Der nachfolgende Text ist erschienen in: Datenschutz-Nachrichten (DANA), Ausgabe 2008/01

Datenschutz und Datensicherheit an deutschen Hochschulen

Martin Rost

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte 2007 erneut einen Anlauf genommen und sich mittels zahlreicher Beratungsgespräche, einer umfänglichen Prüfung vor Ort und eines Audits einen umgreifenden und tiefen Einblick in die Situation des Datenschutzes bei den landeseigenen Hochschulen verschafft. Das am Ende des Jahres zu ziehende Fazit überraschte wenig: Es ist nach wie vor auffallend schlecht um den Datenschutz an den Hochschulen bestellt. Besonders alarmierend ist, dass sich überwiegend auch keine Bestrebungen oder Strategien abzeichnen, diesen Zustand zu verändern. Schon aus Gründen der Verbesserung ihrer Governance müssen Strategen und Verantwortliche an den Hochschulen alles unternehmen, um endlich Transparenz in ihre EDV-gestützten Verfahren, Workflows und Geschäftsprozesse zu bekommen.

Hochschulen können durchgängig keine hinreichend belegte Auskunft darüber geben, welche personenbezogenen Daten ihrer Klientel, Studierenden und Mitarbeiter sie auf welche Weise und von wem verantwortet verarbeiten oder zugänglich machen. Nirgends gibt es den Ansatz eines gezielt entwickelten, nachhaltigen Datenschutz-Managements, wie er in anderen Organisationen länger schon, in Abstimmung mit der Innenrevision, dem Finanzcontrolling oder dem Sicherheitsbeauftragten der EDV, zumindest auf den Weg gebracht wurde. Die Datenschutzbeauftragten vor Ort kennen den Modus des akuten Reparierens – und halten diesen Modus, zusammen mit der Hochschulleitung, eigentlich auch für den ganz normal nur einnehmbaren. Manchmal sind die Datenschutzbeauftragten der Hochschulen sogar unsicher über ihren eigentlich Arbeitsgegenstand, wenn sie sich bspw. primär aufgerufen fühlen, die Welt über die Gefahren der modernen Technik für den Datenschutz aufzuklären, anstatt ihre eigene Organisation im Hinblick auf Datenschutz-Verstöße zu beobachten.

In den Gesprächen anlässlich der ersten Konferenz für Datenschutzbeauftragte an den Hochschulen, die im September 2007 an der Freien Universität Berlin stattfand, zeigte sich, dass diese Verallgemeinerungen dieser Schleswig-Holsteinischen Befunde erlaubt sind. Und ein Blick in die Tätigkeitsberichte der Landesdatenschutzbeauftragten allein der letzten vier Jahre bestätigt die nachfolgend aufgelisteten Einzelbefunde. Die Datenschutz-Situation an deutschen Hochschulen ist von je her bestürzend schlecht.

Man trifft an den Hochschulen zwar allseits ein im persönlichen Gespräch durchaus glaubwürdiges Bekunden von Sensibilität für Datensicherheit und Datenschutz sowohl bei den Hochschulleitungen als auch den für die Technik Verantwortlichen an. Doch sobald man die übergreifenden Prozesse, die verarbeiteten Daten und die Rollenzuschnitte und Zugriffsregelungen vor Ort einmal ganz konkret im Detail in den Blick nimmt und diese dann mit den gesetzlichen Regelungen abgleicht, erzielt man schnell Einigkeit darüber, dass es um die Datenschutzwirklichkeit sehr schlecht bestellt ist. In der Verwaltung der Hochschulen ist in der Regel professionell ausgebildetes, Rechtskonformität anstrebendes Verwaltungsknow-how anzutreffen, in der Systemadministration überwiegen Kompetenz und Orientierung am aktuellen Stand der Technik. An den zumindest teil-autonom agierenden Instituten wird dagegen, von einigen wenigen Ausnahmen abgesehen, hemdsärmelig, nachlässig und frei von rechtlichen oder fortgeschritten sicherheitstechnischen Kenntnissen in Bezug auf die rechtlichen und technischen Datenschutzanforderungen agiert.

Da wurden beispielsweise, um einen konkret gemeldeten typischen Vorfall zu nennen, Dateiserver, die für die private Heimnutzung billig konzipiert über keine Sicherheits- oder differenzierte Authentisierungsmechanismen verfügen, mal eben zu bereits bestehenden zentralen Fileservern hinzugefügt. Auf diesem Dateiserver lagen fortan monatelang Dateien mit Forschungsprojektanträgen herum, die sensible personenbezogene Daten enthielten. Die Motive für derartiges Ad-hoc-Handeln in Bezug auf EDV gleichen sich inzwischen seit Jahrzehnten: Notorisch wenig Geld und zu wenig Plattenplatz.

Ebenso typisch wie der ungeregelte Umgang mit Plattenplatz ist der in den rechtlich wesentlichen Aspekten ungeregelte Umgang mit E-Mail-Accounts. So wird die private Nutzung von E-Mail-Accounts an den Unis relativ umstandslos erlaubt. Zugleich lässt sich die Uni in den immerhin durchgängig vorhandenen Benutzerordnungen das Zugriffsrecht auf derartig private Daten ebenso umstandslos einräumen. Wenn dann Polizei oder Staatsanwaltschaft die Herausgabe von Daten über Studierende einfordern, wird den Forderungen schlicht entsprochen. Obwohl das Briefgeheimnis hochrangig im Artikel 10 des Grundgesetzes formuliert ist. Mit dem Ausscheiden von Personen werden E-Mail-Accounts ebenso gern platt gelöscht wie jahrelang stehen gelassen. Und es gibt dann niemanden, dem die auf diese Weise entstehenden Datengräber auf den Systemen auffallen, zumindest solange nicht, bis ein Administrator, rechtlich möglicherweise grenzwertig durch das System vagabundierend, hin und wieder aufgrund zufälliger Kenntnisse über solche Accounts stolpert. Und dann? Wer ist für die Löschung verantwortlich? Es gilt festzulegen und an die Betroffenen zu kommunizieren, wie die Maßnahmen für die rechtlichen, organisatorischen und technischen Anforderungen insgesamt im Lebenszyklus eines E-Mail-Accounts an einer Hochschule umgesetzt sind.

Ein weiteres Beispiel für das Problem, methodisch geregelte Prozesse in den Hochschulen einzuführen, betrifft die Abbildung von Prüfungsordnungen in der EDV. So wurde eine veränderte Prüfungsordnung in der Software zur Studierendenverwaltung durch einen (eigentlich von Projektgeldern finanzierten) Hilfswissenschaftler auf bloßen Zuruf durch Umkonfiguration umgesetzt. Nach der Konfiguration wurde das Programm, vielleicht und irgendwie aber in keinem Fall prüfbar dokumentiert, getestet. Der Sinn eines Test-und-Freigabe-Prozesses besteht darin, dass die Verantwortung für eine fachgerechte technische Implementation und Konfiguration eines Regelwerks, das große Bedeutung für die davon Betroffenen hat, als erbracht gelten kann und anschließend die Verantwortung für den korrekten Ablauf vom Fachverantwortlichen übernommen wird.

Eine Sekretärin eines Instituts demonstrierte anlässlich einer Prüfung, wie trivial es für sie möglich ist, die Noten Studierender einzusehen, und zwar auch die anderer Fakultäten, zu denen sie überhaupt keinen Bezug hat. Und weil sie sogar die Passworte einsehen konnte, mit denen die Professoren sich über das Internet von ihren heimischen PCs auf die universitätsinternen Server einloggen können, um Daten ihrer Studentinnen und Studenten zu bearbeiten, hätte sie diese Noten, durch keinen Mechanismus kontrollier- und korrigierbar, verändern können. Dies wurde dann sofort abgestellt. Aber allein der Umstand, dass es durchaus problematisch ist, wenn Professoren von ihren zumeist dilletantisch administrierten heimischen PCs aus – und warum dann nicht auch hin und wieder mal aus einem zwielichtigen Internet-Cafe heraus? – derartige Arbeiten verrichten können, traf bei Beteiligten vor Ort wieder auf Unverständnis. Zwar war in diesem konkreten Fall die Verbindung per https SSL-verschlüsselt, doch liegt darunter kein tatsächlich kontrolliertes Zertifikate-Handling, wie es heutzutage etwa beim Online-Banking eine Selbstverständlichkeit ist. Mag man auch Sekretärin vom Zugriff aussperren können, bei

Systemadministratoren geht das grundsätzlich nicht. Systemadministratoren sind auf einem System allgewaltig und können sozusagen von „hinten“ grundsätzlich an alle Daten herankommen – und nicht nur an die persönlichen Daten der Mitarbeiter und Studierenden, sondern bspw. auch an die Rohdaten von Forschungsprojekten oder an Examens- und Doktorarbeiten. Dass das so ist muss allgemein bekannt sein. Und es müssen organisatorische Vorkehrungen getroffen werden, damit ein Systemadministrator, wenn er mit Superuser- bzw. root-Rechten auf dem System arbeitet, dies nicht unbeobachtet macht. Die Strategie muss sein, dass jegliche Handlung in einer Organisation transparent ist und u.a. auf ihre Rechtmäßigkeit hin überprüft werden kann. Systemadministration muss nicht vertrauensselig hingenommen werden. Hier kann insbesondere der betriebliche Datenschützer für entsprechende organisatorische Schutzvorkehrungen sorgen.

Ein wesentlicher Aspekt von Datenschutz in Organisationen besteht generell darin, für alle Beteiligte – für die Mitarbeiterinnen und Mitarbeiter ebenso wie für die organisationsexterne Klientel – Transparenz in die mehr oder weniger organisierten Prozesse zu bringen. Transparenz ist die Voraussetzung dafür, dass Prozesse intern geregelt, geplant und gesteuert werden können, dass Verantwortung für die Prozesse übernommen werden kann, dass die Wirtschaftlichkeit und Gesetzeskonformität von Prozessen und Entscheidungen nachweisbar wird und dass extern die Betroffene gegebenenfalls der Verarbeitung ihrer personenbezogenen Daten widersprechen können. Deshalb müssen gemäß den Landesdatenschutzgesetzen die Prozesse von Organisationen dokumentiert werden. Erfahrungsgemäß lernen Organisationen mit der Anforderung zur Dokumentation ihre Prozesse überhaupt erst in einem hinreichenden Auflösungsniveau kennen.[1] Wir stellten an sämtlichen Hochschulen fest, dass kein einziger IT-gestützter Kernprozess etwa in der Verwaltung hinreichend dokumentiert war. Einzig Dokumente, die die Nutzungsbedingungen der EDV für Studierende betrafen, waren allseits in eine einigermaßen akzeptable Form gebracht. Doch schon bei Dienstanweisungen für die Sachbearbeiter der Hochschulverwaltung hörte es wieder auf, es lagen schlicht keine vor. Es konnten keine aktuellen Organigramme der Hochschulorganisation vorgelegt werden, ebenso wenig gültige Geschäftsverteilungspläne oder Tätigkeitsbeschreibungen insbesondere für die allmächtigen Systemadministratoren. In einem einzigen Fall konnte man zwar so etwas wie eine angefangne Inventarliste von Hardware und Software zumindest für einen klar abgegrenzten Bereich vorlegen. Es fehlten durchgängig Dokumente für IT- und Verfahren oder Sicherheitsmaßnahmen, die einen definierten Sicherheitsbedarf operativ erfüllen. Über die Aktivitäten, die dabei automatisiert zu protokollieren und zu prüfen sind, war man sich vollkommen im Unklaren, entsprechend gab es keine geregelten Verfahren zum Umgang mit den massenhaft anfallenden Protokolldaten, insbesondere denen über die Tätigkeiten der Systemadministration. Zwar konnten in allen Fällen Netzwerkpläne vorgelegt werden, ohne die eine Administration in einem Computernetz sowieso undenkbar ist. Nur waren diese dann weder aktuell noch methodisch zureichend gestaltet. Zum Teil waren Testsysteme für Software, die in „Produktion“ war, vorhanden. Aber es konnte wiederum keine Dokumentation erfolgter Tests und deren Ergebnisse sowie keine Freigaben der Software für die Produktion durch die Fachverantwortlichen vorgelegt werden. Letzteres ist ein Indikator dafür, dass der rechtlich bedeutsame Akt der Übergabe der Verantwortung vom installierenden, konfigurierenden und funktionentestenden Computerspezialisten auf den inhaltlich testenden Fachverantwortlichen ungeregelt ist. Tatsächlich war man vereinzelt noch der Ansicht, dass grundsätzlich nicht der Fachverfahrensverantwortliche sondern die Technikabteilung die Verantwortung für die EDV-gestützten Verfahren habe. Derartig die Rechtslage verkennenden Statements hört man in Privatunternehmen oder öffentlichen

[1] Man misst den Reifegrad von Prozessen mittels eines 5-stufigen Maturity-Modells: Von Stufe 1 „man hat einen Input und man hat einen Output“ bis zur Stufe 5 mit dokumentierten Prozessen, die man je nach funktionaler Anforderungen neu zusammensetzen kann.

Verwaltungen lange nicht mehr. Die Einrichtung der Zugriffsrechte der Hochschulleitung oder des Verwaltungspersonals oder des akademischen Lehrapparats auf Dateiserver oder personenbezogene Daten von Studierenden konnte in keinem Falle dokumentiert werden. Ebenso wenig konnte man dokumentieren, ob die Hochschulleitung, Dekane oder Systemadministratoren, etwa im Rahmen von Revisionsverfahren oder aufgrund von Sicherheitsvorfällen, in der Vergangenheit außergewöhnliche Zugriffe auf personenbezogene Daten genommen haben. Es gab keine Dokumentation darüber, ob es Sicherheitsvorfälle gab und wie diese gesteuert wurden. Verträge mit externen Dienstleistern, insbesondere den IT-Dienstleistungen der „Hochschul-Informations-System GmbH“ (HIS) oder mit lokalen EDV-Häusern, die bestimmte Vor-Ort-Services leisteten, fehlten entweder völlig oder waren unzureichend. Und nicht zuletzt herrschen durchgängig weitgehend Unkenntnisse geltender Rechtsvorschriften insbesondere auf der Ebene von Fakultäts-, Instituts- oder Fachbereichs-Vertreterinnen und Vertreter vor.

Die Datenschutzbeauftragten waren in der Regel mit geringen Zeitkontingenten ausgestattet (von 5% bis 50% ihrer Arbeitszeit), verfügten durch die Bank über nur geringe technische Kenntnisse und hatten keine auf Nachhaltigkeit zielenden Strategien mit Gestaltungsanspruch eines umfassenden Datenschutzmanagementsystems entwickelt. Ihnen verblieben einzig einige Anlass bezogene Aktivitäten. Immerhin konnten in einem Fall einige Artikel vorgelegt werden, in denen in der lokalen Hochschulzeitung auf Datensicherheitsaspekte hingewiesen wurde, sowie Schulungen zur Weiterbildung bei der Datenschutzakademie. Sie wussten durchgängig von keinem Sicherheitsvorfall zu berichten, sie waren dementsprechend nie an deren Management beteiligt worden. Entsprechend war den Datenschutzbeauftragten der Gedanke fremd, im Rahmen eines Sicherheitsmanagements bei Sicherheitsvorfällen bestimmter Qualität, in denen oftmals an vielen bestehenden Richtlinien vorbei gehandelt wird, die zwangsläufige Beteiligung schlicht einzufordern. Auch muss man vermuten, dass die Bewertung eines Vorfalls als Sicherheitsvorfall so gar nicht vorgenommen wird.

Und das ist das Beunruhigende beim langjährigen Blick auf Hochschulen: Während anderen Orts, in öffentlicher Verwaltung und Wirtschaft, die Konzepte etwa zum Risikomanagement a la IT-Infrastructure Library („ITIL“) sowie IT-Architekturstrategien wie Service-Oriented-Architectures („SOA“) oder die Durchleuchtung der eigenen Sicherheitsmaßnahmen nach BSI-Grundschutz oder der Aufbau eines IT-Sicherheits- und Datenschutzmanagementprozessen inzwischen zum langweilig gewordenen Alltag gehören, hat man an den Hochschulen noch nicht einmal angefangen, sich mit diesen Strategien und Konzepten der Verschränkung von Aufgabenstellungen, Organisation und IT-Services überhaupt nur ernsthaft zu beschäftigen**.** Vor Ort, beim einzelnen Administrator, findet man da durchaus Vorstellungen darüber, welche Vorteile beispielsweise der Betrieb eines zentralen Helpdesks brächte, um mit Hilfe eines Ticketsystems im Backofficebereich das Incident- und Changemanagement der gesamten Hochschule effektiver als bislang zu organisieren. Aber auf Seiten der für die Hochschulorganisation Verantwortlichen scheint es so zu sein, dass diese meinen, mit der stärkeren Verwirtschaftlichung der Hochschultätigkeiten in den vergangenen 15 Jahren alles Wesentliche entschieden zu haben.

Dabei lassen sich Hochschulen nach wie vor kaum steuern. Dieser regelrechte Bedarf an Intransparenz lässt sich nicht auf die notwendige Freiheit für Forschung und Lehre in den Fakultäten zurückführen und lässt sich auch nicht dadurch nachhaltig austrocknen, indem man unter größten Mühen ein verbessertes Finanz-Controlling implementiert oder die Ausbildung verschult. Im Kern gilt es, die Produktionsseite von Hochschulen zu professionalisieren, also insbesondere den Wahrheit-konstitutiven Aspekt des wissenschaftlichen Diskurses technisch zu unterstützen. Erst wenn dieser Kern der Produktion, Konsumtion und Distribution von

Diskursbeiträgen auf dem Niveau industrieller Produktion angelangt ist, greifen auch die modernen Steuerungsinstrumente, wird es zu einer Professionalisierung auch der Hochschulorganisation kommen. Man kann Hochschulen, weil sie organisatorisch und mental bislang nicht in der industrialisierten Moderne angekommen sind sondern noch immer in zunftähnlichen Strukturen verhaftet sind[2], auch nicht mit den Mitteln der Moderne steuern. Entsprechend schlecht ist es um die reale Datenschutz-Awareness und das Datenschutz-Management in Bezug auf die Mitarbeiter unter den Wissenschaftlern und der Verwaltung, etwaigen Versuchspersonen und nicht zuletzt der Studenten bestellt. Datenschutz, möglicherweise verstanden sogar im modern-umfassenden Sinne einer ganzheitlichen Kommunikationsökologie, ist an Hochschulen, anders als in anderen Organisationen, bislang kein relevantes Thema.

Was ist zu tun? Einfach nur mehr Ressourcen für den Datenschutzbeauftragten (DSB) einzufordern ist allein wenig zielführend. Ressourcen gibt es nur, wenn die oder der DSB etwas wertschöpfend Funktionales für die Organisation zu bieten hat. Sie oder er sollte deshalb zumindest soviel Professionalität aufweisen, um als ein aktiver Wächter der Rechtmäßigkeit insbesondere im Umgang mit personenbezogenen Daten auftreten zu können. Damit sind nicht nur Kenntnisse der einschlägigen Datenschutzgesetze gemeint sondern generell Kenntnisse darüber, welche Regelwerke (Gesetze, Verordnungen, Verträge, Leitlinien) gelten und wie geforderte Regelkonformität herstellbar ist. Ein DSB sollte aktiv nach Bündnispartnern mit Interessensschnittmengen suchen, also vor allem mit dem Personalrat bzgl. Mitarbeiter-Datenschutz ins Gespräch kommen, mit Studierendenvertretern sprechen und den Kontakt zum Sicherheitsbeauftragten des Rechenzentrums suchen. Mit dem Leiter des Rechenzentrums bzw. dem EDV-Leiter lässt sich eine Dokumentationsstrategie der Verfahren und der Technik vereinbaren. Man sollte damit beginnen, die HIS aufzufordern, zu dokumentieren, was dort wo und in welcher Form protokolliert wird und unter welchen Umständen wer warum und wie diese Daten auswertet und wie mit dann möglicherweise festgestellten Sicherheitsvorfällen und Datenschutzverstößen verfahren wird. Und der Hochschulleitung ist darzulegen, dass Datenschutz heutzutage zu einem konstruktiven Aspekt des Qualitäts- bzw. Risk-Managements einer Organisation geworden ist. Datenschutz heute heißt: Konstruktive Beteiligung am Kommunikationsmanagement nach Innen und Außen.

[2] Rost, Martin, 2001: Zur Produktion des Wissens im digitalen Zeitalter; in: Universität Erfurt/ Heinrich Böll-Stiftung 2001: Universitäten in der Wissensgesellschaft (Erfurter Universitätsreden), München, Iudicium-Verlag. http://www.maroki.de/pub/sociology/mr_wkdz.html