„Daten absolut sicher zu schützen ist schwierig.“

Bei künftigen Bibliothekssystemen wird die Cloud eine wichtige Rolle spielen. Prof. Dr. Andreas Degkwitz, Direktor der Universitätsbibliothek der Humboldt Universität zu Berlin, weiß aus eigener Erfahrung, dass Datenschutz-Themen mit den Anbietern sorgfältig zu verhandeln sind. b.i.t.online befragte ihn zu diesem wichtigen Bereich.

Herr Professor Degkwitz, im Zeitalter der NSA-Affäre stellt sich auch für Bibliotheken die Frage nach dem Datenschutz neu. Sind die Daten der Nutzer vor unbefugten Zugriffen sicher?

› Degkwitz ‹ Aktuell haben wir ein angemessenes, gutes Datenschutzniveau. Für die bestehenden Bibliothekssysteme gibt es in dieser Hinsicht klare Vereinbarungen. Zudem werden die im Einsatz befindlichen Systeme überwiegend lokal gehostet. Das gibt ebenfalls Sicherheit. Künftig werden wir uns allerdings neuen Herausforderungen stellen müssen.

Was meinen Sie damit?

› Degkwitz ‹ Die großen Anbieter von Bibliothekssystemen werden mit ihren Next-Generation-Systems in die Cloud gehen. Für den Einsatz dieser Systemlösungen brauchen wir überzeugende Konzepte und belastbare Vereinbarungen beim Schutz der personenbezogenen Daten. Denn die cloudbasierten Bibliothekssysteme verarbeiten die Daten nicht mehr vor Ort in der Bibliothek oder auf dem Universitätscampus. Daraus ergeben sich neue Aspekte für den Schutz der Daten.

Prof. Dr. Andreas Degkwitz

Was bedeutet das konkret?

› Degkwitz ‹ Cloudbasiert bedeutet, dass die Anbieter entsprechender Systemlösungen in einem Rechenzentrum außerhalb der Bibliothek oder der Universität Rechnerressourcen zusammenführen und zu einer Cloud virtualisieren. Auf dieser Basis werden die Bibliothekssysteme gehostet und von den Firmen betrieben. Die Anwendungsmodule sind für die Bibliothekare über eine Webschnittstelle nutzbar und zugänglich. Damit stellen sich neue Fragen für uns: Wo genau stehen die Rechner, deren Leistung zu Clouds virtualisiert werden? Welche Datenschutzbestimmungen gelten dort? Wer kann auf Daten zugreifen und wie sind die Daten vor missbräuchlichen Zugriffen geschützt?

Welche Daten sind von künftigen Cloud-Lösungen betroffen?

› Degkwitz ‹ Einerseits sind das die Metadaten der Informationsressourcen und Medien, die in diesen Systemen verarbeitet und verwaltet werden. Für sie gelten keine datenschutzrechtlichen Anforderungen. Andererseits geht es um die personenbezogenen Daten der Bibliotheksnutzer und -mitarbeiter. Da sieht die Sache schon anders aus. Für diese Datenbestände müssen datenschutzrechtliche Vorkehrungen getroffen werden, um eine missbräuchliche Nutzung zu vermeiden.

Welche personenbezogenen Daten sind damit genau gemeint?

› Degkwitz ‹ Das sind personenbezogene Daten, die erfasst werden müssen, damit die Nutzer Dienste und Services der Bibliotheken in Anspruch nehmen können, zum Beispiel die Ausleihe von Büchern und Zeitschriften. Oder es sind Daten von Mitarbeitern, die sich in das System einloggen müssen, um ihre Arbeit machen zu können.

Also ein durchaus sensibler Bereich.

Degkwitz Allerdings. Denn wir möchten nicht, dass auf diese Daten von Unbefugten zugegriffen und in der Weise Missbrauch betrieben werden kann, dass Nutzerprofile ausgespäht und zu welchen Zwecken auch immer ausgewertet und weitergeleitet werden. Auch die Mitarbeiter sollen auf diese Weise nicht kontrolliert oder überprüft werden. Genau das müssen und wollen wir mit datenschutzrechtlichen Vereinbarungen und Vorkehrungen verhindern.

Warum ist das bei Cloud-Umgebungen ein Problem?

Degkwitz Bei den Cloud-Systemen der Bibliotheksanbieter befinden sich die personenbezogenen Daten nicht mehr vor Ort, sondern auf einer virtualisierten Serverumgebung des Anbieters, die grundsätzlich irgendwo an einem beliebigen Ort lokalisiert sein kann. Eine solche Umgebung lässt sich technisch nicht so abschotten oder kontrollieren, wie das bei den derzeit im Einsatz befindlichen, lokalen Lösungen möglich ist.

Wo liegen denn die Daten bei cloudbasierten Bibliothekssystemen?

Degkwitz Das kommt auf den Anbieter des Bibliothekssystems an. Theoretisch kann das jeder Ort auf der Welt sein. Für deutsche Bibliotheken ist es deshalb wichtig, dass sich die Firmenclouds im europäischen Rechtsraum befinden und damit den deutschen Regelungen zum Datenschutz unterliegen. An einem Serverstandort in den USA ist die Situation aufgrund der dort geltenden Patriot Acts schon anders.

Wir möchten nicht, dass auf diese (personenbezogenen) Daten von Unbefugten zugegriffen und in der Weise Missbrauch betrieben werden kann, dass Nutzerprofile ausgespäht und zu welchen Zwecken auch immer ausgewertet und weitergeleitet werden.

Wann werden Cloud-basierte Lösungen für Sie ein Thema?

Degkwitz Das ist bereits ein Thema. Die Berliner Universitätsbibliotheken der Freien Universität, der Humboldt-Universität, der Technischen Universität und der Universität der Künste setzen derzeit das System ALEPH 500 der Firma Ex Libris aus Israel ein. Wir verhandeln aber schon über ALMA als Nachfolgesystem von ALEPH 500. Da das cloudbasierte Nachfolgesystem ALMA als Software as a Service (SaaS) in Amsterdam und damit innerhalb des europäischen Rechtsraums gehostet wird, ist eine Grundbedingung für die notwendigen, datenschutzrechtlichen Vereinbarungen mit der Firma Ex Libris erfüllt.

Wo könnte dann ein Problem entstehen?

Degkwitz Im Zuge der Vertragsverhandlungen zu ALMA hatte sich herausgestellt, dass Betrieb und Wartung der ALMA-Cloud von Israel aus und damit von außerhalb des europäischen Rechtsraums erfolgen sollten. Das ist mit den deutschen Datenschutzregelungen nicht vereinbar. Daraufhin hat die Firma Betrieb und Wartung der Amsterdamer ALMA-Cloud nach Hamburg verlagert, um so den in Deutschland geltenden Datenschutzregelungen zu entsprechen.

Was passiert, wenn es doch einmal zu unbefugten Zugriffen kommt?

Degkwitz Das ist dann ein schwerer Vertrauensbruch, der zur Kündigung des Vertrages führen kann. Vertragsseitig werden im Fall von Missbrauch oder ungenügenden Schutzvorkehrungen harte Sanktionen vereinbart. Zugleich muss man aber auch ehrlich sagen: Das ist auch das Äußerste, was sich machen lässt. Denn Daten in der Cloud kann man nicht absolut sicher schützen. Allerdings ist er auch bei lokal gehosteten Systemen nie hundertprozentig gegeben.

Worauf müssen Bibliotheken neben dem Datenschutz noch achten?

Degkwitz Dazu sind vor allem die Datensicherheit und die Datenhoheit zu nennen. Datensicherheit bezieht sich auch auf die datenschutzrechtlich unproblematischen, bibliografischen Daten. Die Anbieterfirma muss auf jeden Fall gewährleisten, dass es im Fall einer technischen Panne nicht zu Datenverlusten kommt. Dafür müssen Vorkehrungen wie eine redundante Datenhaltung und Datenspeicherung getroffen werden. Datenhoheit kann beispielsweise gewährleistet werden, indem es zu Ausspeicherungen von Datenbeständen auf firmenunabhängigen Servern im Sinne eines regelmäßigen Back-Ups kommt. Dabei müssen die Daten natürlich in verarbeitungsfähigen Formaten vorliegen. Dies kann dann auch bei der Beendigung von Verträgen oder bei Kündigungen eine wichtige Rolle spielen. Allerdings wird man heute nicht wirklich wissen, was in zehn oder mehr Jahren ein gängiges Format sein wird. Wenn es da vertragliche Regelungen gibt, sind die immerhin einklagbar.

Verhandeln Sie die Verträge in Eigenregie?

Degkwitz Die Leitungen der vier Berliner Universitätsbibliotheken von FU, HU, TU und UdK führen die Verhandlungen gemeinsam. Die Verhandlungs-

gruppe stimmt sich natürlich mit den Anwendern und Technikern in den Bibliotheken ab. Auf externe Unterstützung sind wir beim Datenschutz angewiesen. Da ist das Know-how der Datenschutzbeauftragten unerlässlich. Zudem ist es im öffentlich-rechtlichen Bereich üblich, standardisierte Vertragsformulare zugrunde zu legen. In denen sind grundlegende Vertragskomponenten wie Gewährleistung, Haftung, Kündigung und einiges mehr geregelt. Das ist der so genannte EVB-IT-System-Vertrag.

Das ist quasi ein Mustervertrag?

› Degkwitz ‹ Ja, beim EVB-IT-System-Vertrag sind eine Reihe vertragsrechtlicher Fragen einheitlich geregelt und rechtlich belastbar formuliert. Zusätzlich haben wir uns noch juristische Unterstützung geholt. So können wir sicher sein, dass wir die vertragsrechtlichen Positionen so bekommen, wie wir sie wirklich brauchen.

Übernehmen die Bibliotheken damit an den Universitäten eine Art Vorreiterrolle für andere Hochschulbereiche, die künftig in vergleichbarer Weise mit cloudbasierten Anwendungssystemen zu tun haben werden, etwa mit Campusmanagement- oder Personalmanagement-Systemen?

› Degkwitz ‹ Auf jeden Fall. Lernen kann man vor allem, dass deutlich mehr Sensibilität für Datenschutz, Datensicherheit und Datenhoheit zu entwickeln ist. Zudem kann man sich besser in Gesamtsituationen hineindenken, also in Situationen, die beispielsweise den Datenschutz betreffen, wo plötzlich die Lokalisierung eines Servers eine wichtige Rolle spielt. Wo plötzlich wichtig ist, wer alles auf die Daten zugreift oder darauf zugreifen könnte. Datensicherheit ist derzeit in vielen Fällen wahrscheinlich durch eine Redundanz vor Ort gelöst. Künftig muss man sich ausdrücklich und erneut darum kümmern. Und man muss sich schließlich auch darum kümmern, in welcher Form man bei einer eventuellen Beendigung eines Vertrages die Daten wiederbekommt. Das ist unter anderem eine Frage nach der Datenhoheit. Man wird wahrscheinlich noch enger als bisher mit den Firmen zusammenarbeiten müssen, um diese Punkte zufriedenstellend zu klären. Mit den Themen ist man auf jeden Fall ganz dicht an aktuellen Entwicklungen – und das ist einfach auch sehr interessant!

Herr Professor Degkwitz, vielen Dank für das Gespräch.

Weitere Infos zum Thema Cloud Computing:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein knapp einhundert Seiten langes Eckpunktepapier zum Thema Cloud Computing herausgegeben. Es richtet sich in erster Linie an die Anbieter von Cloud-Lösungen, bietet aber auch Anwendern einen Überblick über relevante Sicherheitsaspekte:

Weiteres:
https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

Weitere Infos zur Cloud-Lösung Alma von Ex Libris:

Nach Angaben des Anbieters Ex Libris soll das Bibliotheksmanagement-System Alma **sämtliche Aufgabenbereiche einer Bibliothek unterstützen: die Erwerbung** und Selektion von Medien, die Verwaltung von Metadaten sowie die Digitalisierung und das Fulfilment. So soll unter anderem das Medienmanagement für elektronische, digitale und physische Ressourcen möglich sein. Durch automatisierte Geschäftsprozesse und gemeinsam genutzte Daten soll das System Arbeitsabläufe vereinfachen und die Gesamtbetriebskosten reduzieren. Für den Bestandsaufbau stehen Nutzungsdaten, Kostenanalysen und Bestandsauswertungen zur Verfügung. Webbasierte, offene Schnittstellen sollen es ermöglichen, Alma in andere Systeme zu integrieren auch in externe Campus-Systeme.

Weiteres:
http://www.exlibrisgroup.com/de/category/AlmaUeberblick#sthash.qJXvVq7h.dpuf