Notfall Recovery oder Wiederanlaufplan, der Ausweichmöglichkeiten, Systemstartverfahren, Reihenfolge und Prioritäten für den Wiederanlauf nach einem Störfall festlegt, ist in der Universität Zürich vorhanden. In der NB werden diese Massnahmen nicht mehr aktualisiert, da der Betrieb der Bibliotheksumgebung Ende des Jahres 2007 an das Bundesamt für Informatik und Telekommunikation übergeht. Im SWB existiert momentan noch kein Wiederanlaufplan, dieser befindet sich aber bereits in Bearbeitung.

Von Zeit zu Zeit sollten Notfallübungen durchgeführt werden, um den Ernstfall bestimmter Gefahren, wie bspw. einen Stromunterbruch, und die angemessene Reaktion darauf zu proben. Zum Zeitpunkt der Analyse finden in keiner der drei Institutionen Notfallübungen statt, im SWB befinden sich diese in Planung. Der letzte vollständige Test wurde im SWB Ende des Jahres 2005 durchgeführt.

Die Regelung, welche Stelle im Not- oder Störfall dafür zuständig ist, geeignete Massnahmen und Schritte einzuleiten, wird unterschiedlich gehandhabt. An der Universität Zürich übernehmen der CIO und der CSO diese Verantwortung, im SWB das Management und die Systemadministratoren und für die Schweizerische Nationalbibliothek zeichnet das Überwachungspersonal des Bundesamtes für Informatik und Telekommunikation in Zusammenarbeit mit der Applikationsverantwortlichen und dem Leiter Informationstechnologien der NB verantwortlich für die weiteren Schritte im Notfall. Überdies verfügen alle untersuchten Institutionen über einen Alarmierungsplan, der das Vorgehen im Not- oder Störfall regelt.

Damit die vorgegebenen Aktionen und Massnahmen stets aktuell sind, werden die Notfallpläne des IDS Universität Zürich und des Südwestdeutschen Bibliotheksverbunds regelmässig

auf ihre Funktionsfähigkeit überprüft. Der Notfallplan der Schweizerischen Nationalbibliothek wird zurzeit nicht mehr auf seine Funktionsfähigkeit geprüft, da der Betrieb der Bibliotheksumgebung Ende des Jahres 2007 an das Bundesamt für Informatik und Telekommunikation übergeht.

Ein letzter Aspekt im Katastrophen- und Notfall-Management betrifft die Dokumentation der eingetretenen Störfälle. Zum Zeitpunkt der Untersuchung werden Notfälle nur im IDS Universität Zürich ausführlich dokumentiert. Störfälle werden in der NB und im SWB derzeit nicht dokumentiert, allerdings plant der SWB zukünftig eine Dokumentation nach den Vorgaben des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik.

Zusammenfassend wird festgehalten, dass die Sicherheit der Netze, Systeme und Daten sowie die Datensicherung an sich in allen drei Institutionen einen hohen Stellenwert einnehmen. Den jeweiligen Möglichkeiten entsprechend werden sowohl präventive als auch reaktive Massnahmen zur Gewährleistung der Sicherheit und der Datensicherung geplant, umgesetzt und kontinuierlich verbessert.

6 Empfehlungen für die Datensicherung in Bibliotheksverbünden

Sowohl die theoretischen Darstellungen als auch die Analyse der praktisch umgesetzten Sicherheitsvorkehrungen in den drei Bibliotheksverbundorganisationen haben auf eindrückliche Art und Weise verdeutlicht, wie wichtig die Sicherheit und die Datensicherung im Betrieb ist und wie vielseitig und komplex die Möglichkeiten dazu sind. Auf der Grundlage dieser Betrachtungen werden im Folgenden Empfehlungen für eine möglichst optimale Datensicherung in Bibliotheksverbünden zusammengestellt. Die Empfehlungen erheben keinen Anspruch auf Vollständigkeit, sollen aber dazu dienen, bereits vorhandene sicherheitsspezifische Dokumente und Richtlinien zu überprüfen und Hilfestellungen für die Entwicklung neuer Sicherheitskonzepte oder Massnahmen für die Datensicherung zu geben. Da die verschiedenen Aspekte der Datensicherung zwar eng miteinander verknüpft sind, aber dennoch einzeln betrachtet werden können, werden die Empfehlungen modulartig aufgebaut. Dies ermöglicht den Verantwortlichen einer Institution die bedarfsgerechte Unterstützung für die Auseinandersetzung mit den eigenen Sicherheits- und Datensicherungsbestimmungen. Die Empfehlungen gliedern sich in die Bereiche Grundlegende Massnahmen, Risikoanalyse, Datensicherung, Firewall und Katastrophen-/Notfall-Management, wobei unter den grundlegenden Massnahmen vorbereitende Überlegungen zum bestehenden und zukünftig gewünschten Sicherheits-Management verstanden werden. Der Bereich „Datensicherung“ enthält inhaltliche und formale Empfehlungen zum Aufbau eines Sicherheitskonzeptes und/oder eines Datensicherungskonzeptes.

Es wird versucht, eine logische chronologische Abfolge der Empfehlungen zur Vorgehensweise zu erreichen, allerdings müssen die einzelnen Schritte und deren Reihenfolge an die Bedürfnisse jeder Institution angepasst werden, welche sich mit den eigenen Sicherheitsmassnahmen befasst.

Zur Gewährleistung einer übersichtlichen Darstellung werden die Empfehlungen nicht in vollständigen Sätzen, sondern handlungsorientiert in Stichworten formuliert.

Bereich	Empfehlungen zur Vorgehensweise	Verantwortlichkeiten
Grundlegende Massnahmen	• Bewusstsein für Sicherheit und Datensicherung bilden • Initiierung eines an die Institution angepassten Sicherheits-Prozesses • Entwicklung von Sicherheitszielen (SOLL-Zustand) • Erarbeitung einer Sicherheitspolitik, mit Unternehmensstrukturen, Richtlinien und Vorgaben zur Erreichung der Sicherheitsziele • Festhalten der Bedeutung der „Sicherheit“ in einem unternehmensspezifischen Dokument (Strategie, Leitbild, Vision, Mission o.ä.)	Unternehmensleitung/ Management
Risikoanalyse	• Analyse und Dokumentation aller schutzbedürftigen Unternehmenswerte, Prozesse und Daten (Liste/n) • Regelmässige Durchführung von Risikoanalysen zur Erkennung möglicher Gefahren der Datensicherung • Erarbeitung von Massnahmen zur Vermeidung der erkannten möglichen Gefahren (Liste) • Erarbeitung von reaktiven Massnahmen für den Fall eines Eintritts der erkannten möglichen Gefahren (Liste) • Regelmässige Überprüfung der Liste der schutzbedürftigen Werte, Prozesse, Daten und Massnahmen auf ihre Aktualität und Vollständigkeit	Unternehmensleitung/ Management, in Zusammenarbeit mit dem internen Sicherheitsbeauftragten oder Sicherheitsteam

Bereich	Empfehlungen zur Vorgehensweise	Verantwortlichkeiten
Datensicherung	Erstellung eines Sicherheitskonzepts mit folgenden Inhalten: • Abgrenzung des Gültigkeitsbereichs • Definition der Verantwortlichkeiten und Kompetenzen • Begriffe und Definitionen • Liste der der schutzbedürftigen Werte, sicherheitskritischen Prozesse und der Sicherheitsziele • Liste der Subjekte (Personal) • Liste der Bedrohungen (auf Grund der Risikoanalyse) • Liste der Massnahmen • (Integriertes Datensicherungskonzept) • Definition der Verantwortlichkeiten und Konsequenzen bei Nichteinhalten des Sicherheitskonzepts • Regelungen und Massnahmen zur Kontrolle und Überprüfung des Sicherheitskonzepts • Verpflichtung des Managements und des Personals zur Einhaltung des Sicherheitskonzepts	Erstellung und Überprüfung der Dokumente: Unternehmensleitung / Management, in Zusammenarbeit mit dem internen Sicherheitsbeauftragten oder Sicherheitsteam Umsetzung: Unternehmensleitung / Management, alle betroffenen Mitarbeitenden

Bereich	Empfehlungen zur Vorgehensweise	Verantwortlich-keiten
Datensicherung	Konkrete Empfehlungen für einzelne Aspekte der Datensicherung • Art der Datensicherung: Kombination aus vollständigen und inkrementellen Sicherungsverfahren, sowie zusätzlich Datensicherung nach dem RAID-Level 5 • Räumliche Trennung der Server mit dem Original-Datenbestand und dem Spiegelserver in verschiedene Brandschutzzonen oder an unterschiedlichen Standorten • Verantwortlichkeiten für die Datensicherung: Systemadministatoren • Regelmässige Überprüfung der Backups auf ihre Wiederherstellbarkeit, z.B. wöchentlich, monatlich oder alle drei Monate, mindestens aber nach jeder Änderung der Datensicherungsverfahren • Verwendete Speichermedien: Bänder, Spiegelserver, Festplatten[12] • Archivierung der Sicherungsdaten: Wahl eines separaten Standortes für Spiegelserver, Aufbewahrung der Sicherungsbänder in einem feuer- und wasserfesten Tresor	
Firewall	• Anpassung der Firewall-Einstellungen an die von der Unternehmensleitung definierten Sicherheitsziele • Kombination von Paketfiltern und Application Gateways (single-homed, dual-homed) zur Erreichung einer Demilitarisierten Zone (DMZ) zur Sicherung des internen Netzes • Regelmässige Aktualisierung der Firewall-Software (z.B. über einen Support-Vertrag)	Informatik-verantwortliche/r bzw. Informatik-abteilung der Institution

[12] Disketten, DVDs und CD-ROMs eignen sich auf Grund der begrenzten Kapazität weniger für die Sicherung von Daten in Bibliotheksverbundorganisationen.

Bereich	Empfehlungen zur Vorgehensweise	Verantwortlichkeiten
Katastrophen- / Notfall-Management	• Erstellung eines Katastrophen- / Notfallplans; mit Richtlinien zum Vorgehen im Störfall • Erstellung eines Alarmierungsplans • Erstellung eines Wiederanlaufplans; mit Hinweisen zu Ausweichmöglichkeiten, Systemstartverfahren, Reihenfolge und Prioritäten für den Wiederanlauf nach einem Störfall • Definition der Verantwortlichkeiten für die Einleitung geeigneter Massnahmen im Störfall → Möglichkeiten: CIO, CSO, Management oder Systemadministratoren • Erstellung eines Rekonstruktionsplans mit folgenden Inhalten - Speicherort von Programmen und Daten im Normalbetrieb - Bestand der gesicherten Daten (Bestandsverzeichnis) - Zeitpunkte der Datensicherung - Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten • Aufbewahrungsort der gesicherten Programme und Daten und ggf. erforderliche Zutrittsmittel • Regelmässige Durchführung von Notfallübungen → Konkrete Empfehlung: Übungen zu Bränden, Serverausfällen, Stromunterbrüchen, Datenverlust oder –beschädigung durch Fehler in der Datensicherung • Regelmässige Überprüfung der Funktionsfähigkeit des Notfallplans und des Wiederanlaufplans • Regelmässige Überprüfung des Alarmierungsplans auf seine Aktualität (Stellen, Namen, Telefonnummern etc.) • Detaillierte Dokumentation aller eingetretenen Störfälle zur ausführlichen Analyse	Erstellung und Überprüfung der Dokumente: Unternehmensleitung/ Management, in Zusammenarbeit mit dem internen Sicherheitsbeauftragten oder Sicherheitsteam Umsetzung: Unternehmensleitung/ Management, alle betroffenen Mitarbeitenden

7 Fazit und Ausblick

Die im Rahmen der vorliegenden Ausarbeitung gewonnen Erkenntnisse bezüglich der bereits umgesetzten Massnahmen zur Datensicherung in Bibliotheksorganisationen machen deutlich, wie wichtig die Gewährleistung der Sicherheit von Benutzer- und Bestandsdaten in Bibliotheken und Bibliotheksverbünden ist. Ebenso deutlich konnte gezeigt werden, dass sich die untersuchten Bibliotheksinstitutionen dem Aspekt der Sicherheit überaus bewusst sind, dass sie sich ausführlich damit beschäftigen und dass vielfältige Vorkehrungen getroffen werden, um die Vertraulichkeit, die Verfügbarkeit und die Integrität der verarbeiteten und gespeicherten Daten zu garantieren. Neben der Entwicklung von Richtlinien zur Datensicherung werden Risikoanalysen zur Erkennung möglicher Gefahren durchgeführt, präventiv wird mit dem Einsatz von technischen Massnahmen wie Firewalls das institutionsinterne Netz vor Angriffen geschützt. Tritt dennoch ein Störfall ein, kann auf Grund der frühzeitig erarbeiteten Katastrophen- und Notfallpläne angemessen reagiert werden. Und trotzdem bleibt es dabei, um es noch einmal mit Edmund Burke zu sagen:

„Rechtzeitige und vorsorgliche Angst ist die Mutter der Sicherheit."

Die Sicherheitsverantwortlichen aller Datenverarbeitungsinstitutionen sind in einem Umfeld sich stetig verändernder Strukturen, Technologien, Gesetze und Anforderungen des Kundenkreises gezwungen, die angewandten Strategien und Massnahmen der Datensicherung an die sich ändernden Gegebenheiten anzupassen.

Durch die vorliegende Analyse wurde versucht, einen Einblick in die Thematik der Datensicherheit und der Datensicherung zu geben und auf der Basis spezifischer Fachliteratur, ergänzt durch eine kleine praktische Untersuchung, Empfehlungen für das Vorgehen bezüglich der Datensicherung in Bibliotheksverbünden zu geben. Auch wenn die empfohlenen Massnahmen in keiner Weise abschliessend sind, so sollen sie der Unterstützung von Institutionen dienen, die ihr Sicherheits-Management neu konzipieren oder die bestehenden Regelungen zur Datensicherung überprüfen möchten.

Der Aspekt des Datenschutzes wurde in der vorliegenden Arbeit ausgeklammert und nur für die Abgrenzung berücksichtigt, allerdings dürfte das Zusammenspiel von Sicherheit, Datensicherung und Datenschutz in Zukunft an Bedeutung zunehmen, da Bibliotheksverbünde nicht nur bibliographische Daten sondern auch Personendaten ihrer Kunden und Kundinnen verwalten und speichern. Auf Grund der Tatsache, dass die Datenbestände der Benutzer- und Bestandsdaten in Bibliotheksverbünden weiter wachsen werden, wird sich zeigen, ob die Sicherheit der Daten gewährleistet werden kann.

8 Literaturangaben

AEBI, D. (2004): *Praxishandbuch sicherer IT-Betrieb – Risiken erkennen, Schwachstellen beseitigen, IT-Infrastruktur schützen.* Wiesbaden: Gabler.

AMUNDIS COMMUNICATIONS GmbH (2007): *2ask – Die erste Adresse für Ihre Online-Umfragen.* Konstanz. URL: http://www.2ask.ch/ [03.08.2007].

ATTESLANDER, P. (2003): *Methoden der empirischen Sozialforschung.* 10., neu bearb. u. erw. Aufl., Berlin: Walter de Gruyter.

BAERISWYL, B. & RUDIN, B. (2002): *Datenschutz – wie weiter?.*
In: BAERISWYL, B. & RUDIN, B. (Hrsg.) (2002): *Perspektive Datenschutz – Praxis und Entwicklungen in Recht und Technik.* Zürich: Schulthess Juristische Medien AG.

BAUER, M. (1995): *Bibliothek 2000 – Das Online-Buch.* Focus Magazin, 09. Januar.

BACHMANN, P. (2005): *Informatikstrategie.* Version 1.0. Universität Zürich, Informatikdienste. URL: http://www.id.uzh.ch/publikationen/kontakt/InformatikstrategieV1.0.pdf [29.08.2007].

BC INDUSTRIESERVICE (2007): *Raid-4 Datenrettung.* BC Industrieservice: Celic, B. & Fuchs, T. E. GbR, Brigachtal. URL: http://www.rettet-die-daten.de/datenrettung/raid/raid4.html [09.08.2007].

BSI (2005a): *Grundwerte der IT-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn. URL: http://www.bsi.bund.de/gshb/deutsch/baust/04.htm [09.08.2007].

BSI (2005b): BSI Standard 100-2: IT-Grundschutz Vorgehensweise. Version 1.0. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn.
URL: http://www.bsi.de/literat/bsi_standard/standard_1002.pdf [29.08.2007].

BSI (2006): *IT-Grundschutz-Kataloge: Stand 2006.* Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn. URL: http://www.bsi.de/gshb/deutsch/download/itgrundschutz-kataloge_2006_de.pdf [16.08.2007].

BSI (2007a): *IT-Grundschutz-Kataloge – B 1.4 Datensicherungskonzept.* Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn.
URL: http://www.bsi.bund.de/gshb/deutsch/baust/b01004.htm [27.08.2007].

BSI (2007b): *GSTOOL – Das BSI Tool zum IT-Grundschutz.* Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn. URL: http://www.bsi.de/gstool/index.htm [28.08.2007].

BSZ (2007a): *Willkommen beim Bibliotheksservice-Zentrum Baden-Württemberg (BSZ).* Bibliotheksservice-Zentrum Baden-Württemberg (BSZ), Universität Konstanz.
URL: http://www2.bsz-bw.de/cms/ [23.08.2007].

BSZ (2007b): *Über den SWB Online-Katalog.* Bibliotheksservice-Zentrum Baden-Württemberg (BSZ), Universität Konstanz. URL: http://swb.bszbw.de/DB=2.1/START_ABOUT [23.08.2007].

BSZ (2007c): *SWB-Verbundsystem.* Bibliotheksservice-Zentrum Baden-Württemberg (BSZ), Universität Konstanz. URL: http://titan.bsz-bw.de/cms/swb/ [23.08.2007].

BSZ (2007d): *Über uns.* Bibliotheksservice-Zentrum Baden-Württemberg (BSZ), Universität Konstanz. URL: http://titan.bsz-bw.de/cms/bsz/ [23.08.2007].

BUNDESBEHÖRDEN DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT (2006a): *Die NB.*
URL: http://www.bak.admin.ch/slb/org/index.html?lang=de [23.08.2007].

BUNDESBEHÖRDEN DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT (2006b): *Die NB – Auftrag.* URL: http://www.bak.admin.ch/slb/org/auftrag/index.html?lang=de [23.08.2007].

BURKE, E.: *Rechtzeitige und vorsorgliche Angst ist die Mutter der Sicherheit.* [Zitat].
URL: http://www.aphorismen.de/display_aphorismen.php?search=1&page=3 [02.08.2007].

DATACOM BUCHVERLAG GmbH (2007): *ITWissen – Das grosse Online-Lexikon für Informationstechnologie: Datenschutz.* Peterskirchen. Inhaltlich verantwortlich: Klaus Lipinski. URL: http://www.itwissen.info/definition/lexikon//__data%20protection%20_datenschutz.html [06.08.2007].

DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH (2005): *Allgemeines zum Datenschutz – Was ist Datenschutz und warum ist er wichtig?*
URL: http://www.datenschutz.ch/einfuehrung_einleitung.php [06.08.2007].

DICKENMANN, H. (Hrsg.) (2005): *IT/Verbund.* Hauptbibliothek Universität Zürich (HBZ).
URL: http://www.hbz.unizh.ch/index.php?option=content&task=view&id=195&Itemid=130 [23.08.2007].

DICKENMANN, H. (Hrsg.) (2007): *Katalog IDS Zürich Universität – Informationsverbund der Universität Zürich.* Hauptbibliothek Universität Zürich (HBZ).
URL: http://www.hbz.unizh.ch/index.php?option=content&task=view&id=272&Itemid=80 [23.08.2007].

DSG – Bundesgesetz über den Datenschutz, vom 19. Juni 1992 (Stand am 12. Dezember 2006). URL: http://www.admin.ch/ch/d/sr/2/235.1.de.pdf [06.08.2007].

EGGEL, D. (2000): *IT-Sicherheit im Wandel der Zeit – Risikomanagement in der Informatiksicherheit.* Der Schweizer Treuhänder, 10/2000.

HACKER, R. (2000): *Bibliothekarisches Grundwissen.* 7., neu bearb. Aufl. München: Saur.

HANSEN, H. R. & NEUMANN, G. (2001): *Wirtaschaftsinformatik I – Grundlagen betrieblicher Informationsverarbeitung.* 8., völlig neubearb. und erw. Aufl. (UTB für Wissenschaft : Uni-Taschenbücher ; 802 : Betriebswirtschaftslehre, Informatik).

HEINRICH, L. J. (2002): *Informationsmanagement – Planung, Überwachung und Steuerung der Informationsinfrastruktur.* 7., vollst. überarb. und erg. Aufl. München.

HOPPE, G. & PRIEß, A. (2003): *Sicherheit von Informationssystemen – Gefahren, Maßnahmen und Management im IT-Bereich.* Herne: Verl. Neue Wirtschafts-Briefe. (NWB-Studienbücher Wirtschaftsinformatik).

ISB (2007): *Informatikrat Bund IRB.* Informatikstrategieorgan Bund ISB.
URL: http://www.isb.admin.ch/org/informatikorganisation/00184/index.html?lang=de [24.08.2007].

ITSEC (1991): ***I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria – ITSEC*. Version 1.2 (28. Juni 1991). Bundesamt für Sicherheit in der Informationstechnik (BSI).
URL: http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf [10.08.2007].

JUNK, K.-P. & MAYER, M. (2003): *Active Datamanagement – Säulen der Informationssicherheit.* Berlin: VDE-Verl.

KERSTEN, H. & KLETT, G. (2005): *Der IT Security Manager – Expertenwissen für jeden IT Security Manager.* Wiesbaden: Vieweg.

KRUTH, W. (2004): *IT-Grundlagenwissen – Kompaktwissen Informationstechnik für Datenschutz- und Security-Management.* 2., erw. und überarb. Aufl. Frechen: Datakontext-Fachverlag

MICROSOFT TECHNET (2006): *Datenschutz mit RAID.* Microsoft Deutschland GmbH, Unterschleissheim.
URL: http://www.microsoft.com/germany/technet/sicherheit/newsletter/raid.mspx [09.08.2007].

MÜHLENBROCK, F. (2003): *IT-Sicherheit. Effektive Richtlinien und Standards im Unternehmens-Netzwerk.* 1. Aufl. Kilchberg: SmartBooks.

MÜLLER, K.-R. (2003): *IT-Sicherheit mit System. Strategie - Vorgehensmodell - Prozessorientierung - Sicherheitspyramide.* 1. Aufl. Wiesbaden: Vieweg.

NATIONALBIBLIOTHEKSGESETZ, NBibG, (1992): *SR: 432.21: Bundesgesetz über die Schweizerische Nationalbibliothek.*
URL: http://www.admin.ch/ch/d/sr/4/432.21.de.pdf [23.08.2007].

NEDRIK (2004): *Die RAID- Bibel V0.42.* Eintrag im RAID Forum.de: Željko Majkić, Göppingen.
URL: http://www.raidforum.de/viewtopic.php?t=81 [09.08.2007].

PLÖTNER, J. & WENDZEL, S. (2005): *Praxisbuch Netzwerk-Sicherheit. [Risikoanalyse, Methoden und Umsetzung ; für UnixLinux und Windows ; VPN, WLAN, Intrusion Detection, Disaster Recovery, Kryptologie].* 1. Aufl., 1. Nachdr. Bonn: Galileo Press.

RASCH, C. (2000): *Auf dem Weg zum Bücherverbund.* TAZ, Die Tageszeitung, 17. April.

SCHALWAT, M. & THOME, H. (1995): *Lesesäle werden zu modernen Informationsbasen.* Computerwoche, 07. April.

SCHMIDT, K. (2006): *Der IT-Security-Manager.* München: Hanser.

SINGHUBER, H.-C. (2000): RAID-Systeme: Kontinuität plus Performance. Monitor: Das Magazin für Informationstechnologie. Ausgabe 6/2000.
URL: http://www.monitor.co.at/index.cfm?storyid=2558 [09.08.2007].

ST.GALLER BIBLIOTHEKSNETZ (2007): *Bibliotheksnetz SGBN.* URL:
http://www.sg.ch/home/kultur/bibliothek_staatsarchiv/kantonsbibliothek/st_galler_bibliothe ksnetz.html [05.08.2007].

UNIVERSITÄT ZÜRICH, UNIVERSITÄTSLEITUNG (2006): *Reglement über den Einsatz von Informatikmitteln an der Universität Zürich.* Vom 27. Oktober 2006. Universität Zürich.
URL: http://www.rd.uzh.ch/rechtssammlung/richtlinien/Informatik_REIM_2006_10_27.pdf [29.08.2007].

UNIVERSITÄT ZÜRICH, INFORMATIKDIENSTE (2006): *Normen für den Betrieb von Systemen an der Universität Zürich.* Vom 27. Oktober 2006. Universität Zürich.
URL: http://www.rd.uzh.ch/rechtssammlung/richtlinien/Informatik_Normen_2006_10_27.pdf [29.08.2007].

WEBER, R. H. & WILLI, A. (2006): *IT-Sicherheit und Recht – Grundlagen eines integrativen Gestaltungskonzepts.* Zürich: Schulthess. (Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich; 33).

Bisher erschienene Schriften

Ergebnisse von Forschungsprojekten erscheinen jeweils in Form von Arbeitsberichten in Reihen.
Sonstige Publikationen erscheinen in Form von alleinstehenden Schriften.

Derzeit gibt es in den Churer Schriften zur Informationswissenschaft folgende Reihen:
Reihe Berufsmarktforschung

Churer Schriften zur Informationswissenschaft – Schrift 1
Herausgegeben von Josef Herget und Sonja Hierl
Reihe Berufsmarktforschung – Arbeitsbericht 1:
Josef Herget
Thomas Seeger
Zum Stand der Berufsmarktforschung in der Informationswissenschaft
in deutschsprachigen Ländern
Chur, 2007 (im Druck)
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 2
Herausgegeben von Josef Herget und Sonja Hierl
Reihe Berufsmarktforschung – Arbeitsbericht 2:
Josef Herget
Norbert Lang
Berufsmarktforschung in Archiv, Bibliothek, Dokumentation
und in der Informationswirtschaft: Methodisches Konzept
Chur, 2007 (im Druck)
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 3
Herausgegeben von Josef Herget und Sonja Hierl
Reihe Berufsmarktforschung – Arbeitsbericht 3:
Josef Herget
Norbert Lang
Gegenwärtige und zukünftige Arbeitsfelder für Informationsspezialisten
in privatwirtschaftlichen Unternehmen und öffentlich-rechtlichen Institutionen
Chur, 2004
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 4
Herausgegeben von Josef Herget und Sonja Hierl
Sonja Hierl
Die Eignung des Einsatzes von Topic Maps für e-Learning
Vorgehensmodell und Konzeption einer e-Learning-Einheit unter Verwendung von Topic Maps
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 5
Herausgegeben von Josef Herget und Sonja Hierl
Nina Braschler
Realisierungsmöglichkeiten einer Zertifizierungsstelle für digitale Zertifikate in der Schweiz
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 6
Herausgegeben von Josef Herget und Sonja Hierl
Reihe Berufsmarktforschung – Arbeitsbericht 4:
Ivo Macek
Urs Naegeli
Postgraduiertenausbildung in der Informationswissenschaft in der Schweiz:
Konzept – Evaluation – Perspektiven
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 7
Herausgegeben von Josef Herget und Sonja Hierl
Caroline Ruosch
Die Fraktale Bibliothek:
Diskussion und Umsetzung des Konzepts in der deutschsprachigen Schweiz.
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 8
Herausgegeben von Josef Herget und Sonja Hierl
Esther Bättig
Information Literacy an Hochschulen
Entwicklungen in den USA, in Deutschland und der Schweiz
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 9
Herausgegeben von Josef Herget und Sonja Hierl
Franziska Höfliger
Konzept zur Schaffung einer Integrationsbibliothek in der Pestalozzi-Bibliothek Zürich
Chur, 2005
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 10
Herausgegeben von Josef Herget und Sonja Hierl
Myriam Kamphues
Geoinformationen der Schweiz im Internet:
Beurteilung von Benutzeroberflächen und Abfrageoptionen für Endnutzer
Chur, 2006
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 11
Herausgegeben von Josef Herget und Sonja Hierl
Luigi Ciullo
Stand von Records Management in der chemisch-pharmazeutischen Branche
Chur, 2006
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 12
Herausgegeben von Josef Herget und Sonja Hierl
Martin Braschler, Josef Herget, Joachim Pfister, Peter Schäuble, Markus Steinbach, Jürg Stuker
Evaluation der Suchfunktion von Schweizer Unternehmens-Websites
Chur, 2006
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 13
Herausgegeben von Josef Herget und Sonja Hierl
Adina Lieske
Bibliotheksspezifische Marketingstrategien zur Gewinnung von Nutzergruppen:
Die Winterthurer Bibliotheken
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 14
Herausgegeben von Josef Herget und Sonja Hierl
Christina Bieber, Josef Herget
Stand der Digitalisierung im Museumsbereich in der Schweiz
Internationale Referenzprojekte und Handlungsempfehlungen
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 15
Herausgegeben von Josef Herget und Sonja Hierl
Sabina Löhrer
Kataloganreicherung in Hochschulbibliotheken
State of the Art Überblick und Aussichten für die Schweiz
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 16
Herausgegeben von Josef Herget und Sonja Hierl
Heidi Stieger
Fachblogs von und für BibliothekarInnen – Nutzen, Tendenzen
Mit Fokus auf den deutschsprachigen Raum
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 17
Herausgegeben von Josef Herget und Sonja Hierl
Nadja Kehl
Aggregation und visuelle Aufbereitung von Unternehmensstrategien
mithilfe von Recherche-Codes
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 18
Herausgegeben von Josef Herget und Sonja Hierl
Rafaela Pichler
Annäherung an die Bildsprache – Ontologien als Hilfsmittel für Bilderschliessung
und Bildrecherche in Kunstbilddatenbanken
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 19
Herausgegeben von Josef Herget und Sonja Hierl
Jürgen Büchel
Identifikation von Marktnischen – Die Eignung verschiedener Informationsquellen
zur Auffindung von Marktnischen
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 20
Herausgegeben von Josef Herget und Sonja Hierl
Andreas Eisenring
Trends im Bereich der Bibliothekssoftware
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 21
Herausgegeben von Josef Herget und Sonja Hierl
Lilian Brändli
Gesucht – gefunden? Optimierung der Informationssuche von Studierenden
in wissenschaftlichen Bibliotheken
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 22
Herausgegeben von Josef Herget und Sonja Hierl
Beatrice Bürgi
Open Access an Schweizer Hochschulen – Ein praxisorientierter Massnahmenkatalog für
Hochschulbibliotheken zur Planung und Errichtung von Institutional Repositories
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 23
Herausgegeben von Josef Herget und Sonja Hierl
Darja Dimitrijewitsch, Cécile Schneeberger
Optimierung der Usability des Webauftritts
der Stadt- und Universitätsbibliothek Bern
Chur, 2007
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 24
Herausgegeben von Nadja Böller, Josef Herget und Sonja Hierl
Brigitte Brüderlin
Stakeholder-Beziehungen als Basis einer Angebotsoptimierung
Chur, 2008
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 25
Herausgegeben von Robert Barth, Nadja Böller, Sonja Hierl und Hans-Dieter Zimmermann
Jonas Rebmann
Web 2.0 im Tourismus, Soziale Webanwendungen im Bereich der Destinationen
Chur, 2008
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 26
Herausgegeben von Robert Barth, Nadja Böller, Sonja Hierl und Hans-Dieter Zimmermann
Isabelle Walther
Idea Stores, ein erfolgreiches Bibliothekskonzept aus England – auf für die Schweiz?
Chur, 2008
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 27, im Druck
Herausgegeben von Robert Barth, Nadja Böller, Sonja Hierl und Hans-Dieter Zimmermann
Scherer Auberson, Kirsten
Evaluation von Informationskompetenz: Lässt sich ein Informationskompetenzzuwachs messen?
Eine systematische Evaluation von Messverfahren
Chur, 2009
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 28
Herausgegeben von Robert Barth, Nadja Böller, Sonja Hierl und Hans-Dieter Zimmermann
Nadine Wallaschek
Datensicherung in Bibliotheksverbünden.
Empfehlungen für die Entwicklung von Sicherheits- und Datensicherungskonzepten
in Bibliotheksverbünden
Chur, 2009
ISSN 1660-945X

Über die Informationswissenschaft der HTW Chur

Die Informationswissenschaft ist in der Schweiz noch ein junger Lehr- und Forschungsbereich. International weist diese Disziplin aber vor allem im anglo-amerikanischen Bereich eine jahrzehntelange Tradition auf. Die klassischen Bezeichnungen dort sind Information Science, Library Science oder Information Studies. Die Grundfragestellung der Informationswissenschaft liegt in der Betrachtung der Rolle und des Umgangs mit Information in allen ihren Ausprägungen und Medien sowohl in Wirtschaft und Gesellschaft. Die Informationswissenschaft wird in Chur integriert betrachtet.

Diese Sicht umfasst die Teildisziplinen Bibliothekswissenschaft, Archivwissenschaft und Dokumentationswissenschaft. Auch neue Entwicklungen im Bereich Medienwirtschaft und Informationsmanagement werden gezielt aufgegriffen und im Lehr- und Forschungsprogramm berücksichtigt.

Der Studiengang Informationswissenschaft wird seit 1998 als Vollzeitstudiengang in Chur angeboten und seit 2002 als Teilzeit-Studiengang in Zürich. Künftig wird ein berufsbegleitender Masterstudiengang das Lehrangebot abrunden.

Der Arbeitsbereich Informationswissenschaft vereinigt Cluster von Forschungs-, Entwicklungs- und Dienstleistungspotentialen in unterschiedlichen Kompetenzzentren:

- Information Management & Competitive Intelligence
- Records Management
- Library Consulting
- Information Laboratory

Diese Kompetenzzentren werden im **Swiss Institute for Information Research** zusammengefasst.

IMPRESSUM

Verlag & Anschrift

Swiss Institute for Information Research

HTW - Hochschule für Technik und Wirtschaft
University of Applied Sciences
Ringstrasse 37
CH-7000 Chur

www.informationswissenschaft.ch

www.fh-htwchur.ch

ISSN 1660-945X

Institutsleitung

Prof. Dr. Hans-Dieter Zimmermann
Telefon: +41 81 286 24 61

Email: hans-dieter.zimmermann@fh-htwchur.ch

Sekretariat

Telefon : +41 81 286 24 24
Fax : +41 81 286 24 00
Email: clarita.decurtins@fh-htwchur.ch