

Anforderungen an den Datenschutz

Alle Hochschulen¹ haben Tag für Tag neue Probleme mit der Sicherheit in Netzen, und jede Öffnung nach außen bedeutet den Verlust von Sicherheit und die ständigen Versuche Dritter, noch mehr Daten zu erlangen, als die Einrichtung ohnehin schon zugänglich macht. Hierbei haben die Hacker und Cracker keinerlei Respekt vor den berechtigten Interessen der Betroffenen, deren Daten seelenruhig durchgeblättert werden und erst recht kein Verständnis dafür, daß nicht alle Daten einer Einrichtung jedermann zugänglich gemacht werden können. Sicherlich sind wir noch nicht weit genug von den Jägern und Sammlern entfernt. Auch ich muß immer wieder gegen meine eigene Datensammelwut angehen. Die Neugierde ist den meisten Menschen so eigen, daß insbesondere die Information, die man nicht hat, als die wichtigste Information erscheint. Außerdem sind im Informationszeitalter, in dem wir uns zweifelsohne befinden, alle Fakten über Personen und Dinge Macht. Diese Informationen, geeignet (oder ungeeignet) gestreut und eingesetzt, verleihen dem Nutzer (scheinbar) die Position, die er einzunehmen gewillt ist. Unsere Verfassung jedoch orientiert sich nicht am Sammler und Jäger, an dem Neugierigen oder dem Machtbesessenen. Vielmehr sind die Bürger Grundrechtsträger, und der Staat hat dem Bürger und der Gemeinschaft zu dienen und insbesondere dessen Grundrechte, z. B. das informationelle Selbstbestimmungsrecht² zu schützen. Dieses Idealbild stimmt allerdings nicht mit der Realität überein.

Bei nationalen und internationalen Stellen findet man teilweise eine Sammelwut, die jeden Briefmarkensammler erblassen läßt. Die Begründungen für diese Sammelleidenschaft sind ebenso vielfältig, wie die Anfragen, mit denen auch unsere Einrichtung überschüttet wird. So wollen gerne die Militärattachés verschiedener west- und osteuropäischer Staaten wissen, wie weit denn ihre insbesondere männlichen Staatsangehörigen an unserer Universität als Studenten gekommen sind. Ferner solle man doch die aktuellen Adressen übermitteln. Auf den Hinweis auf das Berliner Datenschutzgesetz³ und die Europäischen Richtlinien zur Datenübermittlung⁴ wird unterschiedlich reagiert. Die Antworten reichen von „Versuchen kann man es ja mal“ bis zu „Sie werden schon sehen, was Sie davon haben; wir können auch anders“. Auch andere Stellen sind nicht besser: Mitglieder unserer Hochschule machten in Potsdam eine Erhebung mit dem Ziel, die soziale Fluktuation in einem bestimmten Viertel nach der Wende zu dokumentieren. Hierzu erfragten sie kleinste Details zu Familienstatus, Einkommen und Wohnverhältnissen. Um die Sache abzurunden, wurden die Erhebungsbögen den Probanden direkt und unverschlossen an der Wohnungstür ausgehändigt und dort auch ebenso wieder eingesammelt. Gleichzeitig

wurde versichert, daß dieses Verfahren vollkommen anonym sei. „Leider“ war einer der ersten Befragten der Landesdatenschutzbeauftragte Brandenburgs, der zu Recht Anstoß am Fragebogen und dem Verfahren nahm. Bei einer entsprechenden Vorabstimmung mit dem Behördlichen Datenschutzbeauftragten oder dem Landesdatenschutzbeauftragten wäre dies nicht passiert.

Allerdings muß auch der Datenschutz seinen Teil dazu leisten, daß nicht die Stammtischredner Munition für die stete Rede vom Datenschutz als Täterschutz erhalten. Gefragt ist ein verantwortungsbewußter, sensibler Umgang mit den Daten und eine gefühlvolle, situationsbezogene, aber auch berechenbare und konsequente Anwendung des Datenschutzrechtes. Datenschutz ist nicht das Totschlagsargument für unliebsame Aufgaben. Viele Schritte im Datenverkehr sind bereits durch das allgemeine Datenschutzrecht erlaubt. Allerdings können wir in einer neuen Materie, wie sie das Internet darstellt, nicht alles durch Spezialregelung vorherbestimmen. Manche Probleme tauchen erst später und plötzlich auf. Wir müssen daher im Vorfeld die Rechte und Pflichten der Beteiligten so allgemein wie möglich und so speziell wie nötig aufführen, ohne hierdurch unbewußt geltendes Recht zu verletzen oder zu umgehen. Nur so werden wir dem Gebot des Bundesverfassungsgerichts⁵, daß das informationelle Selbstbestimmungsrecht nur durch ein eindeutiges Gesetz einschränkbar ist, gerecht. Dieses Normsetzungsverfahren kann teilweise durch das Satzungsrecht der HU ausgeübt werden.

Die Humboldt-Universität zu Berlin hat hierzu bereits rechtzeitig die Weichen gestellt. So wurden unterschiedliche, mit Informatikern, Technikern, Fakultätsangehörigen, Verwaltungsmitarbeitern, Juristen und Datenschützern besetzte Gremien geschaffen, die den für eine Hochschule notwendigen Schritt der Vernetzung einschließlich der Internetanbindung und die dafür erforderlichen rechtlichen und sicherheitstechnischen Voraussetzungen diskutieren und erstellen. Diese Arbeit, die vom Direktor des Rechenzentrums,

1 z. B. wie von Clifford Stoll in seinem Buch „Kuckucksei“ beschrieben

2 Dieses folgt aus Art. 1 und 2 des Grundgesetzes [Grundgesetz für die Bundesrepublik Deutschland vom 23.5.1949 (BGBl. S. 1), zuletzt geändert am 3.11.1995 (BGBl. I 1492)].

3 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz) in der Fassung vom 17.12.1990 (GVBl. 1991, 16, 54), zuletzt geändert am 3.7.1995 (GVBl. 404)

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Datenverkehr

5 Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983, BVerfG 15.12.1983 BVerfGE 65, 1 (46)

Herrn Dr. Schirmbacher, und seinen Mitarbeitern mit Elan und Disziplin vorangetrieben wurde, kann hier nicht abschließend aufgezählt werden, zumal auch bei einer sich ständig weiterentwickelnden Technik nie ein Abschluß erreicht werden kann. Aber es wurden beachtliche Zwischenergebnisse erzielt, die auch über den Bereich der Hochschule hinaus Beachtung gefunden haben. Es sei anstatt vieler die Steuerungsgruppe Verwaltungsnetz⁶, das Forschungsprojekt Firewall, sowie die Rechnerkommission genannt. Aus der datenschutzrechtlichen Sicht muß ich insbesondere die sogenannte Clearingstelle als einen Meilenstein der vertrauensvollen Zusammenarbeit und einen der Grundpfeiler der Sicherheitsbemühungen beim Aufbau der Rechnernetze hervorheben. In der Clearingstelle verständigen sich der Direktor des Rechenzentrums der HU und der Behördliche Datenschutzbeauftragte über die Einhaltung der Sicherheit in den Netzen der HU, die gegebenenfalls notwendigen Kontrollen bei Verstößen und die daraufhin erforderlichen Sanktionen. Selbstverständlich geschieht dies nicht, ohne daß vorher fachkundige Unterstützung entweder aus den Fakultäten oder aus der ZUV hinzugezogen wurde. Dieses Verfahren beruht auf Abschnitt 4.1 letzter Absatz der Computerbetriebsordnung (CBO)⁷ der Humboldt-Universität zu Berlin (HU) in Verbindung mit §§ 19 Abs. 5 und Abs. 1 Berliner Datenschutzgesetz.

Wichtigstes internes Instrumentarium ist die CBO, einer Satzung, die die Aufgaben, Rechte und Verantwortungen von Datenverarbeitungsbeauftragten, Systemverantwortlichen und Benutzern festlegt (Abschnitt 3. der CBO). Ferner wurden unter Abschnitt 4 der CBO spezielle Regelungen für Datennetze sowohl innerhalb, als auch außerhalb der HU geregelt. Hierbei wollte man nicht die Strafgesetze⁸, das Berliner Datenschutzgesetz⁹, das Bundesdatenschutzgesetz¹⁰, das Urheberrechtsgesetz¹¹, das Hochschulrahmengesetz¹² oder das Berliner Hochschulgesetz¹³

wiederholen oder verändern. Vielmehr galt es, unter Berufung auf diese allgemeinen gesetzlichen Grundlagen, eine ordnungsgemäße Nutzung der Netze zu ermöglichen. Zum einen gewährt die Hochschule ihren Mitgliedern einen hohen Grad an Eigenverantwortung. Die Nutzer sind beim Umgang mit den Geräten zur Beachtung der allgemeinen Sorgfaltspflichten und der gesetzlichen Bestimmungen verpflichtet, z.B. § 6 Abs. 1 BlnDSG (Zulässigkeit der Datenverarbeitung), § 8 BlnDSG (Datengeheimnis) oder § 30 Abs. 1 Satz 3, 2. Halbsatz BlnDSG (Datenverarbeitung für wissenschaftliche Zwecke und Anzeigepflicht beim Datenschutzbeauftragten). Ferner haben die Nutzer der Datennetze sich aufgrund der besonderen Konditionen, unter denen wir als Hochschule und als Mitglieder die Dienste nutzen können, sich selbst auf Studienzwecke, Forschung, Lehre und Verwaltungstätigkeiten bei ihrer Nutzung zu beschränken.

Neben den Nutzern gibt es ein abgestimmtes System von Systemverantwortlichen und Datenverarbeitungsbeauftragten (DV-Beauftragten). Diese haben Organisations- und Koordinierungsaufgaben. Übergeordnetes Gremium ist die Senatskommission für Rechentechnik des Akademischen Senats der HU (SKR). Um die Sicherheit im Rechnernetz zu gewährleisten, werden mit Einwilligung der Nutzer, die diese bei Antragstellung schriftlich dokumentieren, bei den Nutzern gewisse Daten erhoben. Ferner besteht die Möglichkeit, in einen Datenabgleich mit der Studienabteilung und der Personalabteilung einzuwilligen. Hierdurch werden Bearbeitungszeiten bei der Accountvergabe und Verlängerung deutlich verkürzt. Außerdem werden zu Abrechnungszwecken, aber auch zu Kontrollzwecken Protokolldateien erstellt. Um einem Mißbrauch vorzubeugen, werden diese Daten allerdings mit der klaren Zweckbindung im Sinne der §§ 9 und 11 Berliner Datenschutzgesetz (BlnDSG) erhoben und verarbeitet, so daß sie grundsätzlich nur dann verarbeitet werden, wenn konkrete Anhaltspunkte für schwere Verstöße gegen Nutzungsregeln, also in aller Regel auch Verstöße gegen Strafvorschriften, vorliegen. Diese Daten können aber auch ausnahmsweise zu Zwecken der Datensicherung herangezogen werden, falls dies in einem gesondert zu begründenden Fall notwendig ist. Um jedes willkürliche Verhalten auszuschließen, geschieht diese Nutzung in Abstimmung zwischen dem Rechenzentrum und dem Behördlichen Datenschutzbeauftragten in der Clearingstelle. Selbstverständlich wird hierbei auf die Einhaltung der geltenden Gesetze, insbesondere des Telekommunikationsgesetzes und des Teledienstgesetzes, geachtet. Ein ähnliches Verfahren greift z. B. auch bei Verstößen gegen die geltenden Arbeitsanweisungen zum Virenschutz¹⁴ in der Zentralen Universitätsverwaltung. Somit wird der

6 Diese setzt sich aus dem Organisationsreferenten, dem Direktor des Rechenzentrums, dem Leiter der Haushaltsabteilung, der Abteilungsleiterin im Rechenzentrum „EDV in der Verwaltung“, der Verwaltungsleiterin der MatNatFak II, einer Vertreterin des Personalrats und dem Datenschutzbeauftragten zusammen.

7 Computerbetriebsordnung vom 26.10.1996, veröffentlicht im Amtlichen Mitteilungsblatt der Humboldt-Universität zu Berlin Nr. 22/1996

8 Strafgesetzbuch i.d.F.v. 10.3.1987, zuletzt geändert am 22.7.1997 (BGBl. I 1870)

9 s. Fn. 3

10 Bundesdatenschutzgesetz v. 20.12.1990 (BGBl. I, 2954) zuletzt geändert am 14.9.1994 (BGBl. I, 2325)

11 Gesetz über Urheberrechte und verwandte Schutzrechte vom 9.9.1965 (BGBl. I, 1273) zuletzt geändert am 22.7.1997 BGBl. I, 1870

12 Hochschulrahmengesetz vom 9.4.1987 BGBl. I, 1170) zuletzt geändert am 24.2.1997 (BGBl. I, 1078); Die geplante Neufassung kann unter www.th-darmstadt.de/fsmathe/hopo/HRG-20-8-97.html betrachtet werden.

13 Gesetz über die Hochschulen im Land Berlin (Berliner Hochschulgesetz) i.d.F.v. 5.10.1995 (GVBl. 728)

14 Festlegung im Protokoll der 13. Sitzung der Steuerungsgruppe „Verwaltungsnetz“ am 14.2.1997

Datenschutz mehrstufig durch die abgestufte Zuordnung von Rechten und Pflichten an die Nutzer, DV-Verantwortlichen und das Rechenzentrum gewährleistet.

Dieses Verfahren der abgestuften Sicherheit und des Datenschutzes hat sich bereits vielfältig bewährt bei Maßregelungen gegen Computercracks unserer Universität, die das Sicherheitssystem des Pentagon oder anderer US-amerikanischer Hochschulen „testen“ wollten, Studenten, die die „freizügigen“ Angebote des Internets sehr extensiv und materialaufwendig durch den Abruf oder das Zurverfügungstellen teilweise doch sehr eindeutiger Bilder nutzen wollten, sowie Studenten, die den Gedanken von der kommerziellen Nutzung des Internets rasch (leider auf unser aller Kosten) umsetzen wollten und deren Mailbox den Anstürmen der Käufer nicht standhielten. Nicht alle Fälle waren so spektakulär, daß sich (wie im Fall des Vertriebs von kinderpornographischem Material) die Presse und die Staatsanwaltschaft damit beschäftigten. Dieser strafende Charakter soll auch nicht im Vordergrund stehen, sondern die Beratung, aber auch die Kontrolle. Hierbei ist die Stelle des Behördlichen Datenschutzbeauftragten Vermittler zwischen den verschiedenen Sicherheitsinteressen in Rechnernetzen, dem informationellen Selbstbestimmungsrecht und dem daraus folgenden Recht, sich so anonym wie möglich im Netz zu bewegen (was wir ja auch gewährleisten), und den Aufgaben einer öffentlichen Stelle, Mißbräuchen und Straftaten keinen Vorschub zu leisten. Durch die Befugnisse des Datenschutzbeauftragten und seiner unabhängigen Position ist ein Höchstmaß an Vertraulichkeit der zur Sicherheit des Einzelnen genutzten Daten und der von der Gemeinschaft genutzten Netze gewährleistet. Durch den Dialog mit dem Rechenzentrum wird gleichzeitig eine lebensfremde und sachferne datenschutzrechtliche Lösung vermieden.

Leider muß auch angemerkt werden, daß sich diese technischen und Sicherheitsstandards unseres Rechnernetzes bei der Geschwindigkeit der Technikentwicklung, aber auch unserer eigenen beschränkten universitären Haushaltsmittel, nur mit Mühe aufrechterhalten lassen. Kurzfristig angeworbene Drittmittel und der überdurchschnittliche Einsatz der Kollegen im Rechenzentrum kann nur dazu führen, daß ein Abfall des Standards und damit der Sicherheit nicht stattfindet und eine langsame Steigerung erreicht werden kann.

Bester Datenschutz liegt allerdings immer dann vor, wenn jeder sein eigener Datenschutzbeauftragter ist, d. h. wenn sich die einzelnen, die sich im Netz bewegen, stets bewußt machen, daß cookies und trojan horses an jeder Ecke lauern können. Spätestens außerhalb unseres Rechtskreises wird man auf einen Server treffen, der Nutzer von anonymizern oder Netscape 4.01a, die die cookie-Nutzung unterdrücken, von der Nutzung ausschließt. Das Internet erscheint mir manch-

mal nicht anders als ein riesiges Pinnbrett mit Postkarten. Demnach kann jede Information, die im Internet (unverschlüsselt) weitergegeben wird, ausgelesen und mißbraucht werden. Und selbst Schlüssel bieten nur bedingt Schutz vor kriminellen Handlungen. Die Gemeinschaft der Internetnutzer hat noch keine paradiesischen Zustände erreicht, d. h. den eigenverantwortlichen und rechtstreuen Nutzer in einem technisch ausgereiften Netz mit absoluter Sicherheit und Datenschutz. Soweit ich zu dieser Sicherheit in Rechnernetzen und dem Schutz der personenbezogenen Daten unserer Mitglieder und Nutzer etwas beitragen kann, biete ich mich gern als Ansprechpartner an.

André Kuhring
Datenschutzbeauftragter der HU