Schulen ans Netz - mit Sicherheit

Internetnutzung durch Schulen unter Datenschutzgesichtspunkten

Stand August 2011

Inhaltsverzeichnis

1. Einleitung

"Ich bin drin", sagt nicht nur Boris, sondern sagen auch viele Schulen, die bereits über einen Internetzugang verfügen. Nahezu alle bremischen Schulen sind inzwischen mit Computern ausgestattet.

Mit der Intensivierung des Interneteinsatzes steigt auch die Zahl der Eingaben und Anfragen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen zum Thema Datenschutz und Datensicherheit in den Schulen. Schulleitungen, Lehrerinnen und Lehrer, Erziehungsberechtigte, Schülerinnen und Schüler haben gleichermaßen Beratungsbedarf. Fragen zum datenschutzgerechten und sicheren Umgang mit dem Medium Internet werden leider oft erst gestellt, wenn es zu spät ist. Müssen es Lehrerinnen und Lehrer hinnehmen, dass ihre Namen auf der Schulhomepage veröffentlicht werden? Wie konnte es passieren, dass ein Schüler vom häuslichen Computer aus Fotos von Lehrkräften auf der Schulhomepage virtuell verfälscht, und wer ist dafür verantwortlich? Wer hat zu entscheiden, ob die Daten einer 16-jährigen Schwimmschulmeisterin auf der Schulhomepage veröffentlicht werden dürfen? Dürfen Lehrkräfte private E-Mails ihrer Schülerinnen und Schüler lesen? Was tun, wenn minderjährige Naziseiten oder Pornoseiten über den Schulcomputer abrufen?

Die Chancen des Internets auch und gerade für Schulen sind unbestritten. Aber gerade deshalb sollten sich alle Beteiligten schon vor dem Onlinestart der Risiken des Surfens, Chattens und Mailens im Netz bewusst sein und angemessene Sicherheitsmaßnahmen überlegen. Jede Schule sollte verbindliche Regeln festlegen, damit alle Beteiligten wissen, wer das Internet in der Schule wann und wie nutzen darf und welche Kontrollen und Sanktionen bei einem Verstoß vorgesehen sind.

Diese Orientierungshilfe kann nicht allen Aspekten des Mediums Internet im Hinblick auf Medienrecht und Urheberrecht, Jugendschutz, Erziehungsrecht und Strafrecht Rechnung tragen; sie beschränkt sich vielmehr auf die Gesichtspunkte des Datenschutzes und der Datensicherheit. Da jedoch auch hier die Probleme so vielschichtig und bunt sind wie die Möglichkeiten und Gefahren, die das Internet bietet, können selbstverständlich nicht alle Fallkonstellationen abschließend dargestellt und behandelt werden. Ziel ist es vielmehr, unnötige Crashs auf den Datenautobahnen der Schulen zu verhindern.

2. Internet im Unterricht

2.1 Gegenstand des Unterrichts

Das Medium Internet sollte in den Schulen nicht nur Lehrmittel oder Hilfsmittel sein, sondern auch Gegenstand des Unterrichts. Dabei ist nicht in erster Linie die Vermittlung technischer Fertigkeiten gemeint, zumal für viele Schülerinnen und Schüler der technische Umgang mit dem Internet ohnehin längst selbstverständlich ist.

Wer heute 10-Jährigen erklären will, wie sie "ins Netz kommen" und surfen können, was eine Homepage, ein Chatroom oder ein Soziales Netzwerk ist, wird in der Regel bestenfalls belächelt werden. Erziehung zu Medienkompetenz und Selbstverantwortung im Umgang mit dem Internet muss vielmehr vor allem auch

bedeuten, die Schülerinnen und Schüler über den Tellerrand der bloßen Technik hinaus mit dem Internet als Medium, seiner Funktionsweise, seinen Risiken und Gefahren vertraut zu machen, die Einsatzmöglichkeiten (auch) kritisch zu hinterfragen und den datensicheren Umgang zu erlernen und zu trainieren. Es geht dabei um die Erkenntnis, dass nicht nur der Missbrauch, sondern auch der Gebrauch von Computern riskant ist.

Erziehung zu Medienkompetenz und Selbstverantwortung im Umgang mit dem Internet unter den Gesichtspunkten des Datenschutzes und der Datensicherheit - ein hehres Ziel, aber was bedeutet das konkret für die Unterrichtspraxis? Schülerinnen und Schüler sollten, und zwar nicht nur im Informatikunterricht, vor dem Onlinestart auf jeden Fall mit folgenden Basisinformationen vertraut gemacht werden.

2.1.1 Datenschutz und (Selbst-) Verantwortung

Internetangebote sind rechtlich gesehen Telemedien, die im Telemediengesetz (TMG) geregelt sind.

Telemedien sind alle elektronischen Informationsdienste und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt, wie etwa Telebanking, Datenaustausch, Angebote zur Nutzung von Telespielen und Angebote von Warenleistungen und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit sowie Soziale Netzwerke.

Mediendienste sind die an die Allgemeinheit gerichteten Informationsdienste und Kommunikationsdienste, wie zum Beispiel die Homepage einer Schule mit allgemein abrufbaren Informationen, Messergebnisse in Text und Bild, Fernsehtext und vergleichbare Textdienste.

Allgemein gilt: Daten anderer Personen dürfen ohne gesetzliche Grundlage oder wirksame Einwilligung nicht im Internet verarbeitet werden. Eine Schülerin darf deshalb nicht ohne Einwilligung ihres Freundes (beziehungsweise seiner Eltern) sein Bild oder sonstige Daten über in ins Internet stellen. Ein Schüler darf nicht, auch nicht spaßeshalber, einfach die persönlichen Informationen über seine Lehrerinnen oder seinen Lehrer auf der schuleigenen Homepage verändern.

Richten sie eine eigene Homepage ein, werden sie Diensteanbieter von Telemedien und müssen einige medienrechtliche und datenschutzrechtliche Verpflichtungen erfüllen.
Gegenstand des Unterrichts sollte die Vermittlung des nachstehenden datenschutzrechtlichen Grundlagenwissens sein:

- Was bedeutet Recht auf informationelle Selbstbestimmung?
  Das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.
- Was sind personenbezogene Daten?
  Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

- Was bedeutet Datenverarbeitung?
  Das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.
- Unter welchen Voraussetzungen ist eine Einwilligung wirksam, wer ist einwilligungsfähig?

Weitere Anhaltspunkte zu datenschutzrechtlich relevanten Fragen, die die Schülerinnen und Schüler und ihre Nutzung des Internets betreffen, können den anderen Kapiteln dieser Orientierungshilfe entnommen werden; im Übrigen wird auf das Informationsmaterial verwiesen, das sich unter www.datenschutz-bremen.de oder den Internetadressen anderer Datenschutzbeauftragter befindet, unter www.datenschutz.de.

2.1.2 Risiken der Internetnutzung

Die Schülerinnen und Schüler müssen sich, bevor sie im Internet surfen, spielen und Nachrichten austauschen, bewusst machen, dass sie dabei Spuren hinterlassen und grundsätzlich weltweit die Möglichkeit besteht, auf alle von ihnen preisgegebenen personenbezogenen Daten Zugriff zu nehmen. Eine vollständig anonyme Nutzung ist dem Internet bereits aus abrechungstechnischen Gründen bis heute weitestgehend fremd. In aller Regel wird es personenbezogen, personenbeziehbar über einen Usernamen/User-ID oder unter Gruppenkennungen genutzt. Daher hinterlässt etwa jedes Aufblättern von Homepages Datenspuren. Bei Kommunikationsvorgängen, etwa per E-Mail, werden Daten in der Regel nicht verschlüsselt, sodass sie auf ihrem Weg durch das öffentliche Netz ausgespäht werden können, zum Beispiel unbefugt durch potenzielle Arbeitgeber.

Aus der unsicheren Infrastruktur des Internets erwachsen Gefahren für die Vertraulichkeit und inhaltliche Integrität der übertragenen Daten. Zudem können bestehende Schwachstellen der Endgeräte ausgenutzt werden, um sich mit relativ wenig Aufwand unbemerkt einen unberechtigten Zugang zu dem kommunizierenden Rechner zu verschaffen. So können Daten ausgespäht, aber auch manipuliert oder gelöscht werden. Unverschlüsselte und nicht digital signierte Nachrichten sind so leicht lesbar, veränderbar und unterdrückbar wie eine maschinengeschriebene Postkarte, die außerdem auch eine andere Person geschrieben haben kann. Gewissheit über die Richtigkeit von Inhalt und Herkunft gibt es also nicht.

Beispiele für die gläserne Internetnutzung:

- Mit Suchprogrammen wie etwa "deja news" lassen sich Profile aller in Sozialen Netzwerken wie StudiVZ oder Facebook Kommunizierenden erstellen. Auf diese Weise können zum Beispiel Hobbys und persönliche Neigungen erfasst werden.
- Im Internet werden Datensätze, sogenannte cookies, oft ohne Wissen der Nutzenden auf der Festplatte des eigenen Rechners hinterlassen und bei der nächsten Einwahl möglicherweise automatisch wieder aufgerufen; über diesen Mechanismus können Profile der Nutzerinnen und Nutzer erstellt werden, ohne dass diese es merken.
- Wer sich im Internet - selbst unter so harmlosen Rubriken wie etwa dem "Treffpunkt" oder ähnlichem - mit Namen, Adresse oder anderen Erreichbarkeitsdaten aufnehmen lässt, sollte damit rechnen, dass dies auch

unerwünschte Nutzungen, etwa Übersendung von Werbung zur Folge haben kann. Dies gilt auch für die schuleigene Homepage.

Am Beispiel der unsicheren E-Mail, die auf ihrem Weg durch das weltweite Internet viele Stationen passiert, an denen sie abgefangen, mitgelesen oder auch verändert werden kann und von der niemand sicher sein kann, dass sie von derjenigen Person stammt, deren Namen und E-Mail-Adresse vom Mailprogramm angezeigt wird, lassen sich Risiken und Gefahren gut verdeutlichen.

2.1.3 Schutzmaßnahmen

Es ist wichtig, die Schülerinnen und Schüler altersgerecht über Schutzmaßnahmen zu unterrichten und diese mit ihnen einzuüben. Schon die jüngsten Nutzerinnen und Nutzer müssen wissen, dass sie ihre personenbezogenen Daten nicht im Internet preisgeben sollten, wenn sie zum Beispiel Kinderclubseiten aufsuchen und hier im Rahmen eines Spiels nach ihrem Vornamen und Nachnamen, ihrer Postanschrift und ihrem Geburtsdatum gefragt werden. Denn mit solchen Informationen werden unter Umständen zielgruppengerecht Werbungsmaterialien ausgesucht und übersandt. Mit älteren Schülerinnen und Schülern sollten Maßnahmen zum Schutz von Vertraulichkeit (Verschlüsselungsverfahren), Integrität und Authentizität (Signierverfahren) besprochen und trainiert werden. Diese und weitere Schutzmaßnahmen, gegen Löschen oder Verlust von E-Mails, gegen Viren und Trojanische Pferde, lassen sich wiederum anschaulich am Beispiel der E-Mails darstellen. Bei der Teilnahme an Foren und Chats aller Art oder in Sozialen Netzwerken, aber auch zum Surfen im Internet ist die Verwendung eines Pseudonyms nützlich und ratsam.

Weitere Informationen sind unter www.datenschutzzentrum.de/anon/ und http://anon.inf.tu-dresden.de sowie unter www.bsi.de zu finden.

Allgemeine Empfehlung: Schülerinnen und Schüler sowie Lehrkräfte sollten ihre personenbezogenen Daten im Internet grundsätzlich nicht preisgeben. Es wird empfohlen, bei individueller Nutzung nach draußen, etwa in Chatrooms oder Sozialen Netzwerken, Pseudonyme zu verwenden, auch wenn bei einem Internet-Zugang über einen Schulrechner meist nur die Kennung des Schulrechners in Erscheinung tritt. Ebenso sollten Nachrichten verschlüsselt werden, wenn ihr Inhalt niemanden etwas angeht.

2.2 Nutzung im Unterricht

Die Möglichkeiten der Internetnutzung im Unterricht sind bunt und vielfältig. Schülerinnen und Schüler können im Sozialkundeunterricht Informationsmaterial zum Thema Rechtsextremismus zusammenstellen und im Chat-Forum Fixerstuben - Pro und Contra mitdiskutieren, rechnergestützt Englischvokabeln lernen und eigenständig die neue Rechtschreibung trainieren, am Monitor physikalische Experimente simulieren sowie den Aufbau der DNA nachvollziehen, mit ihrer ausländischen Partnerschule Kontakt über E-Mail pflegen und im Kunstunterricht virtuell durch die Uffizien spazieren.
Grundsätzlich ist die Nutzung aller schulintern erlaubten Internetdienste im Rahmen des Unterrichts zulässig; maßgeblich sind im konkreten Fall allerdings die Anweisungen der unterrichtenden Lehrkraft, die für die Schülerinnen und Schüler

verbindlich sind. Die Lehrkräfte haben die Einhaltung ihrer Anweisungen zu kontrollieren.

Im Unterricht können Lehrkräfte Einsicht in die Netzaktivitäten der Schülerinnen und Schüler nehmen. Die E-Mail-Kommunikation im Rahmen des Unterrichts liegt in aller Regel in der Verantwortung der Lehrkraft. Allerdings reicht ihre Verantwortung nur so weit, wie ihre Aufsichtspflicht geht und sie Kenntnis von dem E-Mail-Verkehr haben kann. Es besteht weder eine flächendeckende Überwachungspflicht noch ein generelles Überwachungsrecht. Jede Kontrolle der Kommunikation muss für die Schülerinnen und Schüler transparent sein.
Der Lehrkraft obliegt es auch, die Einhaltung der Datenschutzregelungen im Rahmen des Unterrichts sicherzustellen.

Wird im Fremdsprachenunterricht mit der ausländischen Partnerschule kommuniziert, darf grundsätzlich die Übermittlung personenbezogener Daten zugelassen werden, soweit diese für die unterrichtsbezogene Kommunikation notwendig sind. Nur mit wirksamer Einwilligung der Betroffenen können weitere Daten mitgeteilt werden, wenn beispielsweise Angaben zu Austauschschülerinnen und Austauschschüler an die Partnerschulen übermittelt werden sollen.
Die E-Mail-Adresse ist so zu gestalten, dass sie eine Zuordnung der Nachricht zur Schule und zur Klasse erkennen lässt und damit deutlich macht, dass die Mails nicht ausschließlich privater Natur sind. Die Schülerinnen und Schüler können E-Mails unter einer Sammelkennung, zum Beispiel Klasse8a@Beispielschule.de, versenden. Sie dürfen diese Nachrichten auch verschlüsselt übermitteln, soweit die Lehrkraft von den Mitteilungen zuvor Kenntnis genommen hat. Offene E-Mails können nach Entscheidung der Absendenden namentlich oder pseudonym geschickt werden. Die Empfängerinnen beziehungsweise der Empfänger müssen erkennen können, dass die Nachricht einem größeren Kreis und nicht nur einer bestimmten Person zuzuordnen ist, damit sie sich bei der Antwort darauf einstellen können, dass auch diese von einem größeren Kreis gelesen werden kann. Der Empfang der E-Mails an die im Unterricht benutzte Box geschieht immer offen, sodass die Nachrichten auch von der Lehrkraft gelesen werden können.

Neben einer Kontrolle durch die verantwortliche Lehrkraft kann im Übrigen eine weitere Kontrolle, auch der Lehrkraft selbst, stattfinden. So protokolliert das System automatisch die während der Nutzung durchgeführten Tätigkeiten im System.
Eine uneingeschränkte Nutzung dieser Protokolldaten zu Kontrollzwecken wäre unverhältnismäßig und somit unzulässig.

Eine gezielte Kontrolle sollte nur erfolgen, wenn dafür ein Anlass gegeben ist. Eine allgemeine, ungezielte Kontrolle durch den Systemverwalter könnte zum Beispiel stichprobenartig, nicht auf einzelne Nutzerinnen und Nutzer bezogen die häufig aufgerufenen Internetangebote ermitteln. Eine Auswertung der Protokolldateien könnte auch daraufhin vorgenommen werden, welche Seiten ohne Bezug auf Unterricht oder Schule besonders häufig besucht werden. Ergeben sich dabei Auffälligkeiten über unzulässige Nutzungen, sollten die Beteiligten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hingewiesen werden. Gleichzeitig sollte angekündigt werden, dass bei Fortdauer der Verstöße eine personalisierte Kontrolle stattfinden wird. Fördert eine spätere Stichprobe tatsächlich weitere Zuwiderhandlungen gegen die Nutzungsordnung zutage, kann festgestellt werden, von welchem Rechner aus zu welcher Zeit solche Zugriffe stattgefunden haben.

In jedem Fall muss für die Betroffenen bereits vorher transparent sein, welche Kontrollmaßnahmen vorgesehen sind. Hierzu sollte eine konkrete Festlegung in der Nutzungsordnung erfolgen, welche Protokolldaten werden wo und wie lange gespeichert, wer darf sie wann nutzen).

3. Internetnutzung außerhalb des Unterrichts in der Schule

Immer mehr Lehrkräfte und Schülerinnen und Schüler möchten in der Schule auch nach Unterrichtsschluss und in den Freistunden unbeschränkt im Internet surfen, chatten und mailen dürfen. Die einen brauchen noch Material zur Unterrichtsvorbereitung, wollen einen Blick auf die Börsen der Welt werfen oder nachschauen, wann ihr Bus nach Hause fährt, die anderen ein Referat vorbereiten, die neuesten Bundesligaergebnisse abfragen oder in Sozialen Netzwerken kommunizieren. Die Schülerzeitungsredaktion tagt selbstverständlich außerhalb des Unterrichts und möchte die neueste Ausgabe auch im Internet veröffentlichen. Private E-Mails, von denen niemand in der Schule Kenntnis nehmen soll, werden in der großen Pause noch schnell verschickt, bevor die nächste Stunde beginnt.

3.1 Grundsatzentscheidung und Verantwortlichkeit

Die Entscheidung darüber, ob und in welchem Umfang der Lehrkraft und Schülerinnen und Schülern oder anderen Personen die Nutzung des Internets auch zu privaten Zwecken außerhalb des Unterrichts gestattet sein soll, obliegt der Schule beziehungsweise der Schulkonferenz. Die Entscheidung sollte jedoch vorab grundlegend diskutiert, sorgfältig abgewogen und in der Nutzungsordnung der Schule festgeschrieben werden, da sie weitreichende rechtliche Folgen und damit eine Reihe von Pflichten für die Schule auslöst.

Wenn eine Schule die Internetnutzung und E-Mail-Nutzung auch für private Zwecke zulassen will, unterliegt die private Telekommunikation am Lehrerplatz beziehungsweise am Internetrechner der Schule dem Fernmeldegeheimnis. Das Fernmeldegeheimnis ist durch Artikel 10 Grundgesetz (GG) und § 88 Absatz 1 Telekommunikationsgesetz (TKG) geschützt. Relevant wird dies zum Beispiel für die Frage, ob die Schule Lehrerinnen und Lehrer sowie Schülerinnen und Schüler oder den anderen Personen den privaten E-Mail-Verkehr gestatten möchte. Das Fernmeldegeheimnis umfasst den Inhalt der Telekommunikation und die näheren Umstände der Telekommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Wenn die private Internetnutzung in der Schule erlaubt ist, darf damit grundsätzlich niemand den privaten E-Mail-Verkehr der Lehrerinnen und Lehrer beziehungsweise der Schülerinnen und Schüler überwachen. Dagegen unterliegen dienstliche E-Mails der Schulleitung oder unterrichtliche E-Mails nicht dem Fernmeldegeheimnis.

Die Schule darf aus Sicherheitsgründen alle eingehenden und ausgehenden E-Mails auf Virenbefall automatisiert kontrollieren, allerdings ohne den Inhalt selbst zu sichten. Vorgesetzte dürfen nicht auf die an die Lehrerinnen und Lehrer gerichteten privaten E-Mails inhaltlich zugreifen und diese lesen. Sie dürfen nicht kontrollieren, wer eine private Nachricht an wen versendet oder von wem bekommen hat. Da dies jedoch einer eingehenden E-Mail nicht ohne Weiteres angesehen werden kann, ist

bei zugelassener privater Nutzung die gesamte Telekommunikation als private Nutzung anzusehen.

Auch die freie E-Mail-Kommunikation der Schülerinnen und Schüler außerhalb des Unterrichts in der Schule unterliegt dem Fernmeldegeheimnis und ist deshalb einer Kontrolle entzogen. Eine Kontrollbefugnis der Schule lässt sich nicht aus der Aufsichtspflicht nach Erziehungsauftrag herleiten, da diese Pflicht nur so weit reicht, wie Lehrkräfte Kenntnis von E-Mail-Nachrichten nehmen dürfen. Wegen des Fernmeldegeheimnisses sind sie dazu bei privaten Mails nicht befugt. Hat die Schule den Verdacht, dass private E-Mails mit strafrechtlich relevantem Inhalt versandt werden oder erlangt sie gar positive Kenntnis von einer strafrechtlich relevanten Kommunikation, bleibt, neben der schulinternen Maßnahme eines (vorläufigen) Ausschlusses von der Nutzung, nur der Weg, Strafanzeige zu erstatten. Wenn die Schule den privaten Gebrauch des Internets außerhalb des Unterrichts erlaubt, ist sie insoweit Diensteanbieter im Sinne des Telemedienrechts (§ 1 TMG).

Deshalb hat sie Pflichtungen nach §§ 5, 6 und 13 TMG zu erfüllen. Dazu gehören unter anderem Hinweispflichten und Unterrichtungspflichten sowie die Verpflichtung, allen berechtigten Nutzerinnen und Nutzer auf deren Verlangen hin Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen.

Fraglich ist, ob und inwieweit die Schule darüber hinaus für das Nutzungsverhalten ihrer Schülerinnen und Schüler oder sonstigen Nutzer im Internet verantwortlich ist. Die medienrechtliche Verantwortung als Diensteanbieter ist grundsätzlich in den §§ 7-10 TMG geregelt. Für eigene Informationen/Inhalte ist sie voll verantwortlich (§ 7 TMG). Für fremde Informationen/Inhalte, die sie im eigenen Netz übermittelt oder zu denen sie den Zugang vermittelt oder die sie temporär zwischenspeichert, ist sie nur unter bestimmten Bedingungen (mit-) verantwortlich (§§ 8-10 TMG).

Auch wenn sie für die fremden Informationen/Inhalte nur eingeschränkt verantwortlich ist, wird jede Schule doch bestrebt sein zu verhindern, dass ihre Schülerinnen und Schüler oder sonstigen Nutzer beispielsweise sexistische, gewaltverherrlichende oder diskriminierende Webseiten aufrufen. Bloße Verbote und Hinweise auf die schulrechtliche oder gar strafrechtliche Relevanz des verbotswidrigen Verhaltens dürften allein nicht ausreichen. Einen gewissen, wenn auch nicht umfassenden, Schutz vermögen Filterprogramme zu schaffen, mit denen der Zugriff auf bestimmte Arten von Angeboten im Internet über den Schulserver zumindest erschwert wird. Außerdem können Adressen von Angeboten mit unerwünschtem Inhalt in eine Sperrliste eingetragen werden, wodurch der direkte Zugriff unterbunden wird.

3.2 Zugangskontrollen und Nutzungsprotokollierung

Einige Schulen legen in Computerräumen und Medienecken Listen aus, in die sich die Benutzerinnen und Benutzer der Computer mit Namen und weitere Angaben eintragen sollen. Mit solchen Listen werden Daten erhoben und zugleich, wegen der offenen Auslegung, an alle Personen, die Zugang zu diesen Räumlichkeiten haben, bekannt gegeben. Eine solche Datenverarbeitung ist aber nur zulässig, wenn sie zur Aufgabenerfüllung der Schule geeignet und erforderlich ist. Unabhängig davon, dass die Schule grundsätzlich befugt ist, sich vor missbräuchlicher Nutzung ihrer Rechner zu schützen, müssen alle organisatorischen Kontrollmaßnahmen ebenfalls den

datenschutzrechtlichen Anforderungen genügen. Zweifelhaft ist aber bereits, ob die Eintragung in offen ausliegende Benutzungslisten überhaupt geeignet ist, um zum Beispiel Beschädigungen am Computer zu verhindern, weil die eingetragenen Benutzerinnen und Benutzer nicht notwendigerweise auch die Beschädigung hervorgerufen haben müssen. Ohne eine zusätzliche (Stichproben-)Kontrolle durch Lehrkräfte oder andere Personen dürfte das Problem der Verhinderung von Beschädigungen nicht wirklich lösbar sein.

Ausgelegte Benutzungslisten sollten daher aus dem Verkehr gezogen und eine datenschutzgerechtere Maßnahme getroffen werden.

Empfehlenswert ist die Einrichtung einer Zugangskontrolle, mit der automatisch der Rechnerzugang protokolliert werden kann, zum Beispiel durch Betriebssystem oder mit zusätzlicher Sicherheitssoftware. Der Zugang zum System ist so nur über einen Benutzernamen und die Eingabe eines individuellen Passwortes möglich. Das Passwort sollte so gestaltet sein, dass es nicht ohne Weiteres ausgeforscht und von anderen verwandt werden kann.

Bei der Protokollierung sind die Grundsätze der Datensparsamkeit und der Zweckbindung zu beachten. Das bedeutet, dass die Protokollierung auf ein Mindestmaß zu reduzieren ist.

Die Auswertung der Protokolle sollte durch die Systemverwaltung erfolgen. Protokollinhalt, das Verfahren der Auswertung sowie die Aufbewahrungsdauer der Protokolle sollten in der Nutzungsordnung festgelegt werden.

Die Protokolle der Internetnutzung sind im normalen Alltagsbetrieb auf URL-Hitlisten zu beschränken. In diesen Hitlisten werden lediglich die aufgerufenen URLs, das Datum und die Anzahl der Aufrufe aufgeführt. Die IP-Adresse des Schulrechners darf dabei nicht protokolliert werden.

In einigen Fällen lässt sich bei den eingesetzten Technologien und Softwareversionen nicht selektieren, was protokolliert wird. In diesem Fall sind die anfallenden Protokollrohdaten zeitnah (mindestens alle sechs Stunden) zu ihrer Entstehung durch geeignete Maßnahmen, zum Beispiel durch zeitgesteuert ablaufende Skripte, auf URL-Hitlisten in der oben beschriebenen Form zu reduzieren. Überschüssige Daten sind durch das Skript zu löschen.

Liefern die URL Hitlisten einen Verdachtsfall über eine auffällig unzulässige Nutzung des Internets, zum Beispiel Herunterladen rechtswidriger Inhalte, kann anlassbezogen eine weitergehende Protokollierung durchgeführt werden. Diese umfangreichere Protokollierung oder Protokollauswertung ist durch die Schulleitung unter Beteiligung des behördlichen Datenschutzbeauftragten vorher zu beschließen und darf nur zeitlich begrenzt vorgenommen werden. Zu Beginn der Protokollierung ist bereits festzulegen, über welchen, möglichst kurzen, Zeitraum protokolliert wird. Unverzüglich nach Abschluss dieser Maßnahmen sind die Betroffenen darüber zu unterrichten. Auch dieses Vorgehen ist in der Nutzungsordnung festzulegen.

Insgesamt sind alle Protokolle und URL-Hitlisten zeitnah auszuwerten und soweit unauffällig zu löschen.

4. Die schuleigene Homepage

Immer mehr Schulen präsentieren sich mit einer eigenen Homepage im Netz. Zu wenig bekannt sind allerdings oft die datenschutzrechtlichen Anforderungen, die sich aus den sogenannten Multimediaregelungen, aber auch aus sonstigen bereichsspezifischen Vorschriften und dem allgemeinen Datenschutzrecht ergeben. Anfragen haben häufig folgende Probleme zum Gegenstand:

- Welche personenbezogenen beziehungsweise personenbeziehbaren Daten dürfen unter welchen Voraussetzungen in die Homepage aufgenommen, und damit ins Netz eingestellt werden?
- Welche Informationspflichten obliegen der Schule als Anbieterin?
- Verantwortlich für die schuleigene Homepage und damit auch für die Einhaltung der datenschutzrechtlichen Bestimmungen ist grundsätzlich die Schulleitung oder die von ihr autorisierte Lehrkraft.

4.1 Inhaltsdaten: Was darf ins Internet?

4.1.1 Grundsätzliches

Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene Benutzergruppe durch zum Beispiel einen mit Passwort geschützten Zugang gebildet wird, bewirkt dies immer auch eine weltweite Veröffentlichung von Informationen, die von jeder Person mit Internetanschluss aufgerufen und grundsätzlich auch auf den eigenen Rechner heruntergeladen, verändert und genutzt werden können. Deshalb ist besonders sorgfältig zu prüfen, ob die Veröffentlichung personenbezogener Daten auf einer Schulhomepage datenschutzrechtlich zulässig ist.

Diese Zulässigkeit bestimmt sich nach den allgemeinen und bereichsspezifischen Datenschutzbestimmungen, zum Beispiel Bremisches Schuldatenschutzgesetz (BremSchulDSG) und das Bremisches Datenschutzgesetz (BremDSG) mit seinem Verweis auf das Bremische Beamtengesetz (BremBG). Daraus ergibt sich Folgendes:

- Sachdarstellungen ohne Personenbezug sind im Rahmen einer Selbstdarstellung und Präsentation der Schule im Internet unproblematisch. Gleiches gilt für die Darstellung interner Gliederungspläne und Organisationspläne, für Telefonverzeichnisse sowie sonstige Informationen ohne Personenbezug. Für Stundenpläne und Vertretungspläne sowie Adresslisten der schulischen Gremien gelten wegen des Personenbezugs besondere Zulässigkeitsregeln.
- Gästebücher, innerhalb derer Dritte Mitteilungen für den allgemeinen Zugriff ablegen können, sollten besonders kritisch auf ihre Erforderlichkeit geprüft werden. Dem meist nur geringen Nutzen für die Aufgabenerfüllung der Schule oder die Attraktivität des Internetangebotes stehen neben dem laufenden Betreuungsaufwand und möglichen Haftungsfolgen auch Gefährdungen für das informationelle Selbstbestimmungsrecht der Gäste gegenüber. Auf die Risiken, die mit der Nutzung dieser Möglichkeit verbunden sind, sollte aufmerksam gemacht werden.

- Sofern die Schule die Möglichkeit der Kontaktaufnahme per E-Mail anbietet, sollten die elektronischen Briefe verschlüsselt verschickt werden können. Hierzu sollte die Schule auf ihrer Homepage einen (öffentlichen) Schlüssel bekannt geben, der von den Absendern einer Nachricht benutzt werden kann. Als Verschlüsselungsverfahren wird PGP (Pretty Good Privacy) empfohlen. Die Schule sollte sich im Übrigen der Gefahren bewusst sein, die mit der Benutzung dieses Dienstes verbunden sind. Außerdem müssten die Schulen interne Regelungen für die Entgegennahme und Behandlung von E-Mails schaffen.

4.1.2 Lehrerdaten im Internet

Für die Zulässigkeit der Darstellung und Präsentation von Daten von Lehrerinnen und Lehrer sowie Lehrmeister oder Referendarinnen oder Referendare im Internet durch öffentliche Schulen im Lande Bremen gelten § 1 und § 2 Absatz 7 BremSchulDSG in Verbindung mit § 20 BremDSG mit Verweis auf §§ 85 folgende Paragrafen BremBG.

Öffentliche Schulen dürfen Daten von Lehrerinnen und Lehrern nur verarbeiten, soweit es zur Erfüllung ihres Unterrichtsauftrages und Erziehungsauftrages und zur Wahrnehmung gesetzlicher Mitwirkungsrechte erforderlich ist (Zweckbindungsgebot und Erforderlichkeitsprinzip). Die Zulässigkeit der Lehrerdatenverarbeitung selbst richtet sich nach den Regelungen des § 20 BremDSG. Danach dürfen öffentliche Stellen personenbezogene Daten über Bewerber, Bedienstete und ehemalige Bedienstete nur nach Maßgabe der §§ 85 folgende Paragrafen BremBG verarbeiten. Die Verarbeitung dieser Daten in automatisierten Verfahren bedarf der Zustimmung der obersten Dienstbehörde.

Als Verarbeitungszwecke werden in § 85 BremBG genannt: Begründung, Beendigung oder Abwicklung des Dienstverhältnisses; Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch Personalplanung und Personaleinsatz. Dem Erforderlichkeitsprinzip werden hier zusätzlich noch die schutzwürdigen Belange der Betroffenen gegenübergestellt. Gemäß § 92 BremBG dürfen Personalaktendaten in automatisierten Verfahren nur für die genannten Zwecke verarbeitet werden. Ihre Übermittlung ist nur nach Maßgabe des § 89 BremBG zulässig. Ein automatisierter Datenabruf, Internetabruf und Intranetabruf, durch andere Behörden und damit besonders auch private Stellen, ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. Nach § 92 BremBG ist dem Beamten bei erstmaliger Speicherung die Art der über ihn gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er zu benachrichtigen. Auskünfte an Dritte, zum Beispiel die Bereitstellung von Lehrerdaten im Internet, dürfen nach § 93 BremBG nur mit Einwilligung der Beamtin beziehungsweise des Beamten erteilt werden, es sei denn, es liegen bestimmte Ausnahmen vor wie zum Beispiel Beeinträchtigung des Gemeinwohls, der Schutz berechtigter höherrangiger Interessen des Dritten. Inhalt und Empfänger der Auskunft sind der Beamtin oder dem Beamten schriftlich mitzuteilen.

Für die Präsentation von Lehrerinnendaten beziehungsweise Lehrerdaten im Internet bedeutet dies:

- Die Präsentation von Lehrkräftedaten im Internet einschließlich eventueller Texte, Beschreibungen, Bilder oder Fotos ist nur mit ausdrücklicher schriftlicher Einwilligung der Betroffenen zulässig. Hierbei gelten das Zweckbindungsgebot, rein schulischer Zweck und das Erforderlichkeitsprinzip, nur die zur Zweckerfüllung notwendigen Daten. Die schutzwürdigen Belange der Betroffenen sind trotz Einwilligung zu berücksichtigen. Die Internetpräsentation ist auch bei Einwilligung auf rein schulische Daten beschränkt.
- Bei Repräsentanten der Schule, zum Beispiel durch Schulleitung oder Vertretung und bei für die Außendarstellung der Schule wichtigen Funktionsträgern sind das Zweckbindungsgebot und das Erforderlichkeitsprinzip anders einzuschätzen als bei den übrigen Lehrkräften. Das prinzipielle Einwilligungserfordernis könnte hier durch das Ausnahmekriterium "Schutz berechtigter höherrangiger Interessen der Öffentlichkeit" ersetzt werden. Zulässig für eine Präsentation im Internet wären danach dann der Name, die dienstliche Funktion, die dienstliche Anschrift und Angaben zur dienstlichen Erreichbarkeit, wie zum Beispiel dienstliche Telefonnummer, E-Mail oder Ähnliches.
- Die oberste Dienstbehörde muss der Präsentation von Lehrerkräftedaten im Internet zustimmen. Bei der erstmaligen Speicherung der Daten, Einstellung ins Internet, ist den Betroffenen die Art der Daten mitzuteilen, bei wesentlichen Datenänderungen sind sie zu benachrichtigen. Im Übrigen haben die Betroffenen die nach dem BremDSG üblichen Betroffenenrechte (Auskunft, Sperrung, Löschung, Berichtigung, Widerspruch).
- Für die Zulässigkeit der Darstellung und Präsentation von Daten des übrigen Schulpersonals wie zum Beispiel Hausmeisterinnen, Hausmeister, Sekretärinnen und Sekretäre, sonstige Beschäftigte gelten analoge Regelungen (§ 20 BremDSG mit Verweis auf §§ 85 folgende Paragrafen BremBG). Die Einstellung von Daten, Texten, Bildern oder Fotos ist nur mit ausdrücklicher schriftlicher Einwilligung zulässig. Sie ist im Einwilligungsfall beschränkt auf die rein dienstlichen Funktionen. Diese Personengruppen haben für die Außenrepräsentation der Schule allerdings keine Bedeutung, sondern nur rein interne Funktionen.

4.1.3 Schülerdaten und Elterndaten im Internet

Für die Zulässigkeit der Darstellung und Präsentation von Schülerdaten und Elterndaten im Internet gilt das BremSchulDSG. Auch hier gelten das Zweckbindungsgebot und das Erforderlichkeitsprinzip des § 1 Absatz 1 BremSchulDSG: Erfüllung des Unterrichtsauftrages und Erziehungsauftrages der Schule sowie Wahrnehmung der gesetzlichen Mitwirkungsrechte. Bestimmte Schülerdaten, zum Beispiel die Bewertung von Leistungskontrollen, persönliche Notizen des Lehrers über Schüler, Klassenbucheintragungen gelten dabei nicht als Daten im Sinne des BremSchulDSG; für sie gelten aber das Verarbeitungsverbot des § 3 Absatz 2 BremSchulDSG (keine Verarbeitung auf privatem Rechner oder auf Rechnern außerhalb der Schule), die Übermittlungsbestimmungen des BremSchulDSG (§§ 5 bis 10) und die besondere Sorgfaltsverpflichtung nach § 1 Absatz 5 BremSchulDSG.

Für die Darstellung und Präsentation von Schülerdaten und Elterndaten im Internet durch bremische Schulen bedeutet dies:

- Die Darstellung und Präsentation von Schülerdaten und Elterndaten einschließlich etwaiger Texte, Beschreibungen, Bilder beziehungsweise Fotos im Internet (Datenübermittlung!) ist nicht zulässig, auch nicht mit Einwilligung der Schüler beziehungsweise ihrer Erziehungsberechtigten. Die Übermittlung ist zur Erreichung des schulischen Zwecks nicht erforderlich. Die Übermittlungstatbestände der §§ 5 bis 10 BremSchulDSG liegen nicht vor. Eine fehlende Einwilligung kann wegen des fehlenden schulischen Zwecks auch nicht von der Schulleitung ersetzt werden (§ 4 Absatz 2 und 3 BremSchulDSG).
- Auch Name, Funktion und schulische Erreichbarkeit der Elternvertretung der Schule (nicht Klassenvertretung!) dürften nur mit Einwilligung der Betroffenen ins Internet gestellt werden. Die Schülervertretung der Schule darf nicht (auch nicht bei Einwilligung) in das Internet eingestellt werden; das BremSchulDSG enthält zur Übermittlung von Schülerinnendaten und Schülerdaten durch die Schulen eine abschließende Regelung. Es wäre allenfalls zulässig, wenn die Gesamtvertretung der Schülerschaft mit Einwilligung der Betroffenen sich im Internet präsentiert.

4.1.4 Schülerzeitungen und Klassenzeitungen im Internet

Für die Einstellung von Schülerzeitungen und Klassenzeitungen ins Internet gilt Folgendes:

Ausgangspunkt ist zunächst § 51 Bremisches Schulgesetz (BremSchulG) mit seinem Verweis auf das Bremische Pressegesetz. Gemeint sind periodische Publikationen, nicht Ad-hoc Berichte über schulische oder klassenbezogene Veranstaltungen und Ereignisse, die von einzelnen Schülerinnen und Schülern oder Schülergruppen erstellt und publiziert werden, zum Beispiel Berichte über einen Klassenausflug, ein Schulfest, das Abitur samt Abiturzeitung. Derartige Ad-hoc Berichte entstehen zwar im Verantwortungsbereich der Verfasser (Meinungsfreiheit), da sie aber auf der Homepage der Schule erscheinen, trifft die Schule letztlich die Verantwortung. Sie ist für die Einhaltung der datenschutzrechtlichen Normen verantwortlich.

Herausgeber von Schülerzeitungen oder Klassenzeitungen sind nach § 51 BremSchulG die Schüler; die Schulen sind hier nicht in der Verantwortung. Ihr Vertrieb ist in den Schulen zulässig, das heißt, es ist keine Zulassung, keine Genehmigung oder Ähnliches erforderlich. Allerdings muss mit Beginn des Zeitungsvertriebs ein Belegexemplar an die Schulleitung gehen. Es besteht eine Impressumspflicht (Schülerinnen beziehungsweise Schüler in Verbindung zu ihrer Schule). Im Übrigen gilt das Bremische Pressegesetz mit weiteren Regelungen zum Beispiel zur Impressumspflicht, zur Sorgfaltspflicht und zum Gegendarstellungsrecht.

Die Vorschrift des § 51 BremSchulG regelt zudem, dass für andere von Schülerinnen und Schülern gestaltete oder herausgegebene Medien diese Bestimmungen entsprechend gelten. Die Regelungen des § 51 BremSchulG sind deshalb auch für Schülerzeitungen und Klassenzeitungen im Internet anwendbar. Hinzu kommen hier die Regelungen des Rundfunkstaatsvertrags (RStV), speziell die §§ 6 - 10 sowie der dritte Abschnitt mit den besonderen Regelungen zum Datenschutz, wobei die verantwortliche Schülerin oder der verantwortliche Schüler als Herausgeber gelten und hier den Anbieterstatus einnehmen. Damit müssen sie auch die im RStV für den Anbieter geltenden Pflichten übernehmen.

Für die namentliche Nennung von Schülerinnen und Schülern, Lehrkräften eventuell Eltern und/oder deren bildliche Präsentation, Standbilder oder Bewegbilder, in Schülerzeitungen und Klassenzeitungen kann man grundsätzlich wohl mit der Einwilligungslösung arbeiten, das heißt, die betroffenen Personen erklären sich schriftlich mit der Namensnennung oder bildlichen Darstellung einverstanden.

Das Einspielen von personenbezogenen Webcam-Informationen in eine von Schülerinnen und Schülern zu verantwortende Internetpublikation muss generell von der schriftlichen Einwilligung der betroffenen Personen abhängig gemacht werden.

Fazit

Schülerzeitungen und Klassenzeitungen im Internet sind grundsätzlich zulässig. Verantwortlich sind die herausgebenden Schülerinnen und Schüler, nicht die Schule. Allerdings besteht eine Informationspflicht gegenüber der Schulleitung bei jeder neuen Internetpublikation ("Belegexemplar"). Zudem besteht eine Impressumspflicht.

Im Hinblick auf die allgemeine Verfügbarkeit des Mediums und seine besonderen Datenschutzprobleme und Datensicherungsprobleme kommt den Sicherheitsverpflichtungen und Sorgfaltsverpflichtungen eine hervorgehobene Bedeutung zu. Gegendarstellungsrecht betroffener "schulöffentlicher" Personen. Im Übrigen gilt das Einwilligungserfordernis bei Namensnennung und bildlichen Darstellungen. Bei Einspielungen von Webcaminformationen mit Personenbezug gilt stets das Einwilligungserfordernis.

Um die beiden Verantwortungsbereiche deutlich zu trennen, empfiehlt sich eine eigene Homepage für die Schülerzeitungen und Klassenzeitung mit einem eigenen Domainnamen.

4.1.5 Beiträge und Berichte von Schülerinnen und Schüler über schulische oder klassenbezogene Veranstaltungen, Schülerhomepages beziehungsweise lehrereigene Homepages

Da die Schulleitung oder die von ihr beauftragte Lehrkraft für die Homepage der Schule verantwortlich ist, ist es insoweit gerechtfertigt, die Veröffentlichung von Beiträgen der Schülerinnen und Schüler grundsätzlich von einer vorherigen Genehmigung der beziehungsweise des Verantwortlichen abhängig zu machen. Eine solche Genehmigungspflicht kann in der Nutzungsordnung festgeschrieben werden. Ausnahmen gelten dabei für eventuell zugelassene Gästebücher oder schwarze Bretter, in die die Schülerinnen und Schüler selbst und ohne gesonderte Genehmigung Eintragungen vornehmen dürfen. Die Schülerinnen und Schüler können dabei frei wählen, ob sie mit ihren Namen oder mit Pseudonymen auftreten wollen.

Die Einstellung von schülereigenen beziehungsweise lehrereigenen Homepages auf den Schulservern oder entsprechender Darstellungen in der Homepage der Schule sollte, sofern überhaupt zugelassen, in der Nutzungsordnung der Schule geregelt werden. Da es sich hierbei um eine reine Privatangelegenheit handelt, die nichts mit Schule zu tun hat, wird aus Datenschutzsicht eine Verbotslösung favorisiert.

4.1.6 Gästebuch, schwarzes Brett und Kontaktlisten

Homepages erfüllen nicht nur einen Informationszweck, sondern bieten sich auch für eine direkte Kommunikation an. So gibt es etwa "Gästebücher", in die Besucherinnen und Besucher einer Seite sich selbst und ihre Meinung zu bestimmten Fragen eintragen können. Oder Personen, die an spezifischen Fragestellungen interessiert sind, soll über das Netz Gelegenheit gegeben werden, mit anderen Interessierten Kontakt aufzunehmen, wofür entsprechende Listen veröffentlicht werden sollen.

Gästebücher auf der Homepage oder andere elektronische Meinungsäußerungsforen erfüllen dieselbe Funktion wie etwa ein "schwarzes Brett", das in der Schule im Eingangsbereich aushängt. Wer möchte, kann unter vollem Namen, aber auch anonym oder pseudonym Kommentare abgeben, zu welchem Thema auch immer.

Ob jedoch solche Kommentare tatsächlich von der bezeichneten Person stammen und ob auch der dokumentierte Inhalt so von ihr gewollt ist, lässt sich sowohl bei realen als auch bei virtuellen schwarzen Brettern zurzeit nur mit einem Aufwand überprüfen und sicherstellen, der die Idee der spontanen Meinungsäußerung, erst recht, wenn sie auch anonym möglich sein soll, in ihr Gegenteil verkehrt.

Den Schulen kann daher nur empfohlen werden, den Nutzerinnen und Nutzern diese Umstände mit einer ausführlichen Information ins Bewusstsein rufen. Eine Art Warnhinweis sollte deutlich machen, dass keine Gewähr für die Richtigkeit der zu findenden Angaben übernommen werden. Weiter sollte darüber informiert werden, dass die Schule strafrechtlich relevante Meinungsäußerungsinhalte nicht zulässt. Da sie dies in eigener Verantwortung sicherzustellen hat, muss sie neue Einträge unverzüglich unter strafrechtlichen Aspekten prüfen. In der Nutzungsordnung der Schule wäre etwa zu bestimmen, dass der Beitrag gelöscht, die Teilnehmende oder der Teilnehmende, sofern ermittelbar, ausgeschlossen oder etwa das Gästebuch insgesamt geschlossen werden kann.

Davon zu unterscheiden sind die Fälle, in denen es darum geht, Kommunikationswilligen durch das Bereithalten von Institutionenlisten und Personenlisten zu bestimmten inhaltlichen Fragestellungen eine direkte Kontaktaufnahme untereinander zu ermöglichen. Das Anliegen ist sicherlich hilfreich, ausgeschlossen sein muss jedoch, dass Personen ungewollt oder sogar ohne ihr Wissen von Dritten in solche Listen eingetragen werden. Ohne die wirksame Einwilligung der Betroffenen oder des Betroffenen beziehungsweise einer erziehungsberechtigten Person (vergleiche 4.1.1) ist die Aufnahme personenbezogener Daten in eine solche elektronische Liste unzulässig.

4.1.7 Webcams

Es wird immer häufiger üblich, Kameras in öffentlichen und privaten Bereichen aufzustellen und deren Bilder im Internet abrufbar zu speichern. Öffentliche Stellen dürfen dies allenfalls dann tun, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter, Autokennzeichen oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder

Bildbearbeitung seitens der Empfängerin beziehungsweise des Empfängers erkennbar gemacht werden können.

Infrage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen. Dabei spielen Rahmenbedingungen wie Bildausschnitt, Bildschärfe oder Bildfrequenz eine wichtige Rolle. Vorab sollte auf jeden Fall sorgfältig geprüft werden, ob die Informationen, die mittels Webcam gegeben werden sollen, nicht auf andere, datensparsamere Weise übermittelt werden können, zum Beispiel durch Fotos, auf denen Räume abgebildet sind, in denen sich keine Personen aufhalten.
Da die Bilder von Webcams weltweit abrufbar, speicherbar, aber vor allem auch veränderbar sind und damit ein erhöhtes Gefahrenpotential begründen, sollte der Einsatz von Webcams im Schulbereich grundsätzlich unterbleiben.

4.2 Informationspflichten als Anbieter

Transparenz ist eine wichtige Voraussetzung für den Schutz des Rechts auf informationelle Selbstbestimmung.
Nur wenn die Nutzerinnen und Nutzer auch im World Wide Web wissen, wann von wem welche personenbezogenen Daten erhoben, gespeichert, verarbeitet und genutzt werden, können sie ihr Recht auf informationelle Selbstbestimmung wahrnehmen. Wer die Homepage einer Schule aufsucht, um sich zu informieren oder mit der Schule zu kommunizieren, muss dementsprechend informiert werden.

Neben der Frage, welche Inhalte in eine Homepage eingestellt werden dürfen, sind auch datenschutzrechtliche Vorgaben für das Angebot von Informationsdiensten und Kommunikationsdiensten zu beachten.
Solche Vorgaben enthalten das Telemediengesetz (TMG) und der Rundfunkstaatsvertrag (RStV), je nachdem, ob der jeweilige Informationsdienst und Kommunikationsdienst als Telemediendienst für eine individuelle Nutzung von kombinierbaren Daten bestimmt ist oder ob er redaktionell gestaltete Beiträge enthält.

4.2.1 Allgemeine Informationspflichten, Anbieterkennzeichnung

Die bunte Webwelt ist bei genauem Hinsehen verwirrend. Die allgemeinen Informationspflichten der Diensteanbieter (§ 5 TMG) beziehungsweise die Anbieterkennzeichnung (§ 54 RStV) soll den Nutzerinnen und Nutzern ein Mindestmaß an Transparenz und Information ermöglichen. Nur mit ausreichenden Informationen über die jeweiligen Diensteanbieter ist es möglich, den eigenen datenschutzrechtlichen Auskunftsanspruch nach § 34 Bundesdatenschutzgesetz (BDSG) geltend zu machen. Auch die Datenschutzbeauftragten des Bundes und der Länder sind für eine effektive Kontrolle auf umfassende Informationen über die Anbieter angewiesen.

Während der Inhalt der allgemeinen Informationspflicht beziehungsweise die Anbieterkennzeichnung noch unmissverständlich normiert ist, fehlt es jedoch an einer Regelung der Präsentation. Sie ergibt sich allerdings aus dem Zweck einer derartigen Information: Sie ist so zu platzieren und auszugestalten, dass sie leicht auffindbar und gut lesbar ist.

Die Informationen über die Anbieterin beziehungsweise den Anbieter oder die Anbieterkennzeichnung haben zumindest auf einer Seite der Homepage alle geforderten Angaben zu enthalten.
Beim Aufrufen der Homepage sollte auf jeden Fall eine eindeutige Kurzbezeichnung (der Anbieterkennzeichnungsanker) und eine direkte Verweisung (Link) auf die vollständige Anbieterinformation vorhanden sein ("one click away").

Da im Internet nicht immer ein Einstieg über die Startseite der Homepage notwendig ist, ist zusätzlich zu gewährleisten, dass die Nutzerinnen und Nutzer auch von allen übrigen Seiten der Homepage direkt auf diejenige Seite gelangen können, von der aus auf die vollständige Anbieterinformation zugegriffen werden kann ("two clicks away"). Der Anbieterkennzeichnungsanker sollte ohne Schwierigkeiten gefunden werden können. Dabei sollte eine bekannte und als solche eindeutig erkennbare Anbieterkurzbezeichnung gewählt werden. Auch farblich sowie hinsichtlich der Schriftart und Schriftgröße sollte eine gute Erkennbarkeit und Lesbarkeit sichergestellt werden. Daher ist es empfehlenswert, dass starke Kontraste in Farbe und Linienführung gewählt werden. Die Anbieterinformation sollte zudem so ausgestaltet werden, dass sie problemfrei auszudrucken ist.

4.2.2 Anzeige der Weitervermittlung

Eine Weitervermittlung an Dritte, etwa zu Homepages anderer Schulen, mittels eines Links ist anzuzeigen. Auch hier steht der Gedanke der Transparenz im Vordergrund. Der Anzeige der Weitervermittlung kann beispielsweise durch einen unmissverständlichen Hinweis in Wortform Genüge getan werden oder durch Schaltung einer Zwischenseite, die auf die vermittelte Adresse hinweist und den Abbruch der Weiterschaltung ermöglicht.

Auch sollte jederzeit erkennbar sein, wer für die aufgerufene Seite verantwortlich ist. Es kann irreführend sein, wenn zum Beispiel der Rahmen (Frame) der Homepage einer Schule bei einer nicht erkennbaren Weitervermittlung noch vorhanden ist. Unter Umständen sind dann die Anbieterinnen und Anbieter der Homepage auch für den fremden Inhalt der Dritten oder des Dritten verantwortlich.

4.2.3 Unterrichtungspflichten

Damit Angebote für die Nutzerinnen und Nutzer schnell und unkompliziert abzurufen sind, werden oft sogenannte Cookies verwendet. Cookies sind Datensätze, die von Internetservern auf die Rechner der Nutzerinnen und Nutzer übermittelt werden und dort in einer Datei auf der Festplatte abgelegt werden. Mit Hilfe von Cookies können Informationen über die Verweildauer auf bestimmten Seiten, die Häufigkeit des Seitenaufrufs und dergleichen mehr ermittelt werden. Cookies dürfen, soweit sie personenbeziehbare Angaben ermitteln, nur mit Einwilligung der Nutzerinnen und Nutzer gesetzt werden.

Da bei Cookies die Verarbeitung personenbezogener Daten erst zu einem späteren Zeitpunkt als dem ersten Aufruf der Seite erfolgt, verlangt § 13 TMG, dass die Nutzerinnen und Nutzer zu Beginn des automatisierten Verfahrens, welches eine spätere Identifizierung der betroffenen Person ermöglicht und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereitet, zu unterrichten sind.

Auch Programme wie Active-X, JavaScript oder sonstige Plug-Ins können ebenso wie Cookies eine Nutzeridentifikation ermöglichen. Hier gelten die bereits im Zusammenhang mit Cookies beschriebenen Anforderungen.
Die genannten Programme stellen zusätzlich eine große Sicherheitsgefahr dar, da sie den Nutzerrechner bei unzureichender Sicherheitseinstellung ausspähen können. Des Weiteren können diese Programme Viren enthalten und sie auf dem Nutzerrechner ablegen.

4.2.4 Transparenz durch Datenschutzpolicy

Wer es mit dem informationellen Selbstbestimmungsrecht seiner Nutzerinnen und Nutzer ernst meint, sollte darüber hinaus Datenschutzhinweise (Datenschutzpolicy) an gut lesbarer Stelle geben. Damit wird offen gelegt, wie mit automatisch anfallenden Daten, den Spuren im Netz, umgegangen wird und ob Cookies oder aktive Inhalte verwendet werden. Sollen personenbezogene Daten erhoben werden, ist das nur aufgrund einer dies ausdrücklich erlaubenden Rechtsvorschrift zulässig oder wenn eine wirksame Einwilligung erteilt ist.

Auch wenn keine personenbezogenen Daten bei den Nutzerinnen und Nutzern erhoben werden, wird bei jeder Internetnutzung auf der Homepage zwangsläufig die IP-Adresse der Kommunikationsverbindung bekannt. Zwar ist es nicht so, dass diese Adresse immer personenbeziehbar ist, da im Regelfall Nutzerinnen und Nutzer über Accessprovider dynamische IP-Adressen zugeordnet werden. Aus Gründen der Transparenz empfiehlt es sich jedoch, darauf hinzuweisen, in welcher Form welche Datensätze gespeichert werden. Und schließlich rundet der Hinweis, dass auf Cookies und aktive Programme verzichtet wird, die Datenschutzpolicy ab.

4.2.5 Individuelle Informationspflichten - elektronische Auskunft

Das Recht, wissen zu können, wer was über die eigene Person weiß, ergibt sich aus dem allgemeinen Datenschutzrecht (Bundesdatenschutzgesetz-BDSG sowie Datenschutzgesetze der Länder). Die Betroffenen müssen die Unterlagen einsehen oder auf Wunsch auch elektronisch Auskunft erhalten können.

5.Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Jeder muss damit rechnen, beim Surfen beobachtet zu werden. Es wird erfasst, wer (welcher Rechner) das Internet wie nutzt, welche Seiten aufgerufen werden und wie lange. Diese Angaben reichen zwar noch nicht aus, um zu erkennen, wer den Rechner gerade nutzt. Eine Zuordnung ist aber unter Umständen später möglich, wenn bei anderer Nutzung die Identität der Nutzerin oder des Nutzers selbst preisgegeben wird.

Weiter sind die Knotenrechner und die Übertragungswege dieses weltweiten Netzes nicht bekannt. Welchen Weg eine E-Mail nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht vorher bestimmbar. Im Internet wird grundsätzlich den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen.

Ohne besondere Schutzmaßnahmen können sich Angreiferinnen und Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts der großen und wachsenden Zahl von Internetteilnehmerinnen und Internetteilnehmern auch die Zahl der potentiellen Angreiferinnen und Angreifer, die diese Sicherheitslücken ausnützen, signifikant ist. Diesem Risiko müssen die Schulen Rechnung tragen; dazu verpflichtet sie § 7 BremDSG.

Diese Pflicht kann bei einem Internet-Anschluss am Besten und Sichersten durch eine sogenannte Insellösung, also den Verzicht auf Vernetzung des Verwaltungsrechners der Schule mit den Rechnern, die ans Internet angeschlossen sind, realisiert werden. Es empfiehlt sich in jedem Falle eine strikte Trennung zwischen der für die Schulverwaltung notwendigen Verarbeitung von personenbezogenen Daten und dem Internetzugang. Webserver sollten sich auf jeden Fall außerhalb der lokalen Netze der Schulen befinden. Die auf dem Webserver gespeicherten Daten, das sind sowohl solche, die sich aus dem Webangebot selbst ergeben, als auch solche, die im Rahmen des normalen Unterrichts anfallen, sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu sichern.

Bei einem Zugang aus dem lokalen Netz der Schule in das Internet sowie zur Onlinepflege des Webservers empfiehlt sich der Einsatz einer Firewall zwischen dem lokalen Netz und dem Webserver. Idealerweise sollte der Webserver in einer DMZ (sogenannte "Demilitarisierte Zone") stehen. Zusätzlich sollte der Webserver selbst gegen Manipulationen aus dem Internet geschützt werden.

Grundsätzlich sollten nur die unbedingt erforderlichen Dienste und Protokolle aktiviert sein, die Schreibrechte sollten auf das unabdingbare Maß beschränkt werden und eine Anzeige der Verzeichnisstruktur nicht möglich sein.

Weitere Informationen zum Aufbau und zur Installation einer gesicherten Serverumgebung sind in der Orientierungshilfe "Datenschutz bei der Nutzung von Internet und Intranet" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder zu finden; erhältlich als Druckausgabe bei den Datenschutzbeauftragten des Bundes und der Länder. Beim Betreiben eigener Webserver sollte darüber hinaus auf Folgendes geachtet werden:

- Der direkte Zugriff auf Datenbanken der Schule sollte grundsätzlich verhindert werden. Soweit ein Datenbankzugriff erforderlich ist, sollten Kopien verwendet werden.
- Das Internetangebot ist durch geeignete Maßnahmen gegen unbefugte Manipulationen zu sichern. Hierzu gehören eine sichere Konfiguration der Rechteverwaltung und eine geeignete Protokollierung unerlaubter Zugriffe auf dem Webserver.
- Besonderes Augenmerk ist auf personenbezogene Daten zu richten, die durch die Nutzung entstehen. Sie müssen gegen den Zugriff über das Internet geschützt werden und sollten nur kurzfristig im Webserver gespeichert sein.
- Zusätzlich zur Firewall müssen Maßnahmen gegen schädliche Kommunikationsinhalte, wie zum Beispiel Computerviren, ActiveX-Programme

und Java-Programme sowie sonstige aktive Inhalte von Webseiten, getroffen werden.

6. Nutzungsordnung

6.1 Ziel und möglicher Weg einer Regelung

Für die schulische Internetwelt sind verbindliche Regeln erforderlich, die insbesondere Nutzungsumfang, Art und Weise der Nutzung und die Kontrolle von Missbrauch festlegen. Wie ein solches Regelwerk ausgestaltet wird, ist, im Rahmen der verbindlichen gesetzlichen Vorgaben, im Wesentlichen die Angelegenheit jeder einzelnen Schule. Die Schule hat die Möglichkeit, eine auf ihre Bedürfnisse zugeschnittene Nutzungsordnung als eigene Schulordnung zu erlassen. Um etwaigen Missverständnissen vorzubeugen, sei betont: Vorschriften einer Nutzungsordnung vermögen nicht die individuelle Einwilligung in die Verarbeitung personenbezogener Daten zu ersetzen, soweit diese erforderlich ist.

6.2 Gegenstand und Elemente

Auch wenn inzwischen viele Schulen über einen Internetzugang verfügen, ist die Ausstattung noch sehr unterschiedlich. In manchen Schulen ist nur ein Internetrechner im Lehrerzimmer aufgestellt, andere verfügen bereits über vernetzte Multimediaarbeitsplätze in den Klassenzimmern oder sogenannte Medienecken, die den Zugang zum Netz auch unabhängig vom Unterricht ermöglichen. Ziel, Art und Umfang des angestrebten Interneteinsatzes werden beispielsweise auch nach Schultyp und Alter der Schülerinnen und Schüler differieren.

In einer Nutzungsordnung sollte insbesondere Folgendes geregelt werden:

- Wer ist für die Systemadministration verantwortlich?
- Welche Internetdienste werden an der Schule zugelassen und welche Nutzungsrechte sollen Lehrkräfte, Schülerinnen, Schüler und gegebenenfalls auch die Erziehungsberechtigten haben? Hierzu gehört neben der Festlegung der zugangsberechtigten Personengruppen, der zulässigen Nutzungsarten und des Nutzungsumfangs auch eine Regelung über die Vergabe der Nutzungsrechte, deren Kriterien und die Verwaltung der Nutzungsberechtigungen.
- In welchem Rahmen und Maß sollen die Lehrkräfte weisungsbefugt sein? Diesbezüglich ist vor allem zwischen der Nutzung des Internets innerhalb und außerhalb des Unterrichts zu unterscheiden.
- Welche Lehrkraft ist für die Homepage verantwortlich? Soll die Veröffentlichung eines Beitrags von Schülerinnen und Schülern (mit Ausnahme der Schülerzeitung) genehmigungspflichtig sein?
- Welche Daten dürfen zu welchem Zweck im Rahmen schulbezogenen oder unterrichtsbezogener Internetnutzungen protokolliert werden, wer darf die Protokolldatei einsehen, auf Verlaufsdateien oder andere temporäre Internetdateien zugreifen und wann sind die Protokolldaten von wem zu löschen?
- Welche Verstöße gegen Nutzungsregeln werden mit welchen Maßnahmen geahndet und welche Kontrollen werden in diesem Zusammenhang von wem durchgeführt? Außerdem sollte über die Verfahrensweise bei strafrechtlich

relevantem Beschaffen oder Verbreiten von Informationen belehrt (Anzeige), insbesondere aber auch die schulischen Konsequenzen für die Nutzerinnen und Nutzern festgelegt werden (Löschung der Nachricht, Sperrung der oder Ausschluss von der Nutzung).

Einem höheren Maß an Klarheit könnte es dienen, in die Nutzungsordnung auch (deklaratorische) Hinweise auf medienrechtliche Bestimmungen und deren datenschutzrechtliche Grundsätze aufzunehmen, etwa dass das Fernmeldegeheimnis zu beachten ist und dass Kontrollen zur Feststellung von unerlaubten Nutzungen außerhalb des Unterrichts nur mit Kenntnis der Betroffenen und nur bei konkreten Anhaltspunkten oder stichprobenartig durchgeführt werden dürfen.

7. Begriffserklärungen

Account

heißt übersetzt Konto. Gemeint ist ganz allgemein der Zugang zum Internet oder sonstigen Netzen. Ein Account beinhaltet immer einen Usernamen, ein Passwort und natürlich bestimmte Nutzungsbedingungen.

Active -X, Java, JavaScript, Plug-Ins

Active-X-Controls, Java-Applets und JavaScripts sind Programme, die beim Aufrufen von Angeboten auf den Rechner des Nutzers heruntergeladen und dort zur Ausführung gebracht werden. Eine Gefahr geht insbesondere von Programmeinheiten aus, die unter Ausnutzung von Sicherheitslücken Funktionen mit schädlichen Eigenschaften beinhalten. Diesen Gefahren kann die Nutzerin beziehungsweise der Nutzer durch Deaktivierung der Ausführbarkeit der Programme begegnen. Anbieter sollten daher damit rechnen, dass Nutzer beispielsweise Active-X-Controls, Java- Applets oder Plug-Ins (im Nutzerbrowser installierte Zusatztools) nicht ausführen können. Dies gilt insbesondere für Active X-Programme, von denen im Allgemeinen die weitreichendsten Gefährdungen für Internetnutzer ausgehen. Die Informationsangebote sollten dementsprechend ohne solche Programme gestaltet werden. Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf IMG SRC="../../gif/pfeil.gif"> FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Servernamen, Verzeichnisnamen und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

Attachment

Heute kann man an E-Maildateien, zum Beispiel ein Winworddokument, anhängen und gemeinsam verschicken. Diese Anlagen werden Attachments genannt.

Brett

ist die deutsche Bezeichnung für Newsgroup. Der Begriff ist vor allem in Mailboxnetzen geläufig und kommt von dem Vergleich mit einem schwarzen Brett, einer Pinwand für öffentliche Nachrichten. Newsgroups werden auch Foren oder Diskussionsgruppen genannt. Browser ist das Programm, mit dem man durch das

WWW surfen kann. Ein Browser ist notwendig, um WWW-Seiten überhaupt anschauen zu können (siehe auch HTML).

Cookies

(englisch cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internetangebot erkennbar. Vor allem Firmen benützen Cookies, um Kundenprofile zu erstellen, oder ein persönliches Angebot zusammenstellen zu können. Man kann einstellen, ob der Browser Cookies akzeptieren darf.

DFÜ

(Datenfernübertragung) ist der Sammelbegriff für alles, was elektronische Kommunikation beinhaltet, besonders verbreitet im Mailboxbereich. Domain ist eine weltweit erreichbare Adresse, die von Computern im Internet gebraucht wird, um Nachrichten automatisch zustellen zu können. Rheinmain.de, spiegel.de oder aol.com sind zum Beispiel eine Domain, siehe auch Username.

Download

nennt man den Vorgang, wenn man sich von einem fremden Rechner via DFÜ eine Datei lädt. Man stellt sich den fremden Rechner quasi oben und den eigenen unten vor (siehe auch Upload).

E-Mail

Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internetdienst. E-Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (zum Beispiel FTP, WWW) genutzt werden.

Emoticons

Auch Smileys genannt, mit ihnen werden Stimmungen in Texten (zum Beispiel in mail und news) ausgedrückt (zum Beispiel: :-) lächeln; ;-) verschmitzt lächeln; :-(traurig). FAQs (Frequently Asked Questions) sind sehr hilfreiche Texte, die für Neueinsteigerinnen und Neueinsteiger empfehlenswert sind und verhindern sollen, dass immer dieselben Fragen gestellt werden.

Finger

ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel und so weiter) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

FTP

steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mithilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Gate(way)

ist ein Computer, der den Übergang von einem Netz zu dem anderen, zum Beispiel von dem Internet zu einem Mailboxnetz darstellt. Gateways sind notwendig, da die verschiedenen Netze mit unterschiedlichen technischen Sprachen (Protokollen) arbeiten.

Gopher

ist ein Menüorientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten zu finden sind, (FTP, Telnet, WAIS und so weiter). Jeder Gopherserver ist öffentlich zugänglich. Benutzer können mit ihrem Gopherclient nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

Header

ist der erste Teil (Vorspann) einer Nachricht, in dem die Adresse, der Absender, die Länge der Nachricht, das Datum und andere Informationen stehen.

HTML (Hypertext Markup Language)

ist die Sprache, in der Webseiten geschrieben werden. Erst der Browser ermöglicht eine grafische Umsetzung der HTML Befehle. Das Besondere von HTML sind die universelle Einsetzbarkeit für alle Arten von Computern und die Verweise, sogenannte Links.

HTTP (für Hypertext Transport Protokoll)

ist quasi die technische Grundlage für das WWW. Dem Computer wird mitgeteilt, dass die Daten aus HTMLCode bestehen, deswegen beginnen WWW Adressen mit

http:// Bei neueren Browsern funktioniert das Ansehen von Webseiten allerdings auch, wenn man http:// weglässt.

Hypertext

wird ein Text genannt, der interaktive Verweise (Links) beinhaltet. IRC (Internet Relay Chat) ist ein Internetdienst, der die Möglichkeit bietet, nicht nur via E-Mail und Newsgroups zeitversetzt zu diskutieren, sondern "live" in Echtzeit rund um die Welt.

ISDN

ist eine Telefon(leitungs)-Technik. Herkömmliche Telefonleitungen funktionieren analog, das heißt übertragen Töne. ISDN hingegen funktioniert, wie der Computer, digital und überträgt also 0 und 1. ISDN bedeutet vor allem auch dadurch eine Geschwindigkeitsverbesserung. Ein ISDN-Anschluss beinhaltet 3 bis 10 Rufnummern und 2 Leitungen, was den Nebeneffekt hat, dass man während des Surfens auch telefonieren kann. IP-Adressen sind Zahlenkombinationen wie zum Beispiel 195.35.6.214. Diese Zahlenkombination ist die Adresse des Computers. Jeder Computer hat sowohl eine Adresse aus Wörtern (siehe Domain) als auch eine IP-Adresse. Die IP-Adressen werden von den Computern benutzt, die Namen sind für die Menschen leichter zu merken.

Link

ist der englische Ausdruck für Verbindung und bezeichnet die (anklickbaren) Verweise von einer WWW-Seite auf eine andere.

Mailbox

Im Internet wird das Wort Mailbox für ein persönliches Postfach benützt, in dem eingehende Nachrichten (E-Mails) gespeichert werden.
Ansonsten ist damit allerdings ein Mailboxcomputer gemeint, der anrufbar ist und nicht nur die persönliche Post für seine Nutzerinnen und Nutzer aufbewahrt, sondern auch öffentliche Diskussionsforen anbietet. Auch Firmen bieten manchmal Mailboxen an, um Produktinformationen, Treiber und Software anzubieten.
Eine Mailbox muss man direkt anrufen (dazu muss man oft einen Account besitzen) und im Gegensatz zum Internetprovider verlässt man den angerufenen Rechner nicht, sondern greift nur auf dort vorhandene Informationen zu. Deswegen sind Mailboxen zu Mailboxnetzen zusammengeschlossen, um eine Vielzahl von Informationen anbieten zu können.

Mailingliste

ist eine Art Diskussionsforum via Briefverteiler. Alle teilnehmenden Personen müssen sich bei dem Mailinglistenverteiler anmelden und schicken alle Nachrichten dorthin. Die Nachrichten werden dann an alle Teilnehmerinnen und Teilnehmer weitergeleitet. Mailinglisten gibt es zu allen erdenklichen Themen. Je nach Mailingliste können verschiedene Regeln gelten. Generell stellt man sich meistens kurz vor. Mailinglisten bieten überschaubarere Gemeinschaften als Newsgroups.

Metasearch

nennt man eine Suche, die in mehreren Katalogen und Datenbanken unterschiedlicher Suchmaschinen gleichzeitig erfolgt, beziehungsweise eine Suchmaschine, die anbietet, auf einfache Art und Weise dieselbe Suche auf beliebigen Suchmaschinen durchzuführen. Netcall nennt man sowohl den Datenaustausch von Mailboxen untereinander als auch das Anrufen und Nachrichtenabgleichen eines Points bei der Mailbox.

Netikette

ist die Menge der Umgangsregeln für das Internet und die anderen Netze. Newsgroup ist die Internetbezeichnung für öffentliche Foren, Gesprächsgruppen, also den öffentlichen Bereich, in dem alle die von einer Person gesendeten Nachrichten lesen und beantworten können (siehe auch Usenet-News, Brett).

Online

bedeutet "mit offener Telefonleitung". Nach der Einwahl bei einem Provider oder einer Mailbox ist man "online", also mit bestehender Telefonverbindung zu einem anderen Rechner.

Offline

ist das Gegenteil von Online. Aus Kostengründen gibt es auch Programme, mit denen man ohne Telefonverbindung Nachrichten lesen und schreiben kann und erst hinterher die fertigen Nachrichten über die Telefonleitung verschickt.

PGP Pretty Good Privacy,

ein Verschlüsselungsprogramm für E-Mails. Das Programm kann sowohl elektronische Unterschriften leisten als auch E-Mails sicher verschlüsseln.

Point

ist ein Programm, das sich in die Mailbox einwählt und automatisch die neuen Nachrichten empfängt und versendet, sodass man die Nachrichten in Ruhe daheim schreiben kann, ohne bestehende Telefonverbindung (offline).

PoP (Point of Presence)

ist gleichbedeutend mit Provider beziehungsweise Einwahlknoten. Postmaster sind die Verantwortlichen eines Systems. Bei Unis oder sonstigen Providern gibt es in der Regel immer einen Account Postmaster, an den man schreiben kann, wenn man Hilfe braucht.

PPP (Point to Point Protocoll)

ist notwendig, um sich von Zuhause über Modem und Telefonleitung ins Internet einzuwählen. Die meisten Betriebssysteme und Provider unterstützen dieses Protokoll.

Protokoll

ist eine technische Regelung von Abläufen, quasi eine Sprachregelung, mit der sich Computer verständigen.

Provider

ist ein Internetanbieter. Er ermöglicht Privatpersonen oder Firmen Zugang zum Internet.

Proxy-Server

ist ein Rechner, der nicht direkt jede Anfrage einer Internetadresse in das Netz weitergibt, um die Seite anzufordern, sondern erst in seinen Speicher nachschaut, ob jemand diese Seite bereits aufgerufen hat, sodass er sie nicht erneut anfordern muss. Er speichert also jede angeschaute Datei zwischen, um so die Leitungen zu entlasten. Proxy-Server werden vor allem auch bei Firmenintranets, die ans Internet angeschlossen sind, verwendet, um Verbindungskosten zu sparen und die Arbeitsgeschwindigkeit zu erhöhen.

Signatur(e)

Abspann nach einer Mail. Meist ein Spruch oder vielleicht auch eine Postadresse, die ähnlich wie bei einem bedruckten Briefpapier immer mitgeschickt wird. Es sollten nur kurze Signaturen verwendet werden, da lange Signaturen eine überflüssige Datenlast ausmachen, die die Leitungen belegt.
Digitale Signatur: Siegel zu digitalen Daten, dass den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vergleiche auch § 2 Absatz 1 Signaturgesetz). Ein solches Siegel wird mithilfe spezieller kryptographischer Verfahren aus dem Signaturschlüssel und den Daten erzeugt.

TCP/IP

Internetprotokoll (genaugenommen zwei verschiedene Protokolle: Transmission Control Protocol/Internet Protocol). Die technische Erfindung, die es erlaubt, dass sich völlig unterschiedliche Computer verstehen können und die festlegt, was warum wie wohin gesendet wird und somit die technische Basis des Internets darstellt.

Telnet

Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken zu nutzen, zum Beispiel Archie. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

URL (Universal Ressource Locator)

ist eine exakte Adressangabe für Dateien im Internet. Http://tal.cs.tu-berlin.de/~babajaga/fliegen ist ebenso eine URL wie http://www.tagesschau.de.

Usenet-News

Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser Newsdienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zurzeit gibt es über 120.000 verschiedene Newsgroups. Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreaderprogramme.

Username

Name, der jeder Benutzerin und jedem Benutzer zugewiesen wird, zum Beispiel nora.b; danach kommt immer ein @ und der Name der Mailbox oder des Heimatrechners User-ID; danach kommt immer ein @ und der Name der Mailbox oder des Heimatrechners (also des Providers) und danach die Domain (die Internetadresse des Rechners). Im Gesamten also nora.b@ipn-b.de Der Teil der Adresse nach dem @ kann unterschiedlich lang sein und hängt von dem Heimatrechner beziehungsweise Provider ab.

WAIS (Wide Area Information Server)

ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen.
WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

WhoIs

wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzerinnen und Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internetnutzern aufzubauen, konnte nicht realisiert werden. Zurzeit existiert eine Vielzahl von einzelnen WhoIsservern, auf die mit Telnet oder mit besonderer Clientsoftware zugegriffen werden kann.

WWW

Der Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertextmechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

8. Wichtige Links

Jeder Internetnutzer sollte sich mit Fragen der Sicherheit im Internet befassen. Es gibt inzwischen eine ganze Reihe von technischen Möglichkeiten, sich selbst zu schützen. Selbstdatenschutz ist für jeden sicherheitsbewussten Internetnutzer erforderlich und möglich. Die Datenschutzbeauftragten geben hierzu Hinweise und Tipps (siehe www.datenschutz.de).