

**Über die Gestaltung  
schulischer Netzwerke  
unter besonderer Berücksichtigung von  
Datenschutz und Datensicherheit  
auf Basis einer  
quantitativen Befragung an Schulen**

Aus Fachbereich 3  
der Bergischen Universität  
Gesamthochschule Wuppertal

## DISSERTATION

### **Über die Gestaltung schulischer Netzwerke unter besonderer Berücksichtigung von Datenschutz und Datensicherheit auf Basis einer quantitativen Befragung an Schulen**

Zur Erlangung des akademischen Grades  
Doktor phil.

vorgelegt dem FB Bildungswissenschaften

von  
Monika Pientka

Gutachter: 1. PD Dr. Gregor Tyrchan  
2. Prof. Dr. Christian Hein

Datum der Promotion: Januar 2005

Die Dissertation kann wie folgt zitiert werden:

urn:nbn:de:hbz:468-20050052

[<http://nbn-resolving.de/urn/resolver.pl?urn=urn%3Anbn%3Ade%3Ahbz%3A468-20050052>]

<b>1</b>	<b>EINLEITUNG .....</b>	<b>1</b>
1.1	Begründung für das Thema.....	1
1.2	Aktueller Stand der Diskussion .....	3
1.3	Methodik der Arbeit.....	10
<b>2</b>	<b>DIE BEDEUTUNG DER INFORMATIONS- UND KOMMUNIKATIONSTECHNIK IN DER MODERNEN GESELLSCHAFT .....</b>	<b>12</b>
2.1	<b>Die Entwicklung der Computertechnologie.....</b>	<b>12</b>
2.1.1	Eckpunkte der Computerentwicklung .....	13
2.1.2	Vernetzung von Computersystemen .....	16
2.2	<b>Gestaltung von Netzwerken .....</b>	<b>19</b>
2.2.1	Netzdimensionen .....	21
2.2.2	Übertragungsmedien.....	22
2.2.3	Vernetzungsarten und Netzwerk-Topologien .....	25
2.3	<b>Der Wandel der Gesellschaftsform: Von der Produktions- zur Informationsgesellschaft.....</b>	<b>34</b>
<b>3</b>	<b>MIKROELEKTRONISCHE IUK-TECHNOLOGIEN UND SCHULE .....</b>	<b>42</b>

<b>4</b>	<b>DATENERHEBUNG IN SCHULEN DURCH BEFRAGUNG ZUM BEREICH VERNETZUNG .....</b>	<b>48</b>
4.1	Methodenwahl.....	48
4.2	Gestaltung des Fragebogens.....	50
4.2.1	Belastung des Bearbeiters .....	50
4.2.2	Ausgewogenheit zwischen Geschlossenheit und Offenheit .....	50
4.2.3	Anonymität .....	51
4.2.4	Grundsatz der Gegenseitigkeit .....	51
4.2.5	Objektivierbarkeit .....	52
4.2.6	Reliabilität .....	52
4.2.7	Auswertungsaufwand .....	52
4.3	Anschreiben und Fragebogen.....	54
4.4	Inhaltliche Gestaltung, Ziele der Befragung, Begründung für die Fragestellungen .....	57
<b>5</b>	<b>DURCHFÜHRUNG DER BEFRAGUNG.....</b>	<b>61</b>
<b>6</b>	<b>DATENERFASSUNG UND DATENAUSWERTUNG.....</b>	<b>65</b>
6.1	Frage 1.....	66
6.2	Frage 2.....	67
6.3	Frage 3.....	68
6.4	Frage 4.....	69
6.5	Frage 5.....	70
6.6	Frage 6.....	71
6.7	Frage 7.....	77
6.8	Frage 8.....	78

6.9	Frage 9.....	79
6.10	Frage 10 .....	80
6.11	Frage 11 .....	81
6.12	Frage 12 .....	83
<b>7</b>	<b>ANALYSE / AUSWERTUNG .....</b>	<b>90</b>
7.1	Fragen 1 und 12.....	90
7.2	Frage 2.....	91
7.3	Frage 3.....	91
7.4	Frage 4.....	94
7.5	Frage 5.....	95
7.6	Frage 6.....	97
7.7	Fragen 7 und 8 .....	98
7.8	Frage 9.....	100
7.9	Fragen 10 und 11 .....	100
7.10	Zusammenfassung der Auswertungsergebnisse .....	102
<b>8</b>	<b>DATENSCHUTZ / DATENSICHERHEIT UND INTERNET .....</b>	<b>104</b>

<b>9</b>	<b>DATENSCHUTZ.....</b>	<b>110</b>
9.1	Grundsätzliche Inhalte des Datenschutzes.....	110
9.2	Entwicklung und Struktur des Datenschutzgesetzes.....	113
9.3	Bedeutung des Datenschutzes in der Gesellschaft .....	121
9.4	Bedeutung des Datenschutzes in der Schule.....	125
9.4.1	Schulinterner Datenschutz .....	125
9.4.2	Schulischer Datenschutz und Vernetzung.....	127
<b>10</b>	<b>DATENSICHERHEIT .....</b>	<b>130</b>
10.1	Kernbereiche der Datensicherheitsproblematik.....	131
10.1.1	IT-Sicherheitsmanagement .....	135
10.1.2	Organisation .....	135
10.1.3	Personal .....	136
10.1.4	Datensicherungskonzept .....	137
10.1.5	Bauliche Maßnahmen, Ausstattung .....	137
10.1.6	Computer-Virenschutzkonzept, Firewall, E-Mail-Verkehr .....	138
10.1.7	Häuslicher Arbeitsplatz, Tragbarer PC.....	139
10.1.8	Behandlung von Sicherheitsvorfällen.....	140
10.2	Erhebung des Grundschutzes.....	141
10.3	Maßnahmen zur Erreichung eines Grundschutzes.....	148

<b>11</b>	<b>AUSWIRKUNGEN UND KONSEQUENZEN: EIN „NEUES NETZVERSTÄNDNIS“ .....</b>	<b>152</b>
11.1	Schaffung eines „allgemeinen Verwaltungsnetzes“ .....	153
11.2	Schule – die kleinste Einheit des Verwaltungsnetzes.....	156
11.3	Vernetzung der Schulen miteinander.....	161
11.4	Einbettung der Schulnetze in das Internet .....	163
11.5	Bezirksregierungen bzw. Regionen.....	166
11.6	Zusammenfassung zum Landesnetz NRW .....	168
<b>12</b>	<b>RESÜMEE.....</b>	<b>171</b>
<b>13</b>	<b>ANHANG.....</b>	<b>174</b>
13.1	Auszug aus Web.de Portal v. 30.04.2003: .....	174
13.2	München rüstet (fast) mit Linux aus.....	175
13.3	Killing-my-software – Text des MP3-Files.....	178
13.4	Lovesan.....	179
13.5	Sobig F.....	180
13.6	Datenschutzerläuterungen der Firma Intersport .....	182
13.7	Auszug aus EU-Richtlinie RL 95/46, Erwägungsgründe:.....	187
13.8	Auszug aus BSI-Grundschutzhandbuch, hier: Kap. 1.4.....	190
<b>14</b>	<b>ABBILDUNGSVERZEICHNIS.....</b>	<b>197</b>
<b>15</b>	<b>LITERATUR- UND QUELLENVERZEICHNIS.....</b>	<b>198</b>

# 1 Einleitung

## 1.1 Begründung für das Thema

Die Bedeutung der Computertechnologie, der Informations- und Kommunikationstechnik (im Folgenden „IuK“ genannt) hat in den letzten Jahren, unterstützt durch gesellschaftliche Veränderungen (s. hierzu Kap. 2.3), rasant zugenommen (s. hierzu Kap. 2). Während noch in den späten 70er und frühen 80er Jahren die Welt der Personal Computer (im Folgenden PC) einigen wenigen Fachleuten vorbehalten blieb, sie für den Laien und technisch Uninteressierten aber unerschlossen geblieben war, ist sie heute Bestandteil des Lebens in praktisch allen Bereichen. Nicht nur in der Berufs- und Geschäftswelt, auch in Familie und Freizeit, haben PCs zunehmend bestimmende Bedeutung. Mit E-Commerce, E-Business, Online-Banking, Nutzung von Messengern, E-Mail-Accounts werden wesentliche Bereiche des bisher notwendigen direkten Umganges mit anderen Menschen für private und berufliche Zwecke an den PC-Arbeitsplatz am heimischen Schreibtisch verlegt. So wird etwa das Telefon als klassische Fernkommunikationsform nach und nach durch die erheblich weiter gestreuten Möglichkeiten des PC ersetzt. Hier wird exemplarisch deutlich, wie die Gesellschaft sich immer mehr zur Informationsgesellschaft entwickelt, die die Chancen und Möglichkeiten der IuK nutzt bzw. nutzen muss. In Kapitel 2 werden hierzu vertiefende Ausführungen gemacht.

Schon im frühen Kindesalter gehört mittlerweile die Handhabung der Maus und des Keyboards ebenso zum Alltag wie das Malen mit Buntstiften oder das Basteln mit Schere und Papier. Nach jahrelangem Tauziehen um die Einführung moderner IuK-Technik<sup>1</sup> in den Grundschulen sollte computergestützter Unterricht heute zum didaktischen Konzept gehören, aus Ori-

---

<sup>1</sup> Die Vorreiterrolle in der Einführung spielten andere Bundesländer. Nordrhein-Westfalen war eher zurückhaltend, teils deutlich ablehnend. Noch im Jahre 1989 wurde durch Landtagsbeschluss entschieden, dass „... in der Grundschule ... auch weiterhin von einer Einführung der neuen Technologien abzusehen ...“ ist (LANDTAG, Drucksache 10/4917, Landtagsbeschluss vom 14.12.1989. Weitere Aussagen finden sich in BÜTTNER (1999), MITZLAFF (1996), TULODZIECKI (1996) u.a.

entierungsstufe und weiterführenden Schulen aller Schulformen und Schularten als Kernbestandteil nicht mehr wegzudenken sein. Es geht also mittlerweile nicht mehr um das „Ob“ einer Einführung von IuK im Bereich der allgemeinbildenden Schule, sondern eher um das „Wie“, das „Wozu“ und das „Was“, und zwar in didaktisch-pädagogischer Hinsicht und in organisatorischer, ökonomischer und technischer Hinsicht<sup>2</sup>. Erst Aussagen und Daten zu konkreten Forderungen bei den Umsetzungen der IuK-Technologien in der Schule zeigen den angestrebten bzw. erreichten Standard. In der weiteren Betrachtung ist zu fragen, wie dieser Standard erhalten bzw. verbessert und ausgebaut werden kann. Die einmalige Beschaffung entsprechender Hard- und Softwareausstattung dient zwar der Befriedigung aktueller Bedürfnisse und Wünsche, ob und in wieweit aber zukünftig den Anforderungen an Support und Folgekosten (allein z.B. hinsichtlich erforderlicher Toner für Drucker oder Updates für Software) entsprochen werden kann, bleibt fraglich; entsprechende Konzepte müssen erarbeitet werden.<sup>3</sup> Daher kann und will die vorliegende Arbeit nicht so sehr von Deklarationen, Lehrplänen und bildungspolitischen Wunschvorstellungen ausgehen, sondern muss sich mit nüchternen Zahlenbefunden zu IuK in den Schulen befassen und von den Erfahrungen der Lehrkräfte und Schulleitungen hinsichtlich der

---

<sup>2</sup> Eine solchermaßen umfassende Initiative, die alle erforderlichen Bereiche abdeckt, findet sich in Hessen durch die Medieninitiative Schule @ Zukunft. Vgl. hierzu [www.schule@zukunft-hessen.de](mailto:www.schule@zukunft-hessen.de) zum Stichwort „Unterricht“, 13.08.2003, 14.44 Uhr:

*„Designiertes Hauptziel der Medieninitiative Schule @Zukunft ist es, durch Verbesserung der IT-Ausstattung an Schulen, dem Aufbau nachhaltiger Lösungen für Service und Support sowie der Stärkung und Förderung von Medienkompetenz bei Lehrerinnen und Lehrern, eine spürbare Qualitätssteigerung des Unterrichts an den hessischen Schulen zu erzielen. Multimediale Lehr- und Lernmethoden sollen in allen Fächern selbstverständlicher Bestandteil des Unterrichts werden, denn sie können den Lehralltag der Lehrerinnen und Lehrer und auch den Lernalltag der Schülerinnen und Schüler bereichern.“*

<sup>3</sup> S. hierzu [www.schule@zukunft-hessen.de](mailto:www.schule@zukunft-hessen.de), Stichwort „Support in Schulen“, 13.08.2003, 14.45 Uhr:

*„In den letzten Jahren wurde der Support vorwiegend von engagierten Lehrerinnen und Lehrern mit großem zusätzlichem Zeitaufwand geleistet, das ist heute nicht mehr zeitgemäß. Land und Schulträger beraten derzeit in einer Arbeitsgruppe sinnvolle und finanzierbare Lösungen für die Zukunft.“*

Diskrepanzen von Soll- und Ist-Zustand leiten lassen. Das ist der Hauptgrund für die umfangreiche Datenerhebung und deren Auswertung in den Kapiteln 1 bis 7.

Eine Unterscheidung hinsichtlich der Schulform kann und darf es in diesem Zusammenhang nicht mehr geben, da PCs in allen Lebensbereichen vertreten sind. Die Genese, Situation und Bedeutung von IuK-Technik im Unterricht und für Unterricht, für Lehren und Lernen, sollen in Kapitel 3 näher erörtert werden.

Über eine inhaltliche und mediale Modernisierung des Lehrens und Lernens hinaus, für eine Optimierung bei der Betreuung von Schülern, wie sie nachhaltig in vielen Publikationen nach den PISA-Studien verbreitet wird, und für eine Verbesserung der Organisation der schulischen Verwaltung und des Lebens der Schulgemeinschaft ist die Nutzung moderner IuK-Technologien unerlässlich. Dazu werden in Kapitel 10 Ansätze und Umsetzungsmöglichkeiten vorgestellt.

## **1.2 Aktueller Stand der Diskussion**

Viele in Zeitungen und in Fernsehsendungen, auf Konferenzen und in Fachveröffentlichungen vorgebrachte Behauptungen und Forderungen, dass Deutschland und das deutsche Bildungssystem auch auf dem Gebiet der schulischen Umsetzungen bei den IuK-Technologien einen großen Nachholbedarf haben, sind nicht erst in jüngster Zeit entstanden. Die auch in den neuesten Studien festgestellten Defizite (s. hierzu S. 7 ff) sind Fortschreibungen älterer internationaler Untersuchungen hinsichtlich der Berücksichtigung von Computern im Schulwesen.<sup>4</sup> Aus derartigen Untersuchungen entstanden sind die vielfältigen Bemühungen, notfalls auch mit Hilfe von Sponsoren aus der Wirtschaft diesen Rückstand aufzuholen. Man

---

<sup>4</sup> Z.B. Council of Europe (Ed): *New Technologies in Secondary Education, A Report of the Education Research Workshop held in Frascati* (1982), Lisse (1983)

hat versucht, den formulierten Forderungen Rechnung zu tragen und hat eine Welle von Aktivitäten losgetreten<sup>5</sup>. Das Vordringen der IuK-Technologien im Erwerbsleben und sogar im häuslichen Alltag kann aus dem täglichen Geschehen der Schulen weder bildungspolitisch noch curricular-didaktisch oder schulorganisatorisch ausgeklammert werden. Daher haben, wie auch von den Verantwortlichen in der Bildungspolitik berichtet wird, immer mehr Schulen immer mehr Computer, Internetzugänge und Computerräume<sup>6</sup>. Ob allerdings damit die Schulen den Forderungen gerecht werden können und die Nutzung moderner IuK-Technik tatsächlich zur Selbstverständlichkeit geworden ist<sup>7</sup>, bedarf einer näheren detaillierteren Untersuchung.

Eine tatsächlich selbstverständlich gewordene Nutzung läge erst dann vor, wenn nicht nur jede Schule einen Computer hat und ans Netz angeschlossen ist und die Möglichkeiten des World Wide Web genutzt würden, sondern wenn auch rechnergestützte Kommunikation in den Lebensalltag der Schulen integriert würde. Z.B. böten sich hier kommunikative Strukturen in Form eines Intranets für verwaltungs – und schulinterne Wege an, es gäbe die Möglichkeit zur Ergänzung durch Laptops und Handhelds zur Einmal erfassung und Mehrfachnutzung von Daten usw. Sofern dies nicht umgesetzt ist, erscheint die Wertung als alltägliches Kommunika-

---

<sup>5</sup> So z.B. „Schulen ans Netz e.V.“ auf Bundes- und Landesebene ([www.schulen-ans-netz.de](http://www.schulen-ans-netz.de)), „D 21“ – Verbund von Ländern, Bund und Firmen ([www.initiatived21.de](http://www.initiatived21.de)), e-initiative in NRW ([www.e-initiative.nrw.de](http://www.e-initiative.nrw.de)), Unterstützung durch c't für schulische Aktivitäten ([www.heise.de](http://www.heise.de)) u.a.

<sup>6</sup> „... Im Rahmen der e-initiative werden verschiedenartige IT-Infrastrukturprojekte vorangetrieben. Ausgangspunkt sind dabei Konzepte zur Medienentwicklung einzelner Schulen und kommunale Medienentwicklungspläne...“ aus: [www.schulen-ans-netz.de/itworks](http://www.schulen-ans-netz.de/itworks), S. 23

<sup>7</sup> Andreas Rittershofer konstatiert in Computer und Unterricht, Heft 41 / 2002: Medienmanagement: Computer und Netzwerke an Schulen, S. 64 f:  
*Computer und lokale Netzwerke (LAN : Local Area Network) sind an Schulen mittlerweile zu einer Selbstverständlichkeit geworden, unvernetzte Rechner ein Anachronismus und unter allen Umständen zu vermeiden.*

tionsmittel noch nicht erreicht<sup>8</sup>. Festzustellen wäre demnach, in welchem Maße innerhalb des schulischen Alltages die technischen Möglichkeiten auch für die interne Kommunikation genutzt werden. Nur durch Aufbau und Nutzung solcher interner Kommunikationsstrukturen sind die technischen Möglichkeiten tatsächlich erschöpfend auszunutzen (s. hierzu Kap. 10). Die entscheidende Frage, die über die rein quantitative Anhäufung von Computern in Schulen in Richtung auf universellen Einsatz der IuK hinauszielt, ist: Wie und in welchem Umfang, nach welchen Konzepten und Regularien, mit welcher Ausstattung im Bereich Hard- und Software haben Schulen zusätzlich zum normalen Einsatz von IuK bei der Stand-alone-Nutzung (s. Kap. 2.12) zur Unterrichtsvorbereitung, zum Einsatz von Teachware / Lernsoftware und zu Internet-Aktivitäten ein funktionierendes Intranet geschaffen und wie gehen sie damit um? Im Kern der Interessen stehen bislang nicht interne Schulvernetzungen auf Instituts-, Bezirksregierungs- oder Kommunalebene (=Intranets), lediglich das Internet ist in der Diskussion. Auch eine aktuelle EUN-Studie<sup>9</sup> befasst sich vornehmlich mit Fragen des Internets; ebendies gilt auch für Veröffentlichungen zu computerbezogenen Themenbereichen im allgemeinen, die zwar das dringende Erfordernis für Vernetzungen jeder Art erkennen, technische Netzaufbauhilfen geben, technische Hinweise und Alternativen erläutern, für die interne Kommunikation im Rahmen von Intranets allerdings Antworten schuldig bleiben, insbesondere

---

<sup>8</sup> Aktionen zur Umsetzung solcher Möglichkeiten sind bereits erfolgt. Nicht nur in anderen Bundesländern (Beispiel Initiative Hessen zum „Lernen mit Laptops“ und „Unterricht mit Laptops“ im Rahmen von Schule@Zukunft), auch in NRW gibt es bereits Schulen, die die Kommunikationsmöglichkeiten weitgehend nutzen, so z.B. Laptop-Schule Bielefeld oder internationale Schule Düsseldorf. Erfahrungsberichte über „Laptop-Schulen“ finden sich in SCHAUMBERG,H.: Neues Lernen mit Laptops? Ein Überblick über Forschungsergebnisse zur Nutzung mobiler Computer in der Schule. In: Zeitschrift für Medienpsychologie 13 (2001), S. 11 – 21 sowie ISSING, L. / SCHAUMBERG,H.: Lernen mit Laptops. Ergebnisse einer Evaluationsstudie. Gütersloh 2002

Auch im Rahmen der Initiative e-initiative.nrw „Schulen-ans-Netz“ werden entsprechende Konzepte erarbeitet. Vgl. hierzu it-works, April 2003, S. 24. Zu den Initiativen im Einzelnen s. [www.bildungsserver.de](http://www.bildungsserver.de) sowie – für NRW – [www.learnline-nrw.de](http://www.learnline-nrw.de).

<sup>9</sup> zu finden unter <http://www.lehrer-online.de>

Bestandsaufnahmen zur Feststellung der vorhandenen Basisdaten vermissen lassen.

Wie anders erscheint doch teilweise die Situation in einigen europäischen Nachbarländern, wie Erhebungen / Veröffentlichungen zeigen. So wird in einer EU-Untersuchung im Rahmen von eEurope (Kommission der Europäischen Gemeinschaft) erhoben, wie der Stand des Fortschritts für „Europas Jugend ins Digitalzeitalter“ ist.

Dazu werden unterschiedliche Indikatoren herangezogen:

- Anzahl von Computern
- Anzahl der PC mit Internetzugang
- Anzahl von PC mit Hochgeschwindigkeits-Internetanschluss, jeweils bezogen auf 100 Schüler bzw. Studenten.

Dabei wird im Rahmen der Untersuchung ebenfalls berücksichtigt, dass nicht alleine Art und Umfang der technischen Ausstattung entscheidend für den Fortschritt sind, sondern dass „...*auch die Qualität der Ausrüstung und der Internetanschlüsse, die Ausbildung der Lehrer, die Einstellung der Lehrer gegenüber den neuen Werkzeugen und die Art, wie sie diese nutzen...*“<sup>10</sup> von grundlegender Bedeutung sind. Die für die vorliegende Arbeit besonders aussagekräftigen Ergebnisse der Untersuchung stellen sich dabei - zusammengefasst – wie folgt dar:

- *Durchschnittlich müssen sich in den Schulen der EU 12 Schüler einen Computer teilen, aber die Unterschiede reichen von 3 bis 25. Die Lage ist besonders günstig in Dänemark und Luxemburg (rund 3 Schüler pro Computer) , und besonders ungünstig in*

---

<sup>10</sup> KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFT: Arbeitsdokument der Kommissionsdienststellen; eEurope, Benchmarking, Europas Jugend ins Digitalzeitalter; Europabarometer Blitzumfragen 101 „Schulleiter“ und 102 „Lehrer“ von Februar-Mai 2001; Brüssel 2001, S. 6

*Deutschland, Griechenland und Portugal (mehr als 20 Schüler pro Computer).<sup>11</sup>*

- *Noch größer sind die Unterschiede bei ans Internet angeschlossenen Rechnern. Bei einem EU-Durchschnitt von 25 Schülern pro Rechner mit Netzanschluss reichen die einzelnen Werte von 4 bis 50. Dabei liegen im Wesentlichen die gleichen EU-Länder an der Spitze bzw. am Schluss wie beim vorigen Indikator.<sup>12</sup> (...) Dies bedeutet jedoch nicht, dass die Schüler den Anschluss in all diesen Schulen auch nutzen können – nur in 8 von 10 Schulen in der EU haben die Schüler auch selbst Zugang zum Internet.<sup>13</sup>*
- *Im Durchschnitt werden 15 % der Computer in Schulen von privaten Gebern gestiftet. Dabei bestehen große Unterschiede von Land zu Land. Am ausgeprägtesten sind private Gaben in Österreich und Deutschland, wo fast 30 % aller Computer von privaten Gebern stammen, und den Niederlanden (25 %)...<sup>14</sup>*
- *Der Einsatz von Rechnern ohne Netzanschluss wird in Grundschulen zum Normalfall; sieben von zehn Lehrern (71 %) nutzen sie dort. 15 (...) Beim Prozentsatz der Grundschullehrer, die Rechner ohne Netzanschluss benutzen, besteht ein ausgeprägter Kontrast zwischen einer führenden Gruppe von acht Ländern mit Werten unter 40 %, bis hinab zu 12 % (Luxemburg, Portugal, Deutschland und Griechenland).<sup>16</sup>*

---

<sup>11</sup> a.a.O., S. 8

<sup>12</sup> a.a.O., S. 8

<sup>13</sup> a.a.O., S. 9

<sup>14</sup> a.a.O., S. 13

<sup>15</sup> Nach Diagramm der Studienergebnisse trifft auch dies auf Deutschland nicht zu; hier liegt die Zahl bei ca. 37 %; s. hierzu S. 15 des Schlussberichtes

<sup>16</sup> a.a.O., S. 15

- *Im Zusammenhang mit den in der EU-Befragung genannten Hauptgründen für die Nichtnutzung von Computern und Internet wird deutlich, dass in einigen Ländern, so auch in Deutschland, der Mangel an fundierter Ausbildung ein wesentlicher Grund ist. Es haben in Deutschland ca. 35 % der Befragten angegeben, am PC ausgebildet zu sein, 22 % auch im Bezug auf das Internet, 63 % aber erklären, keinerlei Ausbildung erhalten zu haben. Damit bildet Deutschland den Spitzenreiter innerhalb der Befragung; alle anderen Länder haben weniger Nicht-Ausgebildete, mehr am Computer ausgebildete Lehrer und fast alle anderen Länder (außer Litauen mit 20 %) mehr Lehrer mit Internet-Ausbildung. Wo die Ursachen für die Mängel in der Ausbildung am PC zu suchen sind, ergibt die Studie nicht. Allerdings kann so viel gesagt werden, dass die Ursache offenkundig nicht in einer besonderen Altersstruktur der bundesdeutschen Lehrerschaft oder etwa in deren Fortbildungsbereitschaft zu suchen sein kann noch etwa darin, dass die IuK-Technologien generell „einen Bogen um Deutschland gemacht“ haben. Dagegen spricht schon der Befund, dass in Europa (und damit in der Bundesrepublik) 9 von 10 Lehrern einen PC zu hause haben (s. S. 10).*
- *Zwar nutzt jeder zweite europäische Lehrer das Internet, um mit anderen Schulen zusammenzuarbeiten, aber weniger als jeder fünfte benutzt es zur Kontaktaufnahme mit einer Schule in einem anderen EU-Staat. Vernetzte Zusammenarbeit hauptsächlich zwischen Schulen in der gleichen Region (31 %) (D: 30 %) oder im gleichen Land (25 %) (D: ca. 25 %). Nur 17 % (D: ca. 24 %) aller Lehrer, die das Internet nutzen, nehmen Kontakt zu Schulen in einem anderen europäischen Land auf, und 11 % (D: 11 %) zu Schulen außerhalb Europas.<sup>17</sup>*

---

<sup>17</sup> a.a.O., S. 21; die Klammervermerke enthalten die Befragungsergebnisse Deutschlands.

- *Zu Hause sind die Lehrer äußerst gut ausgestattet: 9 von 10 europäischen Lehrern haben zu Hause einen Computer und 7 von 10 einen Internetanschluss.*<sup>18</sup>

Diese wenigen Auszüge zeigen bereits, dass offenbar Deutschland nicht zu den europäischen Wegbereitern gehört, die Europas Jugend in das Digitalzeitalter führen bzw. geleiten kann. Offenbar gehört Deutschland eher zu denjenigen europäischen Ländern, die dringenden Nachholbedarf auf manchen der erfragten Gebiete haben.

Dabei wird durch die Befragungsergebnisse in keiner Weise der Tatsache Rechnung getragen, dass Deutschland wegen seines föderalistischen Aufbaus ebenso über ein internes Ungleichgewicht verfügen kann. Durch die unterschiedlichen sozialen und demographischen Strukturen, die ebenso unterschiedlichen Landeshaushalte, Landesgrößen und politischen Ausrichtungen und Programme der verschiedenen Bundesländer können sich auch innerhalb der Bundesrepublik deutliche Unterschiede ergeben, wozu – naturgemäß – eine EU-Studie keine Aussage treffen kann. Ob also deren Ergebnisse auch auf nordrhein-westfälische Verhältnisse zu übertragen sind, erscheint fraglich und soll u.a. im Verlaufe dieser Arbeit festgestellt werden.

---

<sup>18</sup> a.a.O., S. 22; hier liegen auch die bundesdeutschen Ergebnisse mit ca. 94 % und ca. 72 % mit vorne.

### 1.3 Methodik der Arbeit

Der derzeitige Stand der technischen Entwicklung sowie die Einschätzung der Erfordernisse bei den Beteiligten, also bei Schulen und Lehrkräften, zeichnen unterschiedliche Bilder je nach Standort und genutzter Quelle. Während in den Medien die Stellung der politischen Entscheidungsebene (Schulträger, Aufsichtsbehörde, Ministerium) schwerpunktmäßig dargestellt wird, gibt es kaum Untersuchungen und Veröffentlichungen darüber, wie die Schulen selbst die technischen Möglichkeiten, deren Stand der Umsetzung oder deren Nutzung bewerten. Printmedien wie *Spiegel* oder *Focus* beschäftigen sich eher mit der Frage, ob Ebenen mit Regulierungsauftrag und -kompetenz ihrer Aufgabe in ausreichendem Maße nachkommen und welches die Folgen für die Bildung unserer Schüler sein können oder sein werden. Literatur unterschiedlicher Provenienz wiederum stellt ihre Darstellungen auf die jeweilige Fachrichtung ab: Während in den soziologisch orientierten Fachveröffentlichungen eher die Bedeutung der Technologie für die Gesellschaft und die jeweiligen Wechselwirkungen im Vordergrund stehen (s. hierzu Kap. 2.3), finden sich in der technisch ausgerichteten Literatur eher Fragen von Netzaufbauten und in der pädagogisch-didaktisch orientierten zunächst Aussagen über die Bedeutung der Technologie für und in Unterricht. Eine Verbindung dieser unterschiedlichen Betrachtungsebenen in zusammenführende Darstellung soll hier versucht werden.

Zunächst sind Recherchen und die sich anschließende Auswertung und vergleichende Einbeziehung der in den genannten Bereichen vorhandenen Literatur (als theoretische Anforderungen) erforderlich.

Sodann ist die Einbindung der Einstellung und Aussagen von „Praktikern“ im Schulalltag (als Anforderungen aus der Praxis und für die Praxis) in das Thema zu vollziehen und die Frage zu stellen, in wie weit Anspruch und Wirklichkeit, politische Anforderungen und reale Umsetzung bereits in

Einklang gebracht werden konnten oder ob und in wie weit es noch Diskrepanzen auszuräumen gibt.

Hierzu soll durch eine Befragung von Schulen (Kap. 3 ff) Datenmaterial erhoben werden, das Erkenntnisse darüber erbringt, wie weit Schulen die im Zusammenhang mit Vernetzung in Form von Intranets und dem Internet entstehenden Probleme organisatorischer und technischer Art bereits bewältigen konnten. Aus dieser Befragung soll sich letztendlich auch der Schwerpunkt der Arbeit ergeben, der Klärung über solche Bereiche erbringen soll, die die Auswertung des Fragebogens (Kap. 7) als bislang in der Literatur eher unerörtert oder ungelöst oder als zweitrangig erkennen lässt. Diese Bereiche werden als förmlich zwingende, theoretische Defizitbereiche aufgegriffen und aufgearbeitet (Kap. 8, 9 und 10). Ergebnis soll ein Vorschlag sein, der eine sachorientierte, zielgerichtete und arbeits- und produktorientierte Ausstattung und Ausnutzung angemessener Technikausstattung und damit eine effiziente, universelle, umfassende Nutzung von IuK und speziell von Vernetzungen / Netzwerken für Bildungsanliegen und Schulmanagement und gleichzeitig neue Formen des Lehrens und Lernens bietet (Kap. 11).

## 2 Die Bedeutung der Informations- und Kommunikationstechnik in der modernen Gesellschaft

### 2.1 Die Entwicklung der Computertechnologie

Mit Beginn des technischen Fortschritts im Rahmen der Computerforschung und -entwicklung war das rasante Fortschreiten der Technologie ebenso wenig abzusehen wie deren Auswirkungen auf die Gesellschaft (s. hierzu NIEMANN. H.-W., 1985<sup>19</sup> sowie Kap. 2.2). Vornehmlich für militärische Zwecke entwickelt, nahmen die in etwa zeitgleich in Deutschland und den USA während des Zweiten Weltkrieges entwickelten „Maschinen“ sowohl in ihrer Bedeutung als auch hinsichtlich ihres physischen Umfanges großen Raum ein (vgl. Kap. 2.1.1). Erstmals war es möglich, zunächst noch mit Hilfe von Lochkarten oder –streifen als Datenträger bzw. Datenspeicher Daten automatisiert zu verarbeiten.<sup>20</sup> Der dafür erforderliche Platzaufwand stand jedoch in keinem Verhältnis zu heutigen Dimensionen. Auch deshalb kam diese Technik nur für wenige ausgewählte Bereiche in Frage, war für den Normalbürger eine wenig vertraute, beeindruckende und gleichzeitig häufig beängstigende Besonderheit der Militärs, von Staats- und Verfassungsschutzbehörden und weniger Großindustriebetriebe. Die Furcht vor dem gläsernen Menschen, vor dem durch automatisierte Datenerhebung und –verarbeitung lückenlos beobachtbaren Bürger wuchs und wurde noch verstärkt durch die neu aufkommende Welle von Science-Fiction-Romanen (z.B. Asimov, Aldiss, Cooper u.a.) oder Orwells Roman „1984“. Dazu tru-

---

<sup>19</sup> NIEMANN stellt sowohl die Auswirkungen technischen Fortschritts für die Gesellschaft dar als auch die gesamtgeschichtliche Entwicklung der Technik seit der Vorgeschichte dar.

<sup>20</sup> Detaillierte und ausführliche Darstellungen zur geschichtlichen Entwicklung der Computer finden sich etwa bei GRAF (1984), VONDRAN (1982), FRIEDRICH, SCHAFF (1984), CERUZZI, P.E. (2003), MATIS, H. (2002), FRIEDEWALD (1999). Hier finden sich auch Kommentierungen zu den Urheberschaften von Hardware und Software, zur technischen Entwicklungsgeschichte der PCs, zur Namensgebung (ob Mikrocomputer, Heimcomputer oder Personal Computer) und anderes mehr.

gen aber auch die fehlende Nähe zu dieser neuen Technologie und ihre Undurchschaubarkeit bei.

Es ist nicht beabsichtigt, in dieser Arbeit die Entwicklung technischer Standards der PCs oder der Prozessoren wiederzugeben, auch nicht die der internen oder externen Hardware und Hardwareerweiterungen oder die der Peripheriegeräte. Entwicklungen von Disketten-, CD-ROM-Laufwerken, Speicherbausteinen, Druckertypen u.a. bis hin zu den heute bekannten Betriebskenndaten, die jeden Computer älterer Bauart nahezu „alt aussehen“ lassen, werden bereits in der Literatur ausführlich dargestellt.<sup>21</sup>

Hier sollen eher die grundsätzlichen Eckpunkte aufgezeigt werden, die den Siegeslauf der Computer in allen Bereichen und rund um die Welt ermöglichten und erklären.

### **2.1.1 Eckpunkte der Computerentwicklung**

Die Innovation der Computer-Technik hat in den letzten Jahren einen rasanten Entwicklungsschub bekommen, der teils mit der Weiterentwicklung technischer Bauelemente, teils mit der Rationalisierung von Fertigungstechniken für diese Elemente, teils aber auch mit der veränderten Anforderung an technische Leistung und Anwendbarkeit einhergeht. Schon 1985 wurde im Rahmen einer Ausstellung im Deutschen Museum München erkannt, welche Zukunftschancen sich mit der damals hochaktuellen Entwicklung verbanden.<sup>22</sup> Was damals noch Zukunftsträume waren, ist heute Realität und Alltag geworden (so z. B. Breitbandkommunikation inklusive

---

<sup>21</sup> S. z.B. MÖRIKE (1997), aber auch schon die bereits erwähnten Quellen GRAF (1984), FRIEDEWALD (1999) u.v.a.

<sup>22</sup> SIEMENS AG (Hr.): Chancen mit Chips; Zwischenbilanz einer Basistechnologie. Eine Sonderveröffentlichung der Siemens AG zur Ausstellung im Deutschen Museum. Berlin / München 1985

Bildübertragung pp.; SIEMENS AG (1985), S. 26). Dies alles wurde möglich durch die Meilensteine der Entwicklung:

#### 2.1.1.1 Halbleitertechnologie

Mit der Entwicklung und der Einführung von Halbleitertechnik wurden aus den „Ungetümen“ der ersten elektrischen, mit Relais und Elektronenröhren arbeitenden Computern der 40er Jahre des vergangenen Jahrhunderts schreibbischgroße Rechenautomaten mit geringerer Störanfälligkeit und geringerem Energiebedarf. Allerdings wurden in diesen frühen Jahren die entsprechenden Halbleiter-Schaltkreise, bestehend aus diskreten Transistoren, Dioden, Widerständen und Kondensatoren, noch von Hand verdrahtet und auf zuweilen schon gedruckten Schaltungsplatinen (Printplatinen) verlötet. Dabei ist zu berücksichtigen, dass anfänglich die Dioden und Transistoren noch in der langwierigen Legierungstechnik hergestellt wurden und nicht in der späteren Mesa- oder Epitaxietechnik.<sup>23</sup>

Im Jahre 1959 brachte die Erfindung und Verbreitung der Integrierten Schaltkreise (Integrated Circuits – IC) einen weiteren Meilenstein der Computerentwicklung. IC sind Halbleiterplättchen von geringer Größe (rechteckig oder quadratisch, ca. 5 mm Seitenlänge), auf denen ganze Schaltkreise einschließlich der erforderlichen „Verdrahtungen“ und einiger hundert oder gar tausend einzelner elektronischer Elemente in einzelnen Schritten foto-/chemo-physikalisch erzeugt werden. Von Vorteil sind bei dieser Technik neben der Packungsdichte und der enorm kurzen Laufzeit der Signale sowohl die Zeitersparnis in der Produktion, da mehrere IC gleichzeitig auf dem so genannten Wafer (einem hauchdünnen Schnitt aus einer hochreinen Halbleitersäule) hergestellt werden können, als auch die damit verbundene Kostenersparnis.

Die Weiterentwicklung gerade dieser Technik führte zum entscheidenden zweiten Eckpunkt in der Computerentwicklung.

---

<sup>23</sup> SIEMENS AG: Halbleiterbauelemente für die Elektronik; o.O., o.J. sowie zur Herstellung von Speicherbausteinen MÖRIKE (1997), Kap. 1.3

#### 2.1.1.2 Miniaturisierung

Hierbei gelingt es, auf der Fläche von nur wenigen Quadratmillimetern eines Halbleiterplättchens mehrere Dioden und Transistoren „unterzubringen“. Zu Beginn wurden zunächst ein paar Dutzend Bau-Elemente geschaltet, heute gelingt es, mehr als eine Million Dioden und Transistoren zu funktionierenden Schaltkreisen zu integrieren, und dies mit immer höherer Zuverlässigkeit, immer weniger elektrischem Energiebedarf, immer kürzeren Signallaufzeiten für immer mehr verschiedene elektronische Funktionen und Aufgabenstellungen.<sup>24</sup>

Zwei der wichtigsten Bausteine dieser Gattung sind im Zusammenhang mit dieser Arbeit Mikroprozessoren und Halbleiterspeicherbausteine, die auch für die IuK – computergesteuert oder als so genannte embedded systems – von entscheidender Bedeutung sind.

Zum Vergleich: Während für die Rechenleistung eines Rechenautomaten der ersten Generation (Elektronenröhren, Relais, s.o.) z.B. das Volumen eines mittelgroßen Zimmers mit ca. 50 Kubikmetern veranschlagt wurde, reduziert sich bei modernen Rechenautomaten (PCs) die gleiche Rechenleistung auf den Raumbedarf einer einzelnen Haferflocke. Diese Miniaturisierung der räumlichen Dimension findet ihre Entsprechung in der Miniaturisierung des Energiebedarfs wie auch der spezifischen Kosten für die Durchführung eines einzelnen Verfahrensabschnittes solcher Systeme.

Konsequenterweise schloss sich daran der dritte Schritt in der Entwicklung an:

#### 2.1.1.3 Massenfertigung und Kostendegression

Sowohl die Fertigung dieser mikroelektronischen Bauelemente als auch die der informationsverarbeitenden Geräte selbst, der Gehäuse und Peripheriegeräte wurde auf Massenproduktion umgestellt. Damit wurde

---

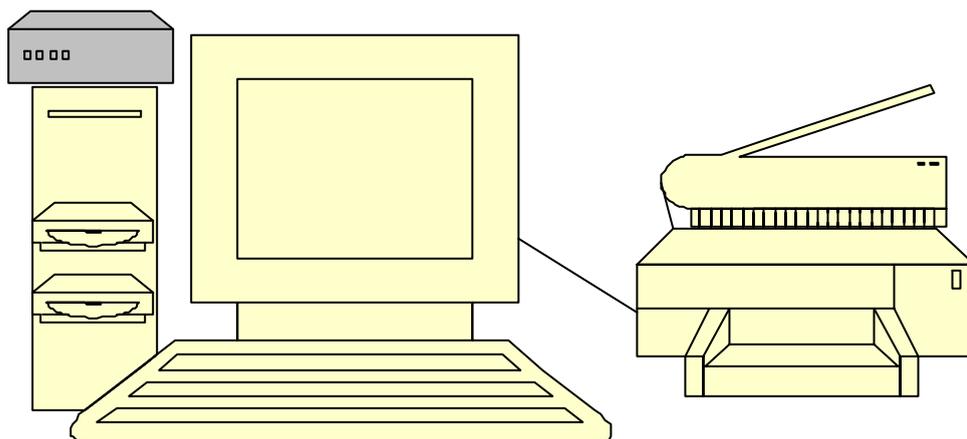
<sup>24</sup> Vertiefende Erläuterungen etwa bei HARTH, W.: Halbleitertechnologie. Stuttgart 1972, sowie SIEMENS AG, o.J.

nicht nur der Aufbau einer völlig neuen Industriesparte möglich, es gelang auch die horizontale Verbreitung der mikroelektronischen Schaltungen, Bausteine, Geräte in vielen Bereichen (vgl. Kap. 3).

Diese enorme quantitative Vermehrung von PCs in der Breite ermöglichte auch die Entwicklung diversifizierter, leistungsstarker Software und damit auch den Einsatz von Computersystemen und mikroelektronik-gestützten Neuen Medien im Schulsektor, im häuslichen Alltag und im Freizeitbereich (vgl. Kap 2.3 und Kap. 3).

### 2.1.2 Vernetzung von Computersystemen

Die bisherigen Ausführungen dieses Kapitels beziehen sich – unabhängig vom Verwendungs- und Einsatzzweck oder von der Leistungsfähigkeit eines Computersystems – auf den so genannten Stand-alone-Rechner (s. Abb. 1). Dabei bleibt die Informationsverarbeitung auf einen recht engen, wohl bestimmten Wirkungskreis beschränkt, in dessen Zentrum sowohl in technischer Hinsicht als auch hinsichtlich des Verarbeitungsablaufes der Computer selbst steht.



**Abbildung 1: Stand-alone-Rechner**

von links nach rechts: Rechner mit Tastatur und Monitor, daneben Drucker mit Scanner, Internet-Zugang wird gestaltet über Modem (grau)  
(Abb. erstellt durch Verf.)

Ein PC in dieser Konfiguration verfügt über Dateneingabe- und Datenausgabeeinheit gleichermaßen und benötigt natürlich ein für die Einsatzfunktion vollständiges und autarkes Software-Paket.<sup>25</sup> Dies war und ist wohl die originäre Einsatzkonfiguration von Computern, wie sie wohl auch aus dem häuslichen Bereich, aber auch – immer noch - aus Schulen und Hochschulen bekannt ist.

Schon früh zeigte sich, dass im Stand-Alone-Modus Computer kaum ausgelastet sind hinsichtlich ihrer Rechenkapazität. Daher wurde auch im Hinblick auf mögliche Betriebskostensenkungen Rechenleistung „außer Haus“ angeboten, Datenverarbeitung also im Time-Sharing-Verfahren. Dies ist dadurch möglich geworden, dass Daten auf externen Datenspeichern „auf Reisen“ gehen.

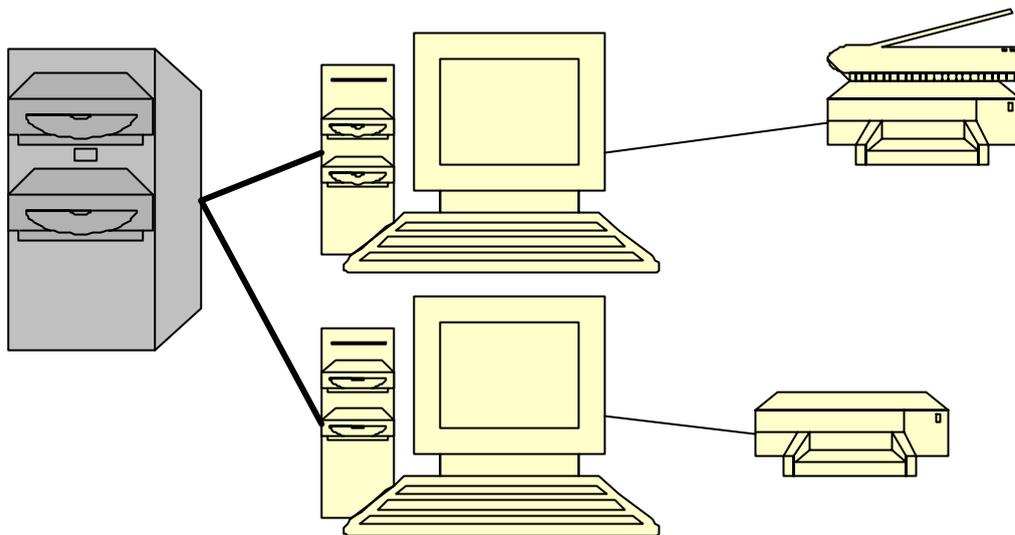
Man schuf also Vernetzungen, die darin bestanden, dass mehrere Datenstationen in einer Organisationseinheit aus Tastatur und Bildschirm bestanden (sog. Terminals). Die Terminals wiederum wurden mit Großrechnern verbunden, die in wohlbehüteten Räumen (eine frühe Form der „Datensicherung“!) untergebracht waren. Befehle zur Datenverarbeitung wurden an den Terminals eingegeben, sodann die Rechenleistung im (Remote) Rechenzentrum erbracht und das jeweilige Ergebnis wiederum am Terminal angezeigt.

Von Anfang an wurde so das Ziel verfolgt, Daten auf speziellen elektrischen Leitungssystemen zur Abarbeitung von A nach B zu schicken und anschließend bearbeitet zurück zu senden. Voraussetzung dafür war zunächst, dass der Computer über einen speziellen Anschluss, das so genannte Gate, verfügte und über entsprechende Leitungen mit einer entfernt liegenden Datenquelle (remote = entfernt) eines physikalisch getrennten Computers (Datenspeicher eines Remote Computers) verbunden wurde (Abb. 2).

---

<sup>25</sup> Zu Konfiguration, Nutzung und Ausstattung s. auch TRAEGER / VOLK (2001), RRZN (2001), BRÜGMANN (2001) u.a.

Auf diese Weise entstand eine Verbindung zweier ehemals separater Stand-alone-Rechner zu einem kleinen System vernetzter Computer, ein kleiner Verbund von Computern:



**Abbildung 2: „Minimal-Netz“**

Remote-Computer (grau unterlegt) und zwei angeschlossene Rechner, jeweils mit eigenen Datenspeicherungs- und -verarbeitungs-möglichkeiten sowie Peripheriegeräten Unten rechts Drucker, oben rechts Drucker mit Scanner).  
(Abb. erstellt durch Verf.)

Bei solchen „Kleinnetzen“ wurde der Datenaustausch zwischen den angeschlossenen Rechnern in aller Regel dadurch vorgenommen, dass Daten mit den jeweiligen Datenträgern (Disketten, CD, Magnetband oder jedes andere mögliche Speichermedium) von einem PC zum anderen transportiert wurden.

So oder ähnlich können mehrere Computer miteinander verbunden, also vernetzt werden (s. hierzu Kap. 2.2). Damit aber diese angeschlossenen Rechner sich nicht gegenseitig stören, die verschickten Daten beim Remote-Computer „richtig“ ankommen und dieser auch erkennen kann, was mit diesen Daten passieren soll, bedarf es zusätzlicher, abgesproche-

ner, spezieller Software und Regeln für den Datenaustausch zwischen den beteiligten Computern: den Protokollen.<sup>26</sup>

Ein weiterer Grund für die Vernetzung von Computern lag in militärischen Sicherheitserwägungen. Daraus entstand dann mit einigen „Zwischenstationen“ das heutige weltumspannende Daten- und Informationsnetz, das „Internet“ und mit ihm die am meisten genutzten Dienste innerhalb des Internet: das world wide web (auch www oder einfach „web“), die e-mail-Funktionen und vieles mehr.<sup>27</sup>

## 2.2 Gestaltung von Netzwerken

An dieser Stelle soll lediglich ein Einblick in unterschiedliche Möglichkeiten zum Aufbau von Netzwerken gegeben werden; technische Detailbetrachtungen sind in der Fachliteratur hinreichend vorhanden<sup>28</sup>. Ziel ist es hier, diejenigen technischen Umsetzungsmöglichkeiten darzustellen, die von besonderer Bedeutung für die in Kapitel 9 und 10 erforderlichen Betrachtungen sind. Alle weiteren, darüber hinausgehenden technischen Fragen sind bereits in der o.g. Literatur umfassend erörtert. Auch die anforderungsbezogenen Aussagen, welche Netzarten sich für welche Anforderungen anbieten, werden nicht hier gemacht; da derartige Betrachtungen abhängig sind von Datenaufkommen, logischen Verknüpfungen und physikalischen Gegebenheiten, werden sie in Kap. 9 aufgegriffen.

---

<sup>26</sup> Zur Darstellung der unterschiedlichen Protokollarten, der Zielrichtung der Protokolle und deren Bedeutung im Netz s. auch TRAEGER / VOLK (2001), BRÜGMANN (2001), COMER (1998), DERFLER (2001) u.a.m.

<sup>27</sup> Häufig werden die Begriffe „Internet“ und „WWW“ synonym verwendet. Es sei hier darauf hingewiesen, dass das WWW ein innerhalb des Internets angebotener Dienst ist, der durch Verlinkung (Hyperlinks) das „Springen“ von einer Seite zu anderen mit ähnlichen Inhalten, also letztlich das Surfen, ermöglicht. Weitere Details im Internet-Wörterbuch unter <http://www.networds.de>.

<sup>28</sup> TRAEGER / VOLK (2001), RRZN (2001), COMER (1998), DERFLER (2001), FRANK (1996), GIBBS (1995), KAUFFELS (1995), LIPINSKI (1998), BRÜGMANN (2001), RIGGERT (2002), LARISCH (2000) u.v.a.

Bereits vor der Möglichkeit, das weltumspannende Netzwerk und damit das www für zivile und private Zwecke zu nutzen<sup>29</sup>, entstanden aus den zuvor bereits genannten Gründen (Einsparung von Ressourcen, Kommunikationserfordernisse, Daten- und Programm-Sharing usw.) die ersten wenn auch kleinen internen Netzwerke innerhalb des Internets oder als Intranets davon losgelöst<sup>30</sup>. Sowohl im Hinblick auf technischen Gestaltungsaufwand als auch im Hinblick auf die Dimensionen unterscheiden sich solche Netzwerke deutlich.

Bei der Einrichtung von modernen Netzwerken, so wie sie mittlerweile für Verwaltungseinheiten, also auch für Schulen, vorgeschlagen werden, sind mehrere Gesichtspunkte und Komponenten zu berücksichtigen, die sich gegenseitig teils bedingen, teils beeinflussen. Ihr Zusammenwirken wird in der Fachliteratur (s. FN 27) ausführlich beschrieben. Für den „Umbau“ bestehender „alter“ Netzwerke gibt es umfangreiche Handreichungen, auch von Stellen der Bildungsverwaltung.

In den letzten Jahren haben sich als essentielle Komponenten herauskristallisiert:

- Server, Arbeitsstationen / Clients, Peripheriegeräte (wie Drucker, Scanner pp), Übertragungsmedien, Netzwerkkarten, Router, Hubs, Switches, Bridges, Gateways u.v.m. im Bereich Hardware
- Netzwerkbetriebssysteme, Protokolle usw. im Bereich Software

---

<sup>29</sup> Am 30.04.2003 feierte das www seinen zehnten „zivilen“ Geburtstag, s. hierzu WEB.de-Portale Internet vom 30.04.2003, s. Anlage 13.1

<sup>30</sup> Die Gestaltung eines Netzwerkes erfordert nicht, dass gleichzeitig eine Anbindung in das Internet erfolgt; Firmen- und Behördennetzwerke erreichen teils äußerst umfangreiche Ausmaße, orientieren sich an den durch das Internet erzielten technischen Errungenschaften (wie z.B. Nutzung der Protokolle), ohne jedoch über eine Anbindung an das Internet zu verfügen.

- darüber hinaus Topologien, Strukturen, Zugriffsverfahren und -regelungen, Netzwerktypen und viele weitere sonstige Komponenten.

Von diesen Komponenten können und sollen im Zusammenhang mit dieser Arbeit nur einige wenige Elemente etwas näher beleuchtet werden (Kap. 2.2, 2.3 und 2.4), da sie (nach Auffassung der Verfasserin) für die Planer in Schulen von besonderer Bedeutung sind.

### **2.2.1 Netzdimensionen**

Eine erste Unterscheidung wird getroffen bezüglich der räumlichen Ausdehnung von Netzwerken. Die gebräuchlichsten und bekanntesten Formen hinsichtlich der jeweiligen Ausdehnung sind das LAN (Local Area Network) und das WAN (Wide Area Network).<sup>31</sup> Zu weiteren, für Schulen und diese Arbeit weniger bedeutsame Unterscheidungen s. auch TRAEGER (2001).

Das LAN ist ein räumlich überschaubares Netz, das in der Regel auf einen Gebäudekomplex beschränkt ist, sich also gerade für schulische Vernetzungen anbietet.

Das WAN ist ein weiter ausgedehntes Netz, das auch geografische Grenzen überschreitet und Länder übergreifend und Kontinente umfassend arbeitet.

Während sich beim LAN die Nutzung von Netzverkabelungen anbietet, ist für das WAN die Frage der Übertragungswege von wirtschaftlicher und sicherheits-entscheidender Bedeutung. Die Wahl, ob es sich um ein

---

<sup>31</sup> Sowohl für die Definition von LAN als auch diejenige von WAN wird hier auf eher populär-fachliche Darstellungen zurückgegriffen (wie z.B. RIGGERT (2002), 12) und nicht auf die für Experten maßgeblichen Beschreibungen wie etwa bei LARISCH (2000), 39, 40, 277).

Funk-Netz handeln soll, oder ob die Anmietung abgeschirmter Leitungswege sicherer und sinnvoller scheint, welche Übertragungsmedien also schlussendlich genutzt werden sollen, ist vor Einrichtung und Aufbau des Netzes zu prüfen (s. hierzu die Ausführungen in Kap. 9 sowie zu weiteren Details C't 1999, Heft 6):

### **2.2.2 Übertragungsmedien**

In Zusammenhang mit dieser Entscheidung über das zu wählende Übertragungsmedium stellt sich zunächst die grundsätzliche Frage, ob kabelgebundene oder kabellose (=drahtlose oder auch leiterungebundene) Datenübertragung gewünscht wird.

Entscheidungsführend sollten neben wirtschaftlichen Erwägungen auch die Sicherheitsaspekte sein (s. hierzu Kap. 9) ebenso wie die vor der Verkabelung bzw. Vernetzung durchzuführenden Bedarfserhebungen. Der Datendurchsatz ist je nach Medium unterschiedlich in Geschwindigkeit (MBit/s) und Menge (Bytes), somit ist von Anfang an das gemessene und für zukünftige Entwicklungen zu erwartende Datenaufkommen in die Überlegungen einzubeziehen. Dabei sollte auch beachtet werden, dass die Entwicklungen der Technik so rasant voranschreitet, dass noch ein gewisser „Spielraum“ hinsichtlich der Leistungsfähigkeit der Übertragungsmedien einzuplanen ist – niemand kann konkret vorhersagen, welche Möglichkeiten eine Vernetzung in den nächsten Jahren neu schaffen wird. Auch für diese aber sollte ausreichend Kapazität vorgeplant werden.

Des Weiteren ist in die grundsätzlichen Überlegungen schon hier einzubeziehen, dass die zu treffende Entscheidung unterschiedliche Folgekosten nach sich ziehen wird: abhängig von der hier getroffenen Wahl ist im fortschreitenden Netzaufbau unterschiedlich zu investieren was z.B. die Auswahl von Netzwerkkarten, evtl. Access-Points (und damit Kosten, Sicherheit, Zukunftsorientierung usw.) u.ä. angeht.

Unterschiedliche Kabelarten repräsentieren unterschiedliche physikalische Eigenschaften; eng mit der Kabelart verbunden sind Fragen z.B. des im schulischen Bereich überaus wichtigen Brandschutzes, der Zugriffs- bzw. Abhörsicherheit, der innerhalb des Kabels auftretenden Störungen usw.

Hier sollen lediglich kurz die Vorzüge und Nachteile leitergebundener und leiterungebundener Systeme aufgezeigt werden<sup>32</sup>:

- Twisted-Pair-Kabel (unshielded = UTP, shielded = STP) sind Verkabelungsmöglichkeiten der einfachsten Form. Sie sind äußerst preiswert und auf Grund ihrer Flexibilität und Biegsamkeit leicht zu verlegen, können allerdings nur zur Überbrückung kurzer Distanzen etwa zwischen wenigen Räumen genutzt werden und sind, sofern es sich um nicht abgeschirmte Varianten handelt, störanfälliger als andere Kabelarten.
- Koaxialkabel sind preiswert und relativ störunanfällig; sie bieten sich allerdings dann nicht an, wenn größere Strecken (z.B. mehrere km zwischen mehreren Gebäuden) überbrückt werden müssen.
- Glasfaserkabel (=Lichtwellenleiter – LWL) sind die Verkabelungsart der modernen Netzwerke, in denen aus besonderen Gründen nicht auf leiterungebundene Vernetzung zurückgegriffen wird. LWL haben den Vorteil, einen hohen Datendurchsatz bis zu 50Gb/s zu ermöglichen, sicher und haltbar zu sein. Dabei ist das Kabel selbst durchaus kostengünstig, problematisch sind aber die Folgekosten, da erhebliche Gerätekosten (Hubs, Schränke usw.) zu erwarten sind.

---

<sup>32</sup> Zur detaillierten Darstellungen von Kabelarten und Verkabelungsvarianten vgl. HANSEN, H.R.: Wirtschaftsinformatik I (2001), S. 569 ff, auch RRZN: Netzwerke, Grundlagen (2001), S. 20 – 35, sowie LARISCH (2000), S. 131 – 173.

- Bei den leiterungebundenen Übertragungsarten ist als wesentlicher Vorteil zu betrachten, dass die Flexibilität der eingebundenen Rechner hinsichtlich ihrer räumlichen Nutzung größer ist und eine in bestehende bauliche Strukturen einzubindende Vernetzung ohne aufwendiges Verlegen von Kabeln durchgeführt werden kann. Von jedem beliebigen Ort (der funktechnisch noch erreichbar ist) innerhalb der Gebäude bzw. des Geländes ist jeder für den Zugang autorisierte Rechner in der Lage, auf das Netz zuzugreifen. Dies setzt voraus, dass die „Antennen“ (access-points) und Funknetzkarten aufeinander eingestellt sind, damit der Zugriff freigegeben werden kann und dass die maximale Reichweite der access-points nicht überschritten bzw. durch abgeschirmte Mauern und Funkstörungen eingeschränkt wird.<sup>33</sup>  
Die möglichen sicherheitsbezogenen Nachteile eines Funknetzes werden in Kap. 9 aufgegriffen.

Weitere technische Möglichkeiten, wie z.B. die Infrarot-Datenübertragung oder bluetooth-Technologie, sollen hier nicht näher beleuchtet werden. Sie spielen im Bereich von Netzwerken, wie sie in Schulen installiert werden können, eine lediglich untergeordnete Rolle. Denkbar ist eventuell eine Kombination zwischen Funk- oder LWL-Netz, in das über Infrarotschnittstellen externe Datenträger (wie PDA, Handys mit Office-Funktion o.ä.), die einzelne User außerhalb des Netzes nutzen, eingebunden werden können. Dies aber ist eine Variante, die im Einzelfall zu bedenken wäre und daher außerhalb der generellen Betrachtungen dieser Arbeit liegt.<sup>34</sup>

---

<sup>33</sup> Zur näheren Gestaltung von Funknetzen siehe TRAEGER (2001), RIGGERT (2002) sowie RRZN (2001).

<sup>34</sup> Detaillierte Ausführung zu den Vorteilen und Unterschieden hierzu finden sich in KURI (1999)

## 2.2.3 Vernetzungsarten und Netzwerk-Topologien

### 2.2.3.1 Peer-to-Peer-Vernetzung

Die einfachste Variante eines Netzwerkes ist die peer-to-peer-Vernetzung (s. Abb. 3). In einem derart gestalteten Netzwerk stehen die eingebundenen Rechner bezüglich der Funktionen, Dienste und Zugriffsrechte (auf Peripheriegeräte, Internet, wobei einer der eingebundenen Rechner als sog. „Host“ den Zugang zum Internet für alle anderen ermöglicht) gleichberechtigt nebeneinander<sup>35</sup>. Das gleichberechtigte Nebeneinander bedeutet auch, dass die beteiligten Rechner völlig autark sind hinsichtlich ihrer jeweiligen Softwareausstattung, ihrer Datenverarbeitung und Nutzung.

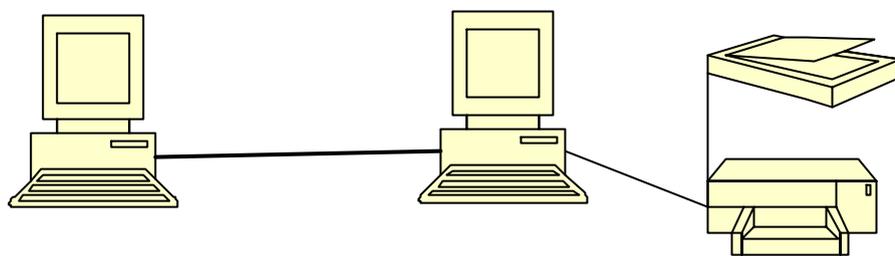
Die Direktverbindung der PCs geschieht mit so genannten Nullmodemkabeln oder mit so genannten Cross-Link-Kabeln und passender Steck-Karte. Im Grunde ist diese Art eines Netzwerkes eine archaische Unterform der im Folgenden dargestellten Bus-Topologie (s. Abb. 6). Spezielle Hardware, besondere Netzbetriebssysteme oder Netzsoftware sind nicht erforderlich; Lizenzfragen für die eingesetzte Software lassen sich rechtlich unproblematisch beurteilen, da für jeden eingebundenen Rechner eine Lizenz erforderlich ist. Jeder PC-Benutzer innerhalb dieses Netzes ist selbst verantwortlich für die Sicherheit und die Freigabe von Ressourcen auf seinem PC und im Netz.

Diese Eigenverantwortlichkeit der Nutzer stellt in umfangreichen Netzen eine Sicherheitslücke dar, das Erfordernis von Einzellizenzen hat u.U. weitreichende finanzielle Konsequenzen. Damit werden die mögliche Anzahl anzubindender Rechner und die räumliche Ausdehnung des Netzes wesentlich eingeschränkt. Peer-to-peer-Netze sind klassisch die im Heimnetzen genutzten Strukturen, die allerdings auch nur den beschränkten Erfordernissen dort genügen können. Peer-to-peer-Netze wurden in den

---

<sup>35</sup> s. hierzu auch RIGGERT (2002), LARISCH (2000), RRZN (2001)

Anfangszeiten der Vernetzungstendenzen auch in Schulen eingerichtet. Dazu lassen sich mehrere Gründe als Ursachen vermuten: zum einen spielte sicherlich die Tatsache eine Rolle, dass die mit den Vernetzungsarbeiten beschäftigten Lehrkräfte (die dies meist wegen des außerberuflichen Engagements zusätzlich übernahmen) die Form der Peer-to-Peer-Vernetzung aus dem privaten Bereich bereits kannten, zum anderen legte die geringe Anzahl von vorhandenen und zu vernetzenden Computern samt Peripheriegeräten eine solche Struktur nahe.



**Abbildung 3: Peer-to-Peer-Vernetzung**

mit zwei PC-Workstations (Desktop), verbunden durch Cross-Link, dazu ein von beiden anzusteuender Drucker sowie Scanner; Internet-Zugang über einen der beiden Rechner, der als Host fungiert.  
(Abb. erstellt durch Verf.)

Seither aber haben sich in den meisten Schulen die Anforderungen an ein funktionierendes Netz sowohl durch das Datenaufkommen als auch durch die Anzahl einzubindender Rechner weiterentwickelt. Alleine aus diesen Gründen, unabhängig von Fragen der Datensicherheit und der Aufgabenprofile an Schulen, sind diese Peer-to-Peer-Netze für die heutigen Anforderungen an Datenverarbeitungssysteme in Schulen aber überholt.

Eine zentrale Einheit, die sowohl die Software für die angeschlossenen PC zur Verfügung stellt (Serverdienst) als auch Zugriffsdaten verwaltet, gibt es nicht; die Benutzerverwaltung wird wegen der direkten Kontaktierungsmöglichkeiten sehr einfach, genügt aber ebenfalls nicht mehr heutigen Ansprüchen.

### 2.2.3.2 Client-Server-Netze

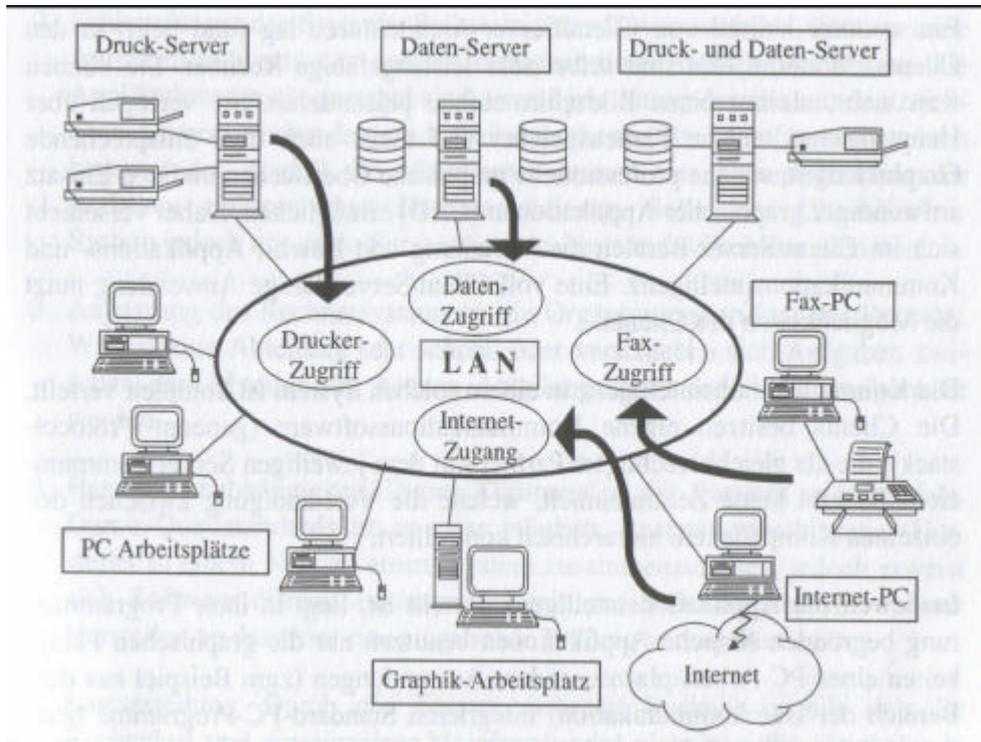
In den meisten Institutionen (Schulen, Verbände, Verwaltungen, Unternehmen usw.) werden jedoch heute viele PCs im Verbund mit Peripheriegeräten (Drucker, Datensicherungsanlagen usw.) arbeiten müssen, wobei je nach Tätigkeits- und Dienstprofil unterschiedliche Hierarchieebenen abzubilden sind. Dies und auch der erhöhte Datendurchsatz erfordern andere Netzwerkarchitekturen als sie das Peer-to-Peer-Netz bieten kann, Architekturen, bei denen im allgemeinen ein oder mehrere Steuerungs- und Verwaltungs-PCs - die Server - die angeschlossenen PC-Arbeitsstationen – die clients – verwalten, steuern und – je nach Dienstprofil – mit spezifischen Daten und Programmen „versorgen“<sup>36</sup>

Die Clients greifen jeweils auf diese zentralen Dienstrechner zu, melden sich dort an, werden autorisiert und dürfen dann die dort vorgehaltenen Leistungen nutzen. Sie können ggf. auch eigene Programme geladen haben und Daten generieren, können die zur Verfügung gestellten Daten bearbeiten, auf einem gemeinsamen Drucker ausgeben oder über den / die Server die Daten außer Haus verschicken u.a. mehr. Der Haupt-Server (Domain Controller) überwacht und verwaltet alle Tätigkeiten und muss daher bezüglich seiner Leistungsdimensionen und Kapazitäten die angeschlossenen Clients überragen.

Kleinere Netze kommen mit einem zentralen Rechner als Server aus, je größer aber das Netzwerk und je vielfältiger die gemeinsamen Bedürfnisse der angeschlossenen User, desto mehr spezielle Server (daher je nach Aufbau und Bedarf u.U. File-, Proxy-, Datenbank-, Mail-, Print-, Application-Server u.a.) hält es vor.

---

<sup>36</sup> Zu den Eigenarten und Vorteilen einer Client-Server-Architektur s. MÖRIKE (1995), Kap. 13, sowie LARISCH (2000), TRAEGER (2001) u.a.



**Abbildung 4: Beispiel einer möglichen Struktur eines Client-Server-Netzes mit mehreren Servern** TRAEGER (2001), S. 339

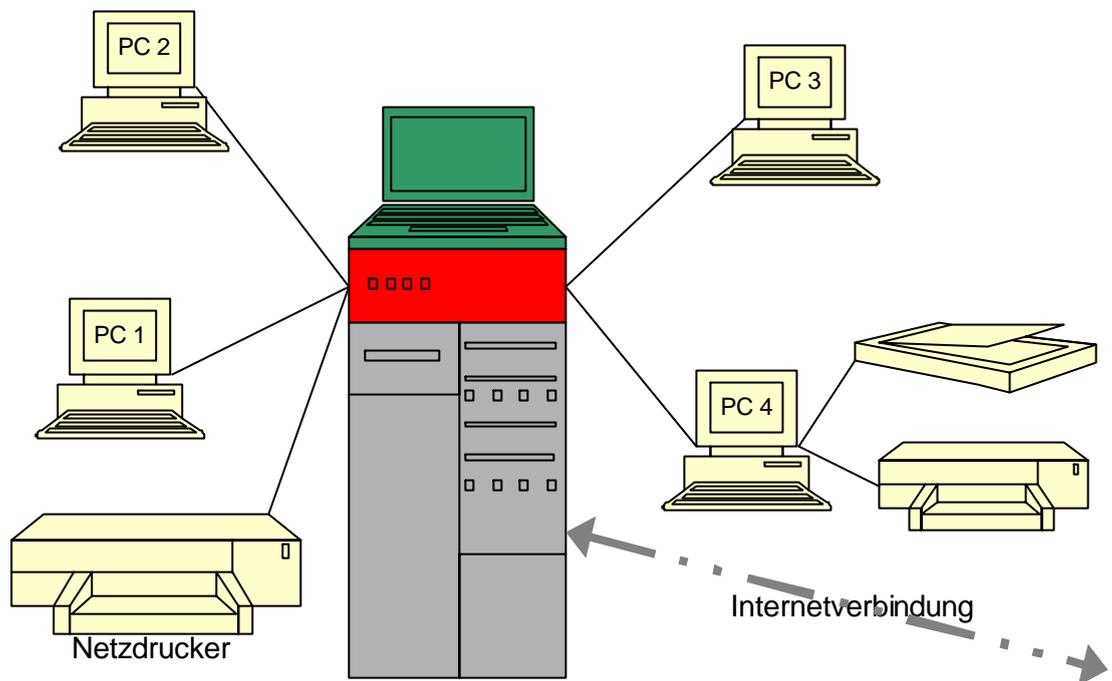
Solche Client-Server-Netze benötigen besondere Betriebssysteme, aber auch besondere Softwarelösungen für die Applikationen und Lizenzrechte (statt des Kaufs der reinen Anzahl von Lizenzen sind Regelungen denkbar z.B. für die Anzahl gleichzeitiger Zugriffe, Anzahl der User o.ä.).

Die konkrete Ausgestaltung eines Client-Server-Modells kann unterschiedliche Formen haben. Ungeachtet der räumlichen Ausdehnung eines Netzwerkes sind drei unterschiedliche reine Formen der Schaltung / Verkabelung gebräuchlich, auf die hier kurz eingegangen werden soll. Da schulische Netze in der Regel nicht erfordern, geographisch entfernte Liegenschaften miteinander zu verbinden oder eine Vielzahl unterschiedlicher Organisationseinheiten mit Teilnetzen zu vereinen, werden weitere Topologien, die sich eher für die Vernetzung solcher Organisationsstrukturen eig-

nen, hier nicht angesprochen, ebenso wenig die unterschiedlichen Mischformen der im Folgenden vorgestellten drei Topologien:

- Stern-Topologie

Um eine zentrale aktive Einheit herum (Impulse werden aktiv gesteuert, daher bezeichnet man dieses Element als aktive Netzkomponente) werden sternförmig jeweils mit eigenen Anschlüssen an dieses Element die benötigten PCs aufgebaut (s. Abb. 5). Die aktive Steuerung wird durch einen Verteiler, den so genannten Hub oder – bei umfangreicheren Netzwerken – dem Schaltschrank, übernommen. Dabei hat jeder angeschlossene Rechner seine eigene Verbindung zum Hub und kann ungehindert durch andere Rechner arbeiten. Dies auch dann noch, wenn einzelne Stationen ausfallen und auch ohne Rücksicht auf den Datendurchsatz, den die Verbindung zum Hub zulässt, da die Daten dort in der Reihenfolge abgearbeitet werden (s. Abb. 5, weitere Ausführungen in TRAEGER (2001), S. 172 ff). Ein so gestaltetes Netzwerk ist aktuell sehr gebräuchlich und bietet sich zur Schaltung von überschaubaren räumlichen Ausdehnungen an. Bei einer derartigen Client-Server-Lösung ist es dabei unerheblich, ob die so miteinander verbundenen Rechner auch zu einer identischen Arbeitseinheit mit gleichen Arbeitsinhalten oder –Schwerpunkten gehören. Der Server sorgt für eine logisch richtige Verteilung, die nicht identisch sein muss mit der physikalischen Zusammenlegung der PCs. So können z.B. bei räumlicher Nähe Sekretariat, Schulleitung und Informatikräume physikalisch-topologisch sternförmig zusammengelegt werden, denn damit ist nicht notwendigerweise auch die Nutzung gleicher logischer Inhalte verbunden.



**Abbildung 5: Stern-Topologie**

An einen zentralen Server (grau) mit Laptop zur Ansteuerung (grün) sind Arbeitsstationen (PC 1 bis PC 4) – Desktops – über Hub (als aktive Komponente - rot) angeschlossen. Sie nutzen gemeinsam einen ebenfalls über den Hub anzusteuernenden Netzwerkdruker (links). Einer der Desktop-Rechner ist zusätzlich mit eigenem Drucker und Scanner ausgestattet (PC 4). Die Schnittstelle zum Internet wird durch den Server zur Verfügung gestellt (blauer Pfeil).  
(Abb. erstellt durch Verf.)

- Bus-Topologie

Kern dieser Topologie ist der Bus, ein zentrales Kabel mit Steuer-, Daten- und Adressleitungen, an das alle erforderlichen Geräte mit einer eigenen „Zuleitung“ angeschlossen werden. Diese Geräte müssen sich den Bus für ihren gesamten Datenverkehr teilen; bei hohem Datendurchsatz ist also die Frage der Leistungsfähigkeit und der Kabelart<sup>37</sup> entscheidend für das ungestörte Funktionieren des Netzes. Einer der wesentlichen Vorteile

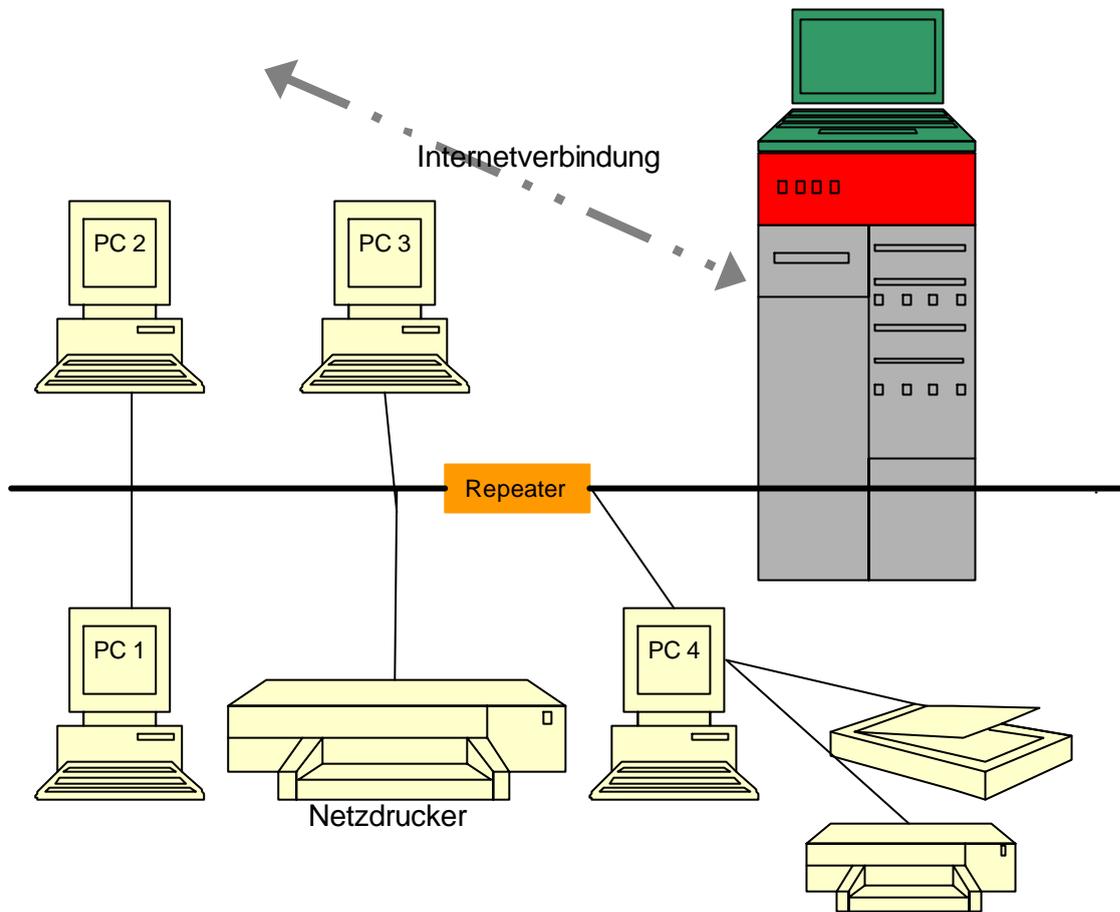
---

<sup>37</sup> Zu den unterschiedlichen Kabelarten, Querschnitten und Leitungstypen siehe auch TRAEGER (2001)

dieser Netzform ist, dass der Aufbau kostengünstig und relativ einfach erscheint.

Allerdings ist bei räumlich weit auseinander liegenden anzuschließenden Rechnern darauf zu achten, dass die Länge des Zentralkabels bedeutsam für die Signalstärke und –deutlichkeit innerhalb des Netzes und damit für die Zugriffe auf Serverleistungen ist. Sofern auf Grund der Kabellänge die Impulse nicht in ausreichender Stärke aufgenommen werden, ist die Zwischenschaltung so genannter „Repeater“ erforderlich.

Auch in einer solchen Konstellation (Abb. 6) wird wiederum (wie auch bei einer Stern-Topologie möglich, wie in Abb. 5 dargestellt) die Schnittstelle zum Internet durch einen eigenen Server bzw. eine Serverleistung des eingebundenen Servers zur Verfügung gestellt und von allen angeschlossenen Rechnern genutzt.

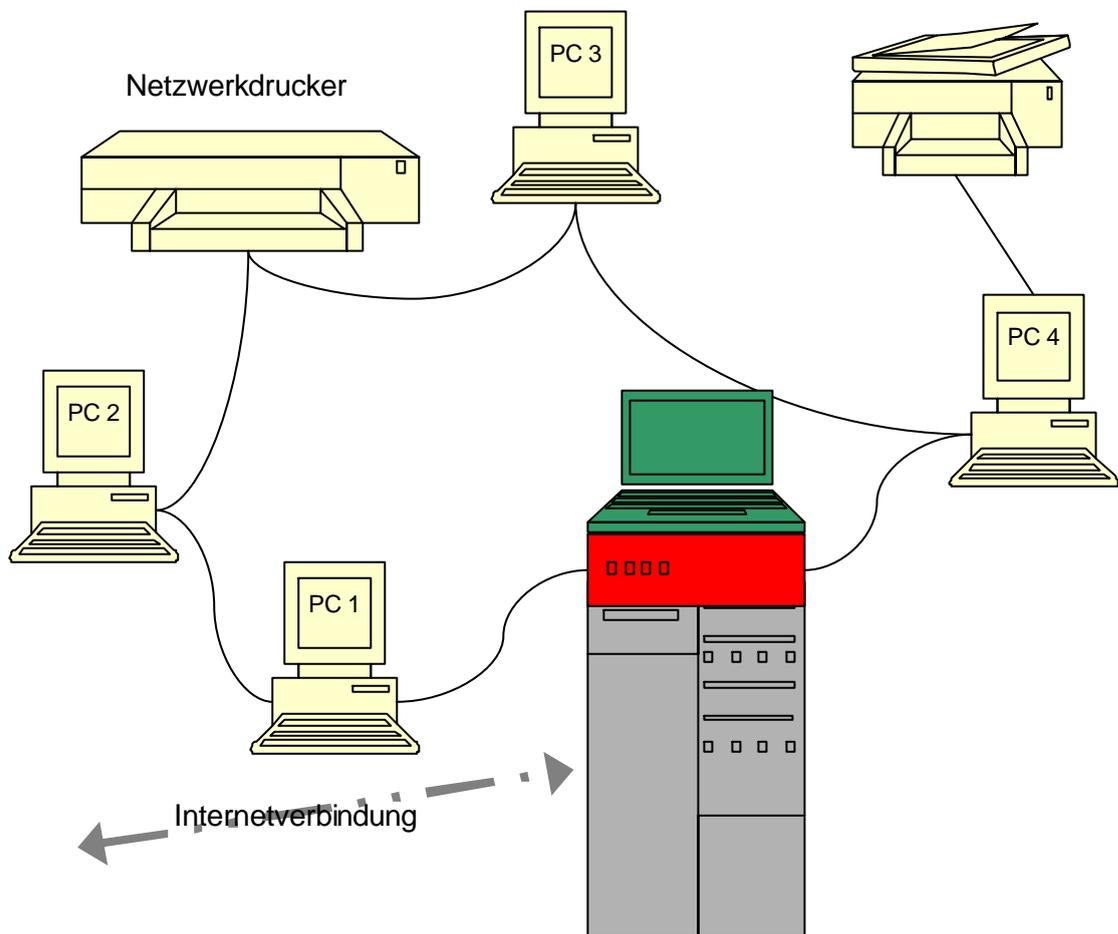


**Abbildung 6: Bus-Topologie**

Zentrales Kabel (Bus) mit vier jeweils mit eigener Zuleitung angeschlossenen Workstations (PC 1 – PC 4), einem Netzdrucker und einem nur durch eine Station zu nutzenden Einzelplatzdrucker und Scanner (PC 4). Steuerungs-PC (Laptop – grün), Server (grau) sowie aktive Komponente (Hub – rot) sind ebenfalls eingebunden, zur Verstärkung der Signale ist ein Repeater (gelb) zwischengeschaltet. Wiederum übernimmt der Server den technischen Internet-Zugang.  
 (Abb. erstellt durch Verf.)

- Ring-Topologie

Ein in der Praxis weniger verbreitetes Modell ist die Ringtopologie. Hier wird an ein topologisch in sich geschlossenes Zentralkabel jedes anzuschließende Gerät gekoppelt. Das bedeutet jedoch, dass alle Daten, Impulse, Netzaktivitäten auch in allen angeschlossenen Elementen (Server und Clients) aufgenommen und zumindest weitergegeben werden. Das wiederum macht dieses Netzvariante wenig komfortabel und vielfach ausfallgefährdet, da jedes einzelne angeschlossene Element funktionsfähig sein muss, um auch das Gesamtnetz funktionsfähig zu halten.



**Abbildung 7: Ring-Topologie**

Vier angeschlossene Workstation (PC 1 – PC 4), Netzwerkdrucker sowie einem Einzelplatzdrucker mit Scanner (an PC 4) Steuerungs-Laptop, Hub und Server, Internet-Zugang wiederum durch Server.  
(Abb. erstellt durch Verf.)

Wie auch immer eine Netzwerkstruktur angelegt wird, ob eines der vorstehenden Modelle in reiner Form gewählt wird oder ob eine Mischform ausgestaltet wird, die Entscheidung ist abhängig von den bereits genannten Rahmenbedingungen. Ihr Ziele und Zwecke aber sind – egal in welcher topologischen Struktur - identisch: sie soll den sie nutzenden Personen ermöglichen, direkte Kommunikation zu führen, Informationen zu erheben, zu sammeln, auszuwerten und zu verarbeiten. Und dies nicht nur im Bereich der Freizeit oder Freistunden in der Schule durch Internet-Surfen, MP3-Files laden, Online-Handeln und Ähnlichem, sondern auch im beruflichen Alltag. So wurden einerseits durch technologischen Fortschritt neue Bedürfnisse der Gesellschaft formuliert, andererseits aber gleichzeitig durch diese Fortschritte – z.B. in Form von Netzwerken - erfüllt.

### **2.3 Der Wandel der Gesellschaftsform: Von der Produktions- zur Informationsgesellschaft**

Der Weg der IuK-Technologie in alle Bereiche des Lebens, die Privathaushalte eingeschlossen, sowie die stetige und rasante Weiterentwicklung der technischen Möglichkeiten machten einen Wandel möglich (und erforderlich), der sich bis heute fortsetzt, sich weiter fortsetzen wird und sich sogar noch beschleunigt zeigt.<sup>38</sup> Diese Beschleunigung bewirkt einen kaum überschaubaren Innovationszyklus der technischen Weiterentwicklungen, der nicht etwa auf die Erfordernisse „ernster“ Anwendungen (wie Textverarbeitungsprogramme, Tabellenkalkulationen und User-Programmierungen wie Autorensoftware u.ä.) zurückzuführen ist, sondern vielmehr Ergebnis des privaten Freizeitnutzers, der Online Videos sehen

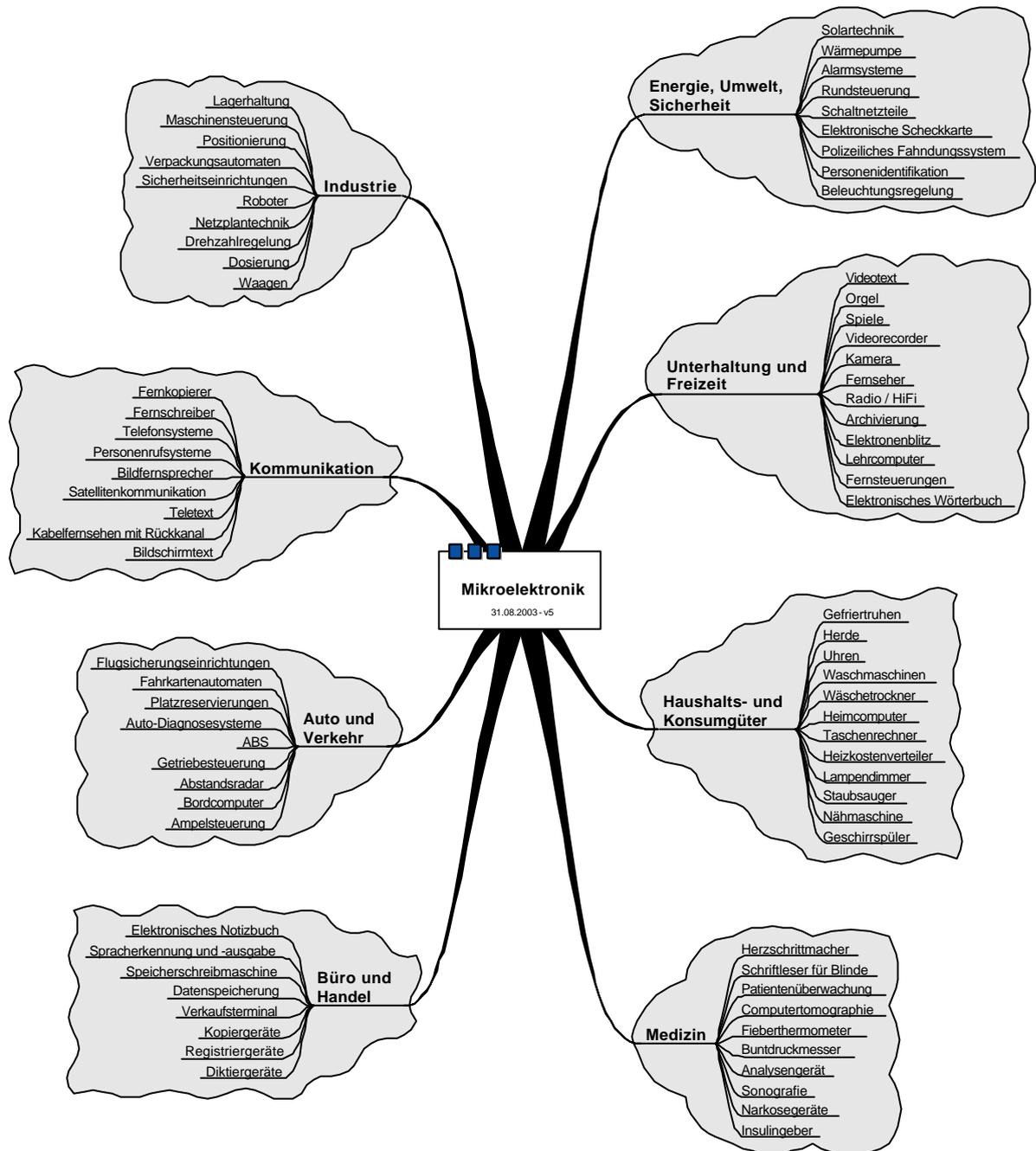
---

<sup>38</sup> Noch 1996 werden visionäre Zukunftsszenarien als besonders kühne Voraussagen entwickelt, die bereits heute durch die Innovation technischer Entwicklung erreicht, teils überholt sind. So stellen REEB / SANDER (1996) dar, dass durch technische Entwicklung und Nutzung gleicher digitaler Basistechnologien in allen Bereichen die Verknüpfung von Sprache, Daten und Bildern möglich werde. S. hierzu REEB, H.-J.: Kommunikation im Wandel; in: Wochenschau Nr. 3 / 4, Ausgabe Sek. II: Multimedia-Informationsgesellschaft; Frankfurt 1996

und Spiele nutzen will, dazu hochleistungsfähige Video- und Grafikkarten benötigt, Prozessorenleistungen als wesentlich ansieht, von denen noch vor wenigen Jahren nur zu träumen war. Damit ist heute ein Level erreicht, das noch zu Beginn der Entwicklungen nur als Vision vorhanden war und in manchen Bereichen als absolut außergewöhnlich galt.

Bereits 1985 stellt die SIEMENS-AG in der von ihr herausgegebenen Broschüre „Chancen mit chips“ heraus, dass die Mikroelektronik bereits eine Vielzahl von Lebensbereichen bestimmte und vereinfachte. Einige der dort dargestellten Anwendungsgebiete sind heute bereits so zur Selbstverständlichkeit geworden. Daraus folgt, dass häufig gar nicht im Bewusstsein steht, dass ein Gerät – z.B. der Kühlschrank - überhaupt ein mikroelektronisches Steuerungselement enthält; erst im Zusammenhang mit der Jahrtausendwende wurde der Blick wieder auf diese Geräte gelenkt (s. S. 41).

Die folgende Darstellung (Abb. 8, vergleichbare Übersichten etwa bei KIRCHMAIR (2001), S. 52) ist inhaltlich übernommen von und in der Darstellung angelehnt an die Übersicht in SIEMENS AG (1985), die – übertragen auf heutige Gegebenheiten – nur einen Teil der Möglichkeiten aufzeigt:



**Abbildung 8: Nutzung mikroelektronischer Steuerungselemente**

Geordnet nach 8 wesentlichen Bereichen wird nur eine Auswahl derjenigen Systeme, Geräte und Arbeitsbereiche dargestellt, die durch Mikroelektronik gesteuert werden. Inhaltlich übernommen aus SIEMENS (1985) (Gestaltung durch Verf.)

Diese Übersicht (Abb. 8) allerdings geht nicht auf den komplexen Bereich ein, den der Wandel für das Lernen, die Bildungsarbeit und –politik und die Schul- und Hochschullandschaft mit sich gebracht hat und noch mit sich bringen wird. 1999 stellte Bundespräsident Herzog beim Deutschen Bildungskongress in Bonn fest, dass man ...*die Pädagogik für das Informationszeitalter ... erst noch erfinden ...*“ müsse.<sup>39</sup>

Mit dieser Aufgabe befassten sich Wissenschaftler der unterschiedlichsten Disziplinen zum Ende des letzten Jahrhunderts, das Thema war ein „dankbares Feld“ für Abhandlungen und Veröffentlichungen zahlreicher Publizisten und Medienexperten, Sozialwissenschaftler und Technikphilosophen, Experten aus der Wirtschaft und Pädagogik. Auf die Kernelemente der so entstehenden Gesellschaftsformen sowie den Ablauf der Verwandlung soll daher hier nicht näher eingegangen werden. Um hierzu nähere Informationen zu erlangen, ist die themenspezifische Literatur heranzuziehen. Hier sei aus der Vielzahl der Veröffentlichungen lediglich auf einige richtungsweisende Werke verwiesen wie BARON (1997), CHOMSKY (1996), CEBRIAN (1999), MUTIUS (2000).<sup>40</sup>

Als Ursache für derartige Veränderungen wird jedoch nicht nur technische Innovation herangezogen werden können, auch Veränderungen in den Gesellschaftsstrukturen und den Einstellungen und Wertvorstellungen der Bevölkerung sind zu betrachten.<sup>41</sup>

---

<sup>39</sup> s. [http://www.bundespraesident.de/top/dokumente/Rede/ix\\_12049.htm](http://www.bundespraesident.de/top/dokumente/Rede/ix_12049.htm)

<sup>40</sup> Eine Recherche im Internet mit der Suchmaschine „Google“ erbringt mit den Suchbegriffen „Von der Produktionsgesellschaft zur Informationsgesellschaft“ weit über 100 Einträge mit jeweils weiteren Verzweigungen. Weitere Abfragen in unterschiedlichen Portalen mit dem Stichwort „Informationsgesellschaft“ ergaben: OPAC – Bibliothekenkatalog Uni Wuppertal - 97 Veröffentlichungen; KVK – Karlsruher Virtueller Katalog – bundesweite Abfrage – 985 Veröffentlichungen; FIZ Technik – Fachinformationszentrale – allein im Bereich IuK noch drei Veröffentlichungen (Stand: 23. August 2003).

<sup>41</sup> Schon 1996 ergab eine repräsentative Forsa-Umfrage, dass die Mehrheit der Befragten das Erlernen des Umgangs mit dem PC für sehr wesentlich erachtet. Vgl. hierzu SANDER, W.: Sozialer Wandel – der „Multimedia-Bürger“; in: REEB (1996), S. 122.

Durch den Einsatz der IuK-Technologie rückt die Welt erneut weiter zusammen. Die Möglichkeit, weltweit aktiv in unglaublicher Geschwindigkeit Informationen<sup>42</sup> abzurufen und zu verarbeiten, ist durch das Internet und andere Datennetze und Informationspools gegeben.<sup>43</sup> Das Bedürfnis der Menschen, auch mit räumlich weit entfernten Personen kommunizieren zu können, Einblick in andere Kulturen und Lebensweisen zu erhalten, Informationen über alle möglichen Fragen zu erlangen (und nicht, wie bislang in den tradierten Medien, lediglich als Rezipienten damit „bedient“ zu werden), zieht sich durch alle Alters- und Gesellschaftsschichten.

Die Veränderung der Gesellschaft nach der Produktionsgesellschaft und der Dienstleistungsgesellschaft zu einer Informationsgesellschaft<sup>44</sup> nimmt ihren Lauf, wobei diese Entwicklung eben durch das Internet entscheidende Prägung erhält. Diejenigen Menschen, die diese moderne Kommunikationsstruktur nicht nutzen können oder wollen, haben keinen Zugriff auf den immer weiter anwachsenden Bereich des Wissens- und Informationspools. Anders als zuvor sammelt man die notwendigen Informationen nicht mehr nur in Büchern und Bibliotheken oder Videotheken und Mediotheken.<sup>45</sup> Vielmehr fließen die Informationen und das Wissen der Menschheit in den Datennetzen, ständig aktualisiert, dauernd und zu jeder

---

<sup>42</sup> Über den Informationsbegriff, die Bedeutung von Informationen deren Strukturen im gesellschaftlichen Kontext s. FLEISSNER, P.: Der Mensch lebt nicht vom Bit allein...: Information in Technik und Gesellschaft. Frankfurt / Main 1998, 3. Aufl., sowie KIRCHMAIR, G.: Digitale Klüfte. Aktuelle Anwendungen und soziale Auswirkungen des Internet in der Gesellschaft; Wien 2001

<sup>43</sup> S. hierzu Ministerium für Wirtschaft und Mittelstand, Technologie und Verkehr des Landes NRW / Ministerium für Schule und Weiterbildung des Landes NRW: NRW-Schulen ans Netz; Verständigung weltweit; Düsseldorf 1996

<sup>44</sup> Ganz speziell zu diesem Gesichtspunkt sei verwiesen etwa auf BARON (1997); KIRCHMAIR (2001) (hier vor allem S. 41 – 86).

<sup>45</sup> REEB, H.-J.: „...**Buch und Multimedia – ein Vergleich** Was kann man mit einem normalen Buch alles „machen“, und was sollte man mit einem elektronischen Buch – darüber hinaus – alles machen können...“ in: REEB / SANDER (1996), S. 134 f

Tages- und Nachtzeit verfügbar. Dabei ist nicht immer ad hoc erkennbar, ob die verfügbaren Daten, das präsentierte Wissen einer realen Wirklichkeit entstammen oder einer virtuellen Realität (Cyberspace) zuzurechnen sind, ob die Daten und Informationen vertrauenswürdig, „echt“ oder manipuliert, variiert, „unecht“ sind.

Aber eben deshalb hat sich auch der klassische Inhalt des Lernens verändert.<sup>46</sup> Ständige Verfügbarkeit von Daten führt dazu, dass das Lernen von Fakten und Sachwissen mehr und mehr in den Randbereich gerückt wird. Der medienkompetent Lernende der heutigen Zeit holt sich die benötigten Informationen aus dem Internet.<sup>47</sup>

An dieser Stelle sollen einige wenige kennzeichnende Neuerungen in verschiedenen Lebensbereichen betrachtet werden, die durch die IuK-Technologie entstanden sind:

- Die Güterherstellung, in denen das reine Handwerk (im eigentlichen Sinne des Wortes) und seine Kenntnis zur erfolgreichen Berufsausübung ausreichten, hat an Bedeutung entscheidend verloren. Der moderne Handwerker hat fundierte Kenntnisse über die PC-gestützte Steuerung seiner Maschinen, weiß um die Ausstattung mit CPU und die – je nach Produktion unterschiedliche – Programmierung seiner Maschinen, genau so wie er seine Buchhaltung, seine Steuererklärung und jegliche Büroarbeit mit entsprechender Software am PC erledigt.
- Moderne Unternehmen jeglicher Größenordnung verfügen über ausgeklügelte interne Datenverarbeitungsnetze mit entsprechenden Dienst- und Zugriffshierarchien, und sie sind nur dann am

---

<sup>46</sup> Vgl. u.a.: STRUCK, P.: Die Schule der Zukunft. Von der Belehrungsanstalt zur Lernwerkstatt. Darmstadt 1996; BILDUNGSKOMMISSION NRW (Hr.): Zukunft der Bildung, Schule der Zukunft. Neuwied 1994

<sup>47</sup> vgl. REEB, H.J.: Herausforderungen für Bildung und Ausbildung; in: REEB / SANDER (1996), S. 125 ff

Markt erfolgreich, wenn sie ihre Fortschrittlichkeit auch durch die Nutzung moderner Präsentationsformen dokumentieren und mit eigener Site im Internet vertreten sind.

- E-Commerce nimmt immer weiter zu, Einkaufen über das Netz ist Normalität geworden, Einzelhandelsketten, die nicht zumindest im Netz Werbung betreiben, möglichst auch verkaufen, sind nicht auf neuestem Stand der Technik. Rein virtuelle Unternehmen gewinnen immer mehr an Bedeutung<sup>48</sup>, die Möglichkeit des privaten Handels wurde durch das Internet erheblich ausgeweitet (man betrachte nur die im Internet boomenden Auktionsmöglichkeiten, allen voran „Marktführer“ ebay).
- Selbst e-government wird zunehmend angeboten und genutzt: das Abrufen von erforderlichen Vordrucken für An- und Ummeldungen, die online-Steuererklärung, die Reservierung von Wunschkennzeichen bei den Straßenverkehrsbehörden usw. machen bürgerorientierte Verwaltungsarbeit aus und zeigen die Bemühungen der öffentlichen Verwaltung, mit der technologischen Entwicklung Schritt halten zu wollen.
- Die Verschmelzung unterschiedlicher Kommunikationsmedien führt zu einer lückenlos möglichen Nutzung aller verfügbarer Medien. Der Zugang ins Internet über Handy, WAP-Funktionen, MMS, PC-Telefonie usw. verwischen die ehemals fest gefügten Grenzen der technischen Möglichkeiten. Es gibt keine Beschränkung auf einzelne Hardwaresysteme mehr, stattdessen wird die Verbindung unterschiedlicher Systeme zur Normalität.
- Alleine die mit dem Jahrtausendwechsel einhergehenden Befürchtungen, damals unter dem Stichwort Y2K in aller Munde, zeigten die unerwartete Verbreitung auch verborgener computergestützter Systeme (sog. embedded systems). Kaum ein Kühl-

---

<sup>48</sup> s. hierzu MÖRIKE (1995), Kap. 22: Virtual Reality – schöne neue Welt

schrank, Fernseher, Videorecorder, bei dem nicht Befürchtungen über die eventuelle Unfähigkeit zur Umstellung auf das Jahr 2000 auftraten.

Diese wenigen Beispiele zeigen, dass computergestützte Technik unwiderruflich Einzug in alle Bereiche des Lebens genommen hat.

Damit ist der PC unverzichtbarer Bestandteil der Lebensrealität<sup>49</sup> geworden. Gerade im Zusammenhang mit der Nutzung des Internets ist aber auch zu beachten, dass es gerade durch diese Möglichkeiten der permanenten Kommunikation, des ständigen Informations- und Datenaustausches zu einer Art „Entprivatisierung“ der Einzelperson kommen kann bzw. sogar kommen muss, die wiederum zu Reaktionen z.B. im Bereich des Datenschutzes und der Datensicherheit für diese Einzelnen führen muss (s. hierzu Kap. 9).

Auch für Kinder ist der Computer aus dem Leben nicht mehr wegzu-denken; der Umgang mit PC und seine Bedienung sind als wesentliche Kompetenz einzustufen und wird seit Jahren als immanenter Bildungsauftrag gesehen, wenn auch über Einzelfragen des „Was“, „Wann“, „Womit“ und „Wie“ bei Politikern, Medien, Wirtschaftsvertretern, Didaktikern, Lehrern und nicht zuletzt Schülern und Eltern immer noch unterschiedliche Vorstellungen bestehen.

---

<sup>49</sup> Anm. d. Verf.: Die Nutzung des PC ist also nicht etwa als Flucht vor der Realität zu sehen, wie vormals die Kritiker den Usern vorwarfen, vielmehr ist diese Nutzung eben die Realität der Jetzt-Zeit. Dazu GLOTZ, P.: „:::Viele Kulturpolitiker, Lehrer und Pädagogikprofessoren neigen dazu, das Toben im Matsch oder die „Reise nach Jerusalem“ gegen den Computer in Stellung zu bringen. Sie verkennen dabei, dass jede Erziehung auf Vielseitigkeit, Filterfähigkeit und Media-Mix drängen muss“. Vortrag im Rahmen des 1. TeleLearning-Symposiums der DEUTSCHEN TELEKOM (1995)

### 3 Mikroelektronische IuK-Technologien und Schule

Der Auftrag der Schulen, Kinder für die Lebenswirklichkeit zu befähigen, kann demzufolge nicht vor dem PC Halt machen. Die grundsätzliche bildungspolitische und auch pädagogische Diskussion hierzu ist in den 80er und 90er Jahren des letzten Jahrhunderts in aller Breite und Tiefe geführt worden und nunmehr grundsätzlich positiv entschieden.<sup>50</sup>

Parallel dazu erfolgte die sich ebenfalls verändernde technische Umsetzung in Anpassung an die jeweiligen Diskussionsstände: Auch in Schulen wurden zunächst Stand-alone-Rechner verwendet, dann zur Reduzierung der Kosten mehrere Rechner mit einem Peripheriegerät verbunden (z.B. 3 PCs an einen Drucker angeschlossen). Mit dem Verschieben der Bedeutung der PCs entstanden erste „echte“ Netzwerke in den frühen 90er Jahren. Sie wurden zunächst in den Informatikräumen der Schulen eingerichtet als so genannte pädagogische Netze („Master-Eye“). Ende der 90er Jahre mit der Positionierung der Diskussionsergebnisse zum heutigen Stand ging ein Ruck durch die PC-Landschaft der Schulen: hauptsächlich getragen von Initiativen auf Bundesebene (z.B. „Schulen ans Netz“, [www.san-ev.de](http://www.san-ev.de)), unterstützt von Landesprojekten und gesponsert durch die Wirtschaft wird eine flächendeckende Anbindung ans Internet angestrebt und umgesetzt.

Computer, ihre Nutzung, die Kenntnis der Möglichkeiten müssen seither notwendigerweise in den schulischen Alltag überführt, die Vermittlung der erforderlichen Medienkompetenz in den pädagogischen Auftrag und die Aufgaben der Schulorganisation und –verwaltung im weitesten Sinne integriert werden. Dazu ist notwendige Voraussetzung die Kenntnis, welche Chancen sich durch die Nutzung der Computertechnologie im schulischen Alltag bieten.

---

<sup>50</sup> VON STITZKY (1995), TREUMANN (2002), TULODZIECKI (1996) (2002), STRUCK (1996), SCHELL u.a. (1999), MITZLAFF (1997), BÜTTNER (1999) u.a.

Zur Nutzung der Computer-Technologien sind unterschiedliche Zielrichtungen innerhalb der Schule zu nennen.<sup>51</sup> PCs können demnach genutzt werden,

- als selbständiges Unterrichtsthema, etwa zur Behandlung von Inhalten über Hardware, Software, Programmierung usw. In diesem Zusammenhang ist allerdings bedeutsam, dass Schüler heute oft den reinen Umgang mit dem Medium als alltägliche Selbstverständlichkeit ansehen. Also nicht nur die Nutzung der Technik ist als Unterrichtsgegenstand bedeutsam, vielmehr sollten verstärkt auch daraus resultierende Inhalte wie Hardware- und SoftwareAspekte, Bedeutung und Nutzen unterschiedlicher Betriebssysteme u.ä. in den Unterricht einbezogen werden. Kenntnisse über Sicherheitsrisiken (z.B. der Datensicherheit) zu erlangen und entsprechende Vorsorgemaßnahmen gezielt und sicher einsetzen zu können, müssen zusätzliche Ziele im Unterricht werden.<sup>52</sup>
- zur Beschaffung von Informationen für die Unterrichtsvor- und –nachbereitung durch Recherchen in Datenbanken und Portalen unterschiedlicher Richtungen sowie zur Nutzung von Newsgroups und Foren. Nutzender Personenkreis sind demzufolge Lehrerinnen und Lehrer für ihre Unterrichtsgestaltung und SchülerInnen und StudentInnen für Hausaufgaben, Referate und viele andere Lernsituationen.
- zur Vorbereitung und / oder Gestaltung des Unterrichts innerhalb eines Klassenverbandes und damit beschränkt auf den

---

<sup>51</sup> Die Diskussionen haben sich jedoch im Laufe der Jahre inhaltlich verschoben: So spielte in den 80er Jahren noch das Programmieren algorithmischer Probleme eine wesentliche didaktische und pädagogische Rolle: „Programmieren als vierte Kulturtechnik?“. –ausführliche Erörterungen der didaktischen, pädagogischen und schulpraktischen Aspekte eines Einsatzes von Computern im Unterricht sei verwiesen auf TULODZIECKI, G. / HARZIG, B. (2002)

<sup>52</sup> Zu den mit der exzessiven PC- und Internet-Nutzung verbundenen Gefahren s. auch RIFKIN, J. (2002)

Klassenraum, etwa durch Einsatz von Textverarbeitungs-, Grafik- oder Lernsoftware, durch Einsatz von Autorenprogrammen, Einrichten virtueller Klassenzimmer (s. hierzu [www.pupil.lo-net.de](http://www.pupil.lo-net.de)) u.ä.

- zur Durchführung von Unterricht, der sowohl Klassenverbände als auch schulische, regionale oder nationale Grenzen überwinden kann. So können z.B. durch Vernetzung der Schule und ausreichend Zugang zu einem der zahlreichen Internet Messenger – natürlich nach Beachtung der sicherheitsrelevanten Fragen – als Medium für Fremdsprachenunterricht eingesetzt werden. So erfährt die Brieffreundschaft traditioneller Art (auf die als zusätzliche Gestaltung allerdings auch nicht gänzlich verzichtet werden sollte) eine neue Dimension: Unterhaltung in Dialog- oder Konferenzform, Kommunikation via PC, preiswert, schnell, in Realzeit und mit direkter Antwortmöglichkeit.<sup>53</sup>
- zur Verwaltung schulisch relevanter Daten, so. bspw. Schüler-, Lehrerdaten, zu nutzen durch Schulleitung und Sekretariat, Schulverwaltung, evtl. auch Lehrerinnen und Lehrer, soweit die Daten zugänglich gemacht werden dürfen.<sup>54</sup>
- zur Internet-Präsentation der Schule, die sowohl als Unterrichtsinhalt zur Gestaltung von Web-Sites als auch zur Darstellung der Schule mit Werbecharakter dienen kann (unter den Prämissen des Datenschutzes und der Datensicherheit, vgl. hierzu Kap. 9 und 10),

---

<sup>53</sup> Zu grundlegenden Argumenten für eine Vernetzung von Schul-PC sowohl in Form eines Intranet als auch in Form eines Internet-Zuganges, wie er für die Messenger-Nutzung erforderlich ist, s. TULODZIECKI, G. / HARZIG, B. (2002), S. 167 ff

<sup>54</sup> Bei Vernetzung der Schulen mit den Aufsichtsbehörden können als zusätzlich Nutzende auch die Lehrerinnen und Lehrer selbst hinzukommen, die z.B. Beihilfeanträge im Intranet ausfüllen könnten und ähnliches mehr (s. hierzu Kap.10).

- zur „grenzenlosen“ Kommunikation im Internet.<sup>55</sup>

Jeder dieser Bereiche, jede dieser Zielsetzungen erfordert eine spezifische technische Ausgestaltung der Computer bzw. Netzwerk-Topologie in der Schule, erfordert seine spezifische Hardware-Basis, eigene Softwareinstallationen, eigene Applikationen, seine eigene Struktur und damit notwendigerweise auch jeweils spezifische Qualifikationen der jeweiligen User und des Wartungspersonals.

Schüler sind in der heutigen Zeit oft die fundierter vorgebildeten PC-User als es Lehrerinnen und Lehrer sind. Sie wurden in eine computerisierte Welt geboren. Die Handhabung technischer Kommunikationsmittel, einschließlich Handys mit WAP, SMS und MMS, PCs mit Internet-Zugang, Vernetzungen innerhalb des Freundeskreises zum „Zocken“ (=online-Spielen) sind die Norm, nicht die Ausnahme.

Demgegenüber steht eine Lehrerschaft, die sich diese Inhalte erst mühsam erarbeiten muss. Ohne das persönliche technische Interesse an derartigen Weiterentwicklungen in den Kommunikationsmöglichkeiten scheint eher das Verhafteten Einzelner in der überholten Welt der Briefpost und des Telefons. Damit entfernen sich Lehrer und Schüler voneinander immer mehr, statt sich in einem ihrer wesentlichen gemeinsamen Lebensbereiche aufeinander zu bewegen und gerade dies als Chance für Gemeinsamkeiten zu nutzen.

---

<sup>55</sup> RONALD, unter [www.goethe.de/oe/mos/](http://www.goethe.de/oe/mos/) :

*Nun kommt das Internet und die Frage, welche Rolle es als Unterrichtsmedium einnehmen kann. Seine Stärke liegt sowohl im Bereich behavioristischen Trainings und Einschleifens als auch im Bereich der Wissensbildung im Sinne des Kognitivismus. Beide Richtungen, Lernen als Training und Lernen als Entdecken sind im Internet angelegt. Und es ist in ihm noch mehr angelegt: Die mediale Vernetzung von Lehrmaterialien, Unterrichtsgeschehen, Lernerautonomie und Sprachhandeln erfüllen die Forderungen einer kommunikativ-interkulturellen Didaktik so umfassend wie es bisher nicht möglich war. Das Internet erzeugt darüber hinaus einen didaktischen Mehrwert, wie ich ihn weiter unten in der didaktischen Grundlegung ausführen werde.*

Dazu ist es erforderlich, den Lehrern und Lehrerinnen die Möglichkeit einzuräumen, auch innerhalb des schulischen Alltags gemeinsam mit den Schülern und Schülerinnen experimentieren zu können.

Das heißt aber auch, dass zum zielgerichteten Einsatz der Technik in all diesen Bereichen auch in der Lehrerschaft ein Umdenkungsprozess erforderlich ist: das Rollenverständnis muss sich ändern, die persönliche Offenheit für technische Innovation ist wesentliche Grundvoraussetzung für einen vernünftigen Umgang mit dem Medium und damit für den Weg auf die Schüler und Schülerinnen zu.<sup>56</sup>

Ob und in wie weit die technischen, finanziellen, organisatorischen, inhaltlichen und begleitenden (wie motivierenden, fortbildenden pp.) Voraussetzungen nach den politischen Willensbekundungen der jüngsten Vergangenheit bereits geschaffen werden konnten, ist bislang unklar.<sup>57</sup> Zwar meldet seit einiger Zeit das Bundesministerium „Jede Schule ist am Netz“<sup>58</sup>. Aber was heißt das in der Praxis? Wird das Netz auch genutzt, und wenn ja, wofür wird es genutzt? Sind die Netzanschlüsse nicht nur vorhanden, sondern auch real verfügbar? Zwar wird, wie ein Blick in das Internet und das Surfen über Schule-Sites zeigen, von einigen Schulen und Initiativen in

---

<sup>56</sup> GRÄTZ, unter [www.goethe.de](http://www.goethe.de):

*Generell wird sich das Verhältnis zwischen Lehrer und Schüler ändern in die Richtung, daß der Lehrer nicht mehr Wissensvermittler, sondern Lernberater ist. In-ternet-Berater wird er nicht werden. Die Schüler sind meist ein ganzes Stück voraus. Der Lehrer soll auch kein Internet-Kenner werden, aber seine Rolle verändert sich. Lernprozesse werden zunehmend zwischen Lehrer und Schüler ausgehandelt werden.*

sowie STRUCK (1996), BILDUNGSKOMMISSION NRW, STRUCK, P.: Netzwerk Schule – Wie Kinder mit dem Computer das Lernen lernen; München 1998; DÖNHOFF, H.-U.: Eine neue Lernwelt – Das Netz als Medium für die Unterrichtspraxis. Reihe „Arbeitshefte Lehrerbildung“. Gütersloh 1999; GARBE, D.: Schulen ans Netz – warum? Die Schule auf dem Weg in das Informationszeitalter. In: RUTZ, M. (Hr.): Die Byte-Gesellschaft – Informationstechnologie verändert unser Leben. München 1999, S. 55 - 67

<sup>57</sup> S. hierzu VDI Nachrichten v. 01. August 2003, S. 19: Der „Depp vom Dienst“ soll's weiterhin regeln

<sup>58</sup> Am 11. Januar 2001 verkündet Wolfgang Clement, Ministerpräsident NRW, im Rahmen einer Presseerklärung, es sei „...in einer gemeinsamen Kraftanstrengung“ mit der Deutschen Telekom, dem Land, den Kommunen und der e-initiative.nrw gelungen, „für alle Schulen Internetanschlüsse zu realisieren“.

ihren Internetpräsentationen der Eindruck erweckt, dass bereits alles für eine funktionierende umfassende Nutzung der IuK-Technologie nach aktuellen Konzepten getan sei. Es entsteht allerdings der Verdacht, dass es sich dabei um gerade diejenigen Schulen und Initiativen handelt, die bereits über fundierte Kenntnisse und funktionierende Strukturen verfügen, die daher ihre Präsentationen auch entsprechend gestalten können. Die große „schweigende Mehrheit“ der anderen scheint jedoch eben nicht auf dem aktuellen Stand zu sein, modernste Technik auch nutzen zu können. So auch Ausführungen der vortragenden Experten und Diskussionsbeiträge auf der Tagung „Scientific Literacy“ im Dezember 2001, die vom Lehrgebiet Technologie der Bergischen Universität organisiert und von der Landesinitiative „e-initiative.nrw“ unterstützt wurde.

Wie weit die aktuelle Verbreitung innerhalb eines ausgewählten Raumes tatsächlich gediehen ist, soll daher durch eine Befragung der Schulen festgestellt werden.

Der Fragebogen soll außerdem eventuell bestehende Diskrepanzen zwischen den Erfordernissen und offiziellen Meldungen einerseits und den Gegebenheiten andererseits aufdecken und die in der EU-Studie erhobenen Daten (s. Kap. 1.2) dahingehend betrachten, ob sie teils auch auf nordrhein-westfälische Konstellationen zu übertragen sind.

## 4 Datenerhebung in Schulen durch Befragung zum Bereich Vernetzung

### 4.1 Methodenwahl

Die Bedeutung von IuK-Technik für und in Schulen ist, wie bereits Kap. 1.2 und 2.3 gezeigt haben, weitreichend und grundlegend. Entscheidungen, die heute getroffen werden, werden spürbare Auswirkungen zeigen in den zukünftig benötigten Ressourcen jedweder Art, in den zukünftig ermöglichten oder verhinderten Unterrichtsmethoden und –inhalten usw. Damit ist es unumgänglich, umfassendes Datenmaterial zu erhalten, das derartig zukunftsweisende Entscheidungen fundiert ermöglicht. Solche sowohl quantitativ als auch qualitativ zuverlässigen Basisdaten lassen sich nur mittels statistischer Erhebung erhalten.<sup>59</sup>

In der Vorbereitung der Datenerhebung werden zunächst die Zielrichtung der Datensammlung definiert<sup>60</sup> und die Modellbildung vorbereitet<sup>61</sup>, im Anschluss daran werden Entscheidungen zur Art der einzuholenden Informationen getroffen. Es wird der Schwerpunkt auf zahlenmäßige Informationen der Datenerhebung gelegt, lediglich in Freitextzeilen zu ergänzen durch verbale Informationen. So soll versucht werden zu vermeiden, dass durch die Befragten die Begrifflichkeiten unterschiedliche Interpretations-

---

<sup>59</sup> vgl. hierzu BUTTLER, G., STROH, R.: Einführung in die Statistik; Reinbek 2000, S. 17 ff

<sup>60</sup> Das Datenmaterial soll eine Darstellung erbringen, wie weit Schulen mit Technik, Support und Know How ausgestattet sind, wobei es sich hier nur um eine Momentaufnahme handeln kann.

<sup>61</sup> Unter Modellbildung wird die Beschränkung auf das Wesentliche verstanden, vgl. BUTTLER (2000), S. 21

richtungen erhalten, wodurch eine Auswertung der erhaltenden Antworten nicht mehr eindeutig möglich wäre (s. hierzu 4.2.3, 4.2.6 und 4.2.7).<sup>62</sup>

Weiterhin wird die Gesamtheit definiert als „Schulen aller Schultypen bezogen auf einen örtlich begrenzten Raum“ (s. hierzu Kap. 5). Damit ist die Masse der Befragung sowohl sachlich als auch räumlich abgegrenzt. Eine Übertragung der Befragungsergebnisse auf allgemeingültige Aussagen außerhalb des begrenzten Raumes wird daher zunächst nicht beabsichtigt; sie erfolgt – bestenfalls – in einigen ausgewählten Bereichen unter Abgleich mit anderen Untersuchungen (z.B. EU-Studie o.ä.). Ebenso wird darauf verzichtet, Korrelationen darstellen oder bivariate Analyseteile einfügen zu wollen<sup>63</sup>; dazu reichen weder Kapazität der Frageninhalte noch die Anzahl der Befragten aus.

Voraussetzung für die Datenerhebung ist also, einen Fragebogen zu entwickeln, der diesen Grundanforderungen gerecht wird und in der Gestaltungsform weiteren Anforderungen genügt:

---

<sup>62</sup> Zur näheren Darstellung des Bedeutungsspielraumes als Problem s. BUTTLER (2000), S. 20

<sup>63</sup> Zur näheren Betrachtung vgl. BENNINGHAUS, H.: Einführung in die sozialwissenschaftliche Datenanalyse; München 1991, S. 66 ff

## **4.2 Gestaltung des Fragebogens**

Es soll versucht werden, sowohl den Grad der Vernetzung von Schulen als auch Hintergrundinformationen zum Thema zu erfahren. Damit ist die Zweckbindung der Erhebung deutlich, wobei durch einige Freitextfelder dem Bearbeiter auch die Möglichkeit gegeben werden soll, eigene Prioritäten oder persönliche, zielorientierte Erfahrungen zu formulieren. Es sind die folgenden Kriterien als wesentliche Grundüberlegungen in die Entwicklung des Fragebogens eingeflossen:

### **4.2.1 Belastung des Bearbeiters**

Als Bearbeiter werden Mitglieder der Lehrerkollegien bzw. der Schulleitungen der angeschriebenen Schulen gesehen; bei ihnen ist davon auszugehen, dass sie auf Grund ihres Studiums die Zielrichtungen der Fragen erfassen, andererseits aber nicht unbedingt über fundierte Kenntnisse in speziellen Fragen des LuK-Bereiches verfügen müssen.

Der Zeitaufwand für die Beantwortung der Fragen sollte, selbst bei maximaler Bearbeitung und dezidierten Freitexten 30 Minuten nicht überschreiten. Damit sollte erreicht werden, dass die Fülle von Fragen und der zu erwartende Aufwand nicht von vornherein den Adressaten abschrecken und somit negative Auswirkungen für die Anzahl der Rückläufe mit sich bringen.

### **4.2.2 Ausgewogenheit zwischen Geschlossenheit und Offenheit**

Durch die Gestaltung der Fragen sollte es einerseits möglich sein, weitreichende Hinweise über die Kernbereiche des Themas zu erhalten, andererseits die Möglichkeit zu eigenen Kommentaren bzw. Anregungen und Wünschen zu eröffnen. Darüber hinaus sollte es auch möglich sein,

den Fragebogen nur teilweise zu bearbeiten, ohne einen spürbaren Verlust an Auswertungsmöglichkeiten zu erhalten.

#### **4.2.3 Anonymität**

Trotz der Möglichkeit, Kommentare anzufügen, muss die Zusicherung und Einhaltung der Anonymität, sofern gewünscht, gewährleistet sein. Daher werden in den Fragebögen keine sensiblen Daten, insbesondere keine Personaldaten und solche, die Rückschlüsse auf bestimmte Personen zulassen würden, aufgenommen.

Nur dort, wo eine Kontaktaufnahme erwünscht ist, werden die Daten des Bearbeiters erfasst, jedoch nicht veröffentlicht.

Darüber hinaus sollte im Anschreiben und / oder auf dem Fragebogen ausdrücklich darauf hingewiesen werden, dass bei der Auswertung der Daten und im Umgang mit dem Material die Anonymität gewahrt bleibt. Daher wurde auch der Hinweis auf den wissenschaftlichen Zweck der Befragung und den Hintergrund in das Anschreiben aufgenommen.

#### **4.2.4 Grundsatz der Gegenseitigkeit**

Die Bearbeitung des Fragebogens erfordert Zeit und Mühe eines Mitarbeiters der angeschriebenen Schulen. Das Interesse der Schulen an den Befragungsergebnissen kann vielschichtig sein: Darstellung der eigenen Leistungsfähigkeit und eventueller „Vorreiterpositionen“, Nutzung einer der selteneren Gelegenheiten, die Meinung zu einem durch Ministerien auferlegten Programm äußern zu können o.ä., kann aber – und das wohl in der Mehrheit der Fälle - durch Betrachtung der Relation von Aufwand und Nutzen gegen Null tendieren. Allein der Hinweis im Anschreiben, mit der Beantwortung der Fragen ein Dissertationsvorhaben zu unterstützen, kann

nicht Anreiz genug sein. Daher werden Kontaktaufnahme und Beratung angeboten, um den möglichen Nutzen der Teilnahme zu verstärken.

#### **4.2.5 Objektivierbarkeit**

Die Fragen sollten so eindeutig sein, dass durch Standardisierung der Antwortmöglichkeiten (Ankreuzen) oder konkrete Zielgerichtetheit bei Freitexten eine jederzeitige Wiederholung der Befragung mit gleichen Ergebnissen möglich wäre.

#### **4.2.6 Reliabilität**

Die Formulierungen in den Fragen sollten zuverlässig zum eigentlich zu erhebenden Bereich führen und bei fachkundigen Bearbeitern durch Nutzung der erforderlichen *termini technici* eindeutige Antworten ermöglichen.<sup>64</sup>

#### **4.2.7 Auswertungsaufwand**

Zu Beginn der Fragebogenentwicklung war nicht festgelegt, welche Instrumentarien für eine sich anschließende Datenerfassung und Analyse zur Verfügung stehen würden. Der zu antizipierende Aufbereitungsaufwand sollte daher durch Anzahl und Gestaltung der Fragen sowie durch die Auswahl von Merkmalen mit nur wenigen Ausprägungen<sup>65</sup> in einem annehmbaren Rahmen gehalten werden, wobei auf Standardauswerteprodukte,

---

<sup>64</sup> Dass die Annahme der Eindeutigkeit nicht durchgehend Gültigkeit haben kann, ist bereits bei der Auswahl der Befragtengruppe deutlich, da nicht immer von einem einheitlichen Verständnis dieser Begrifflichkeiten ausgegangen werden kann. In so fern finden diese Grundsätze bereits ihre Grenzen dort, wo andere Grundsätze eingehalten werden sollen und damit ein Spannungsfeld entsteht.

<sup>65</sup> S. hierzu BUTTLER (2000), S. 54 ff;

Standardtabellenanwendungen oder auch auf die eventuelle Auswertung der Ergebnisse ohne weitere Hilfsmittel hingearbeitet werden sollte.

Unter Beachtung dieser Prämissen entstanden das nachfolgende Anschreiben sowie der Fragebogen:

### 4.3 Anschreiben und Fragebogen

## BERGISCHE UNIVERSITÄT GESAMTHOCHSCHULE WUPPERTAL

GAUSS-STRASSE 20  
42097 WUPPERTAL

(KORRESPONDENZANSCHRIFT)

TELEFON (0202) 439-1  
TELEFAX (0202) 439-2901

BERGISCHE UNIVERSITÄT - GESAMTHOCHSCHULE WUPPERTAL  
GAU&STR. 20, 42097 WUPPERTAL, FB 3 - TECHNOLOGIE



**Fachbereich 3**

Fach: Technologie und Didaktik der Technik

PRIV.-DOZ. DR. GREGOR TYRCHAN

DATUM

GESPRÄCHSPARTNERIN G. TYRCHAN

AKTENZEICHEN

DURCHWAHL (02 02) 439-2014

GEBÄUDE S

EBENE 11

RAUM 22

TELEFAX (02 02) 439-2014

EMAIL [tyrchan@uni-wuppertal.de](mailto:tyrchan@uni-wuppertal.de)

### Vernetzung an Schulen

Sehr geehrte Damen und Herren,

im Rahmen einer Dissertation, die ich in meinem Fachbereich betreue, sollen (technische, didaktische) Möglichkeiten, Chancen und Risiken zum Bereich „Vernetzung in / von Schulen“ diskutiert, aber auch Vorschläge zur Gestaltung erörtert werden.

Dazu sind zunächst gesicherte Erkenntnisse schon bestehender Netzwerke (Art, Anzahl, Umfang, Strukturen) erforderlich. Um diesen Überblick zu erhalten, bitte ich Sie um Ihre Unterstützung. Als Anlage ist ein Fragebogen beigefügt (max. Zeitaufwand 30 Minuten). Ich bitte Sie, diesen Fragebogen zu bearbeiten und mit Schulstempel bis 31.05.2001 an uns per Brief oder Fax zurück zu senden.

Für die Beantwortung informationstechnischer Anliegen bei einigen Fragen wird der Beauftragte für I&K-Technologien Ihrer Schule Ihnen sicher behilflich sein können.

Ich versichere Ihnen, dass die von Ihnen gemachten Angaben nach eventuell erforderlicher Anonymisierung lediglich in eine statistische Auswertung für die wissenschaftliche Arbeit einbezogen werden, sofern Sie nicht ausdrücklich mit einer eventuellen Kontaktaufnahme (Frage 12 c) einverstanden sind.

Für Ihre Mithilfe bedanke ich mich im Voraus.

(G. Tyrchan)

Anlage: Fragebogen

Bergische Universität  
 Gesamthochschule Wuppertal  
 FB 3 – Technologie und Didaktik der Technik  
 - Priv.-Doz. Dr. G. Tyrchan -  
 Gaußstr. 20  
**D 42097 Wuppertal**

Absender (Schulstempel):

1. Arbeiten an Ihrer Schule die vorhandenen PCs in einem Netzwerk?  
 Falls „Nein“, weiter mit Frage 12 Ja    Nein
  
2. Haben Sie Teilnetze eingerichtet?  
 (Für einzelne Gebäude/ Fachbereiche/ ...) Ja    Nein
  
3. Mit welchem Betriebssystem arbeiten Sie im Netz? \_\_\_\_\_
  
4. Gibt es ein extra Mailing-System / eine Mailing-Software?  
 (zusätzlich zum vorhandenen Browser) \_\_\_\_\_
  
5. Ist Ihre Schule mit anderen Schulen vernetzt?  
 (in einem speziellen u.U. städtischen Netzwerk) Ja    Nein
  
6. Welche Strukturen/ Merkmale haben das
  - a. Berechtigungskonzept für unterschiedliche Zugriffsarten? \_\_\_\_\_
  - b. Berechtigungskonzept für verschiedene Personen? \_\_\_\_\_
  - c. Datensicherheitskonzept? \_\_\_\_\_
  - d. Datenschutzkonzept? \_\_\_\_\_
  
7. Von wem wird das Netz hauptsächlich genutzt? Von \_\_\_\_\_
 

	Lehrern	ÿ
	Schülern	ÿ
	Schulleitung	ÿ
	Sekretariat	ÿ
	_____	€
  
8. Zu welchen Zwecken wird das Netz bzw. werden die Teilnetze genutzt?  
 (auch Mehrfachnennungen)
 

	Für	
	Unterrichtsvorbereitung	ÿ
	Unterricht	ÿ
	Unterrichtsnachbereitung	€
	Verwaltungsaufgaben	ÿ
	Projektarbeit	ÿ
	Stundenplan/ Vertretungen	€
	Hausaufgaben, Referate, ...	€
	_____	€

9. Sind Sie mit Ihrer Schule auch im Internet vertreten („Home-Page“, Web-Site)?

Ja Nein

10. Haben Sie Unterstützung zur Pflege des Netzes? (Förderverein, Schulträger, Firma, ...)

Ja Nein

11. Haben Sie in Ihrer Schule einen verantwortlichen Netzwerk-Administrator? Welche Ausbildung, welches Training hat er als Administrator?

Ja Nein

---

---

---

11. Falls Sie noch kein Netz eingerichtet haben:

a. Ist eine Vernetzung der Schule in Planung?

Ja Nein

b. Sind Sie an einer Vernetzung interessiert?

Ja Nein

c. Welche Gründe sprechen gegen ein Computer-Netz?

---

---

---

---

e. Sind Sie an einer Kontaktaufnahme bzw. Beratung interessiert?

Ja Nein

Raum für zusätzliche Hinweise, Anmerkungen oder Wünsche:

---

---

---

---

#### **4.4 Inhaltliche Gestaltung, Ziele der Befragung, Begründung für die Fragestellungen**

**Frage 1** dient einerseits als „Türöffner“ und zur Klarstellung des näheren Themenfeldes (das Thema selbst wird bereits im Anschreiben grob dargelegt), andererseits zur Feststellung des im Kreis der befragten Schulen erreichten Grades der Vernetzung. Der Verweis auf Frage 12 bei Fehlen eines Netzwerkes bewirkt die Auslassung der Fragen 2 bis 11. Die Möglichkeit zur Beantwortung von Frage 12 wird durch ein eventuelles „Ja“ bei Frage 1 nicht vollends ausgeschlossen.

Die Beantwortung mit „Ja“ führt zu den folgenden Fragen, die die Ausgestaltung des Netzwerkes näher darlegen sollen.

**Frage 2** bezieht sich auf die Gestaltung der innerschulischen Vernetzung bzw. des schulischen Intranets und auf die Frage, ob ein LAN der Schule in mehrere Bereiche untergliedert ist. Die Beantwortung der Frage ermöglicht in Analyse und Auswertung auch die Erkenntnis, ob der Bearbeiter des Fragebogens das Thema ausreichend durchdrungen hat und die Begriffe in ihrer Bedeutung erkennt. Sie soll außerdem die konzeptionelle Gestaltung von Teilnetzen (räumliche Gliederung, organisatorische Gliederung o.ä.) erkennen lassen.

**Frage 3** dient sowohl der statistischen Feststellung der Verbreitung unterschiedlicher Betriebssysteme (die Microsoft-Welt ist trotz aller Bemühungen der Konkurrenzfirmen - wie z.B. kostenlose Abgabe, „abgespeckte“ freeware-Varianten u.ä. - in einzelnen Bereichen hartnäckig die am weitesten verbreitete) als auch der Erörterung der Frage, ob und wie weit eine Kopplung unterschiedlicher schon bestehender Netzwerke zu einem umspannenden „Schulnetz“ unterschiedlicher Ausdehnungen und Ausprägungen sinnvoll und möglich wäre.

**Frage 4** steht mit der vorhergehenden in engem Zusammenhang, bestimmte Betriebssysteme legen die Nutzung dazugehöriger Mailing-Systeme bzw. Mailing-Software nahe. Macintosh-Netze werden sich kaum eines MS-Exchange-Servers bedienen. Da, wo durch Kopplung unterschiedlicher Netze, etwa durch Nutzung mehrerer Netzwerkkarten o.ä., die Vermischung gelungen ist, besteht eine Erfahrung, auf die zurückgegriffen werden könnte bei Zusammenlegung unterschiedlicher Netzwerke.<sup>66</sup>

**Frage 5** soll zeigen, ob der Weg zu einem möglichst umfassenden schulischen Netz bereits beschritten wird, oder ob die Initiative „Schulen ans Netz“ sich nach wie vor lediglich durch die Bereitstellung bzw. Vermittlung eines ISDN – Anschlusses und eines Multimedia-PC's zum Anschluss an das Internet erschöpft, womit Chancen zu Informations- und Wissensmanagement ineffektiv angegangen würden. 1996 wurde in NRW durch das Ministerium für Wirtschaft, Mittelstand, Technologie und Verkehr und das Ministerium für Schule und Weiterbildung in Aussicht gestellt, dass bis zum Jahr 1999 „... alle nordrhein-westfälischen Schulen der Sekundarstufen I und II mit einem Multimedia-Computer ausgestattet werden. Diese Gerät verfügt über einen ISDN-Anschluss zur Netzwerk-Kommunikation...“ In wie weit der damals für 1999 avisierte Stand der Ausstattung heute überschritten wurde oder noch Stand der Dinge ist, soll festgestellt werden.<sup>67</sup>

**Frage 6** soll Klarheit darüber erbringen, ob tatsächlich in den meisten Schulen die Netzwerkadministration als zusätzliche Aufgabe von Lehrerinnen und Lehrern übernommen werden muss, wie Aussagen in der Literatur vermuten lassen.<sup>68</sup>

---

<sup>66</sup> Zur näheren Erläuterung der technischen Strukturen sowie zur Begriffserklärung s. Kap. 2.2

<sup>67</sup> Broschüre NRW-Schulen ans Netz, Stand 1996

<sup>68</sup> so die Aussagen in Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000, Teil 2-2

**Frage 7** ist als offene Fragestellung angelegt. Es wird davon ausgegangen, dass bei Vorhandensein eines Netzwerkes in der Schule bereits Konzepte zu den einzelnen Bereichen bestehen und bestimmte Strukturen erarbeitet sind. Diese sollen hier kurz angesprochen werden. Die Frage soll außerdem zeigen, ob die durch das Bundesamt für Sicherheit in der Informationstechnik geforderten Mindestvoraussetzungen beachtet und spezielle Gefährdungen eines schulischen Intranets bekannt sind. Diese Frage korrespondiert eng mit der darauf folgenden

**Frage 8**, da durch den Personenkreis der User Gefahrenpotentiale gesetzt oder ausgeschlossen werden können. Frage 7 wiederum steht in unmittelbarem Zusammenhang mit

**Frage 9**, da die Nutzung durch bestimmte Personenkreise zwangsläufig auch die Nutzung für bestimmte Bereiche impliziert (z.B. Sekretariat – Verwaltungsaufgaben mit Speicherung und Bearbeitung sensibler personenbezogener Daten). Diese Nutzungsbereiche wiederum wirken zurück und haben Bedeutung für die Anforderung von Sicherheitskonzepten nach Frage 7, sind also auch dort zu berücksichtigen.

**Frage 10** weist den Anteil der Schulen aus, die nach der Initiative „Schulen ans Netz“ bereits Web-Sites erstellt haben und die Gelegenheit der eigenen online-Präsentation nutzen. Sie macht außerdem deutlich, ob das Verständnis für die unterschiedliche Bedeutung von Internet-Präsentation und Intranet der Schule gegeben ist.

**Frage 11** zielt sowohl auf fachliche als auch auf finanzielle oder technische Unterstützung ab. Sie soll klären, ob innerschulisch oder außerschulisch Hilfe angeboten und in Anspruch genommen wird.<sup>69</sup>

Da jedoch vermutet wird, dass die Netzwerkadministration zusätzliche von Lehrerinnen und Lehrern geleistet wird (s. Frage 6), ist anzunehmen, dass hier der Schwerpunkt auf der Komponente „Ausbildung / Training“ liegen wird, die als wesentliche Voraussetzung durch Schulträger, Ministerium pp. geschaffen werden muss.

**Frage 12** schließt den Kreis und führt zurück zur Ausgangsfrage; sie ermöglicht denjenigen Schulen, die noch nicht in der Einrichtung eines Netzes stecken, die Darstellung ihrer jeweiligen Pläne, Gegenargumente usw. Sie ermöglicht allen anderen, die Nachteile des von ihnen schon eingerichteten Netzes darzulegen und Pläne, eventuell für eine weitere Vorgehensweise (Funknetz, Teilnetze o.ä.) zu nennen. Und sie gibt nicht zuletzt die Möglichkeit, einen eigenen Nutzen aus der Beantwortung des Fragebogens zu ziehen, sofern dies gewünscht wird.

Nach Abschluss von Datenerfassung und -analyse wird der in der Arbeit konkret, spezifisch zu bearbeitende Themenbereich aus dem Gesamtkomplex ausgewählt. Dabei sollen gerade diejenigen Felder, die bereits hinreichend Klarheit in der Umsetzung erfahren haben oder eher nachgeordnete Problemstellungen aufweisen durch die Analyse erkannt, ausgeklammert bzw. an anderer Stelle erörtert werden.

---

<sup>69</sup> Hintergrund sind

- die Tatsache, dass durch die Bezirksregierungen technische Ausstattung, die aus unterschiedlichen Gründen von Institutionen der Landesverwaltung abgegeben wird, gesammelt und nach Bedarfsmeldung verteilt wird,
- Hinweise auf Sponsoring durch Banken und Sparkassen und Unternehmen in den Medien im Rahmen des Projektes „Schulen ans Netz“.

## 5 Durchführung der Befragung

Der Fragebogen wurde einschließlich Anschreiben an insgesamt

215 Schulen

gerichtet. Darunter waren die privaten und öffentlichen weiterführenden Schulen (außer Kollegschaften Düsseldorf und Wuppertal) in den

Postleitzahlenbezirken 40xxx, 41xxx und 42xxx.

Damit sind Sekundarschulen aus Düsseldorf, Meerbusch, Erkrath, Hilden, Langenfeld, Monheim, Mettmann, Ratingen, Mönchengladbach, Nettetal, Korschenbroich, Schwalmatal, Niederkrüchten, Wuppertal, Radevormwald, Wülfrath, Hückeswagen, Velbert, Heiligenhaus, Solingen erfasst.

Die in diesen Städten ansässigen Sekundarschulen repräsentieren die nach den Internetdarstellungen der betreffenden Gemeinden ermittelten, in der nachfolgenden Tabelle (Tabelle 1) dargestellten Bevölkerungszahlen und Flächenausdehnungen. Allerdings ist davon auszugehen, dass zumindest teilweise der Einzugsbereich der Schulen über die kommunalen Flächen und Einwohnergrenzen hinaus geht und auch solche Schüler diese Schulen besuchen, die nicht zur Kommune gehören und aus angrenzenden Städten und Gemeinden kommen.<sup>70</sup>

---

<sup>70</sup> Beispiel: Schwelmer Schüler besuchen Wuppertaler Gymnasien wegen der dort teils gebotenen besonderen Konzepte und Zielrichtungen, sind jedoch in der Tabelle nicht erfasst, da Schwelm nicht zu den befragten Kommunen zählt.

	Einwohner	km <sup>2</sup>
Düsseldorf	569.364	217,00
Meerbusch	55.175	64,39
Erkrath	48.767	26,86
Hilden	56.412	25,96
Langenfeld	58.429	41,06
Monheim	43.514	23,13
Mettmann	38.708	42,52
Ratingen	91.437	88,72
Mönchengladbach	263.014	170,44
Nettetal	41.871	83,86
Korschenbroich	33.782	55,26
Schwalmtal	19.177	48,11
Niederkrüchten	14.190	67,07
Wuppertal	366.434	163,38
Radevormwald	24.800	53,77
Wülfrath	22.531	32,23
Hückeswagen	16.397	50,46
Velbert	89.782	74,91
Heiligenhaus	28.442	27,47
Solingen	164.973	89,45
gesamt	2.047.199	1446,05

Tabelle 1: Bevölkerungs- und Flächendaten derjenigen Kommunen, deren Schulen in die Befragung einbezogen wurden. Entnommen aus den Internet-Präsentationen der Kommunen. Stand Okt. 2001/71

---

<sup>71</sup> Zum Vergleich die Gesamtdaten Stand April 2003, bezogen auf NRW:  
*Fläche 34.081 km<sup>2</sup>*  
*Einwohnerzahl 18 Mio.*  
*Schüler/innenzahl allgemein bildende Schulen: 2.323.118*  
*Anzahl allgemein bildende Schulen: 6405;*  
aus: itworks, [www.schulen-ans-netz.de](http://www.schulen-ans-netz.de), S. 23

Somit sind die Auswahl der Schulen und die Verteilung der Fragebögen nicht selektiv. Es sind gänzlich unterschiedliche Regionen, differenzierte Infrastrukturen, städtische, ländliche, mehr und weniger privilegierte Wohngebiete und Schulen erfasst. Ein breit gefächertes Spektrum möglicher Antworten ist ebenso zu erwarten wie gänzlich unterschiedliche Arten, Formen und Standards der Umsetzung von Schulnetzen. Sowohl die Auswahl der Schulen, damit verbunden die Verteilung der Fragebögen und das Beantwortungsverhalten wurden dem Zufall überlassen, es wurde lediglich nach den oben bereits benannten Auswahlkriterien selektiert und strukturiert. Daher ist die durchgeführte Befragung auch nicht repräsentativ; das Vorhandensein bestimmter Bearbeitungsgruppen zum modellhaften Abbild der Gesamtbevölkerungsstruktur kann und soll durch die Befragung nicht erreicht werden.

Die Befragung fand im Frühjahr 2001 statt, Termin für die Rückgabe ausgefüllter Fragebögen war der 31. Mai 2001. Auf diese Weise sollte die Erfassung der Daten und Auswertung der Ergebnisse bis zu den Sommerferien ermöglicht werden, um eine eventuell erforderliche Kontaktaufnahme mit den Schulen noch für Beginn des Schuljahres 2001 / 2002 vorzusehen. Die Rückgabe der Fragebögen war sowohl per Post als auch per Fax möglich.<sup>72</sup>

Von den	215 Fragebögen
wurden	119 ausgefüllt zurückgeschickt,
was einem Prozentsatz von	55,35 %

entspricht.

---

<sup>72</sup> Im Nachhinein muss ich feststellen, dass der Fragebogen zweckmäßigerweise auch in der Internet-Präsentation des betreuenden Fachbereiches hätte eingestellt werden sollen. Dies wäre konsequent und themenorientiert korrekt gewesen. Ob dadurch eventuell weitere Schulen zur Beantwortung animiert worden wären, bleibt allerdings fraglich. Für die Glaubwürdigkeit einer Arbeit über Netzwerkausnutzung wäre eine derartige Entscheidung allerdings sicherlich zuträglich gewesen.

3 der Fragebögen konnten nicht ausgewertet werden, da sie per Fax nur teilweise übertragen wurden und daher unleserlich waren. In den 119 zurückerhaltenen Fragebögen sind teilweise nicht alle Fragen bearbeitet worden.

Damit ergibt sich ein auswertbarer Anteil von 53,95 %.

Es wurden sowohl in der Rückgabe- als auch in der Auswertungsquote Werte erreicht, die die Erwartungen weit überschritten.

Es entsteht die Vermutung, dass das Thema für die Schulen ebenso wichtig ist wie die damit in Planung und Umsetzung verbundenen Probleme, andererseits wird auch die umspannende zentrale Rolle des Themenkomplexes in der Gesamtgesellschaft deutlich.

## 6 Datenerfassung und Datenauswertung

Bereits in der Entwicklung der Fragebögen wurde darauf hingearbeitet, die Erfassung (und anschließende Auswertung) mit möglichst geringem Aufwand und Standardanwendungen durchführen zu können (s. Kap. 4).<sup>73</sup>

Die Datenerhebung musste allerdings auf Grund ganz unterschiedlichster Ursachen dennoch mit hohem Aufwand ohne elektronische Unterstützung durchgeführt werden; lediglich für die Auswertung und Berechnung der Daten wurde letztendlich auch auf eine vorhandene Standardsoftware (hier: Excel) zurückgegriffen.

Die Auswertungsergebnisse im Einzelnen:<sup>74</sup>

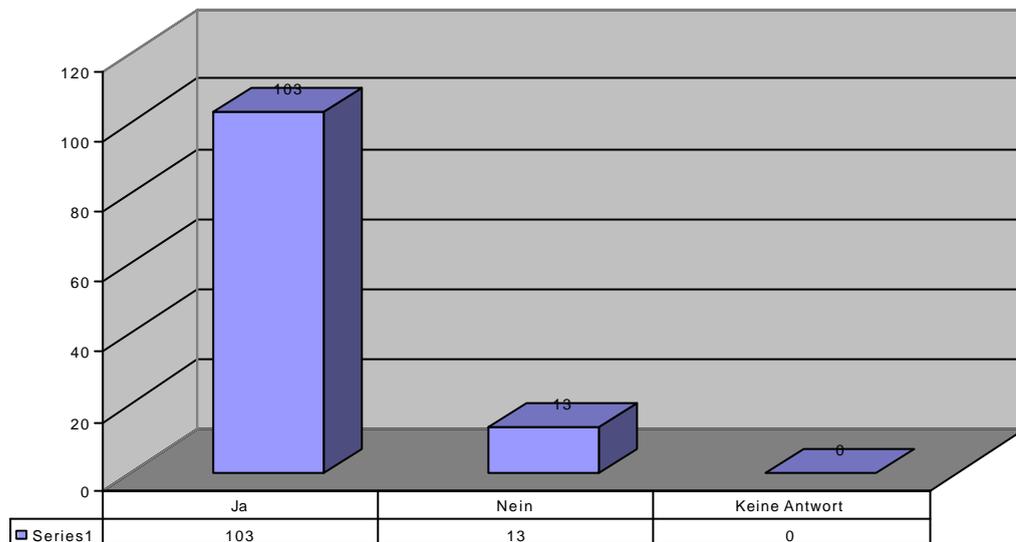
---

<sup>73</sup> In diesem Zusammenhang verweise ich auf die durch einen Fragebogen bekannt gewordene Anwendung, die von Bildungseinrichtungen unter [www.grafstat.de](http://www.grafstat.de) als freeware downgeloadet werden kann. Sie ermöglicht die Erstellung und Auswertung von Fragebögen „aus einem Guss“.

<sup>74</sup> Differenzen in den Gesamtsummen ergeben sich aus der Tatsache, dass nicht in allen Fragebögen alle Fragen bearbeitet worden sind. So kann statt der Gesamtsumme von 119 zurückgehaltenen Fragebögen die Gesamtsumme durchaus darunter oder – bei möglichen Mehrfachantworten darüber – liegen.

## 6.1 Frage 1

Arbeiten an Ihrer Schule die vorhandenen PCs in einem Netzwerk?

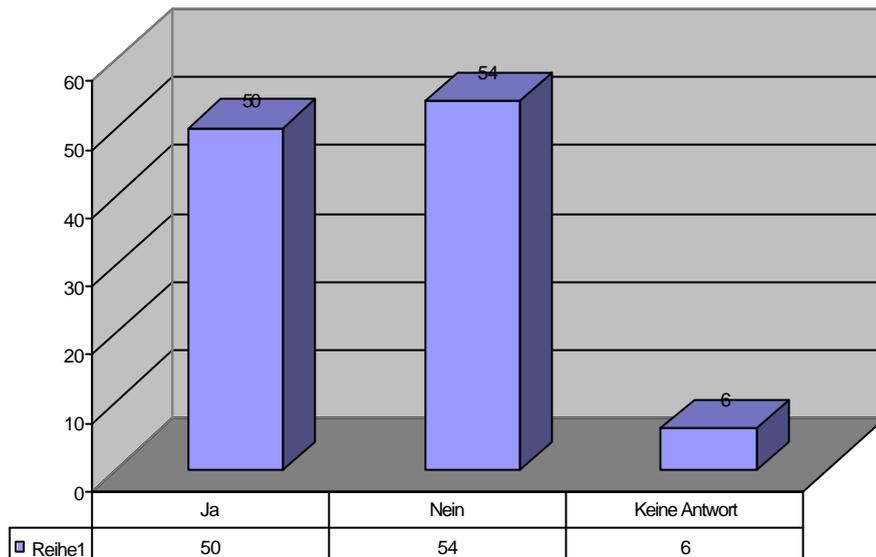


Zusätzliche Anmerkungen:

- „1 Internetinsel (4PCs)“
- „17 PCs im Computerraum“
- „teilweise“
- „nur Informatik“
- „nur ein Teil“

## 6.2 Frage 2

Haben Sie Teilnetze eingerichtet?



Zusätzliche Anmerkungen:

- „Computerraum“
- „Verwaltung / Schülernetz“
- „2 Netze: Schüler / Schulleitung“
- „Es gibt ein Schülernetz im IF-Raum und ein Verwaltungsnetz (Sekretariat / Lehrer usw.)“
- „Teilnetz im Informatikraum“
- „2 Räume jeweils einzeln vernetzt“
- „Verwaltungsbereich eigenes unabhängiges Netz“

### 6.3 Frage 3

Mit welchem Betriebssystem arbeiten Sie im Netz?<sup>75</sup>

Novell	11
Windows NT 4.0	22
Windows 95	18
Windows 98	26
Windows 2K Server	1
Windows 2000	15
Windows NT	15
Unix	1
Linux Proxyserver	1
Windows 98 Workstations	1
Novell 5.1	1
Windows 3.11	3
peer to peer	2
Mac	2
Novell Netware 5.1	2
TCP/IP-Clients unter 2000	1
Linux	15
Linux Server	2
Windows	4
Windows 9x	1
Windows 2K	2
Windows 98SE	1
Mac OS	1
Mac	1
Windows NT 98	1
Windows NT 2000	2
Windows 2000 Server	1
Novell 3.12	1
Linux für Internetzugang	1
Windows 95 c	1
gesamt	156

Tabelle 2: Verteilung der Originalantworten

Zusätzliche Anmerkungen:

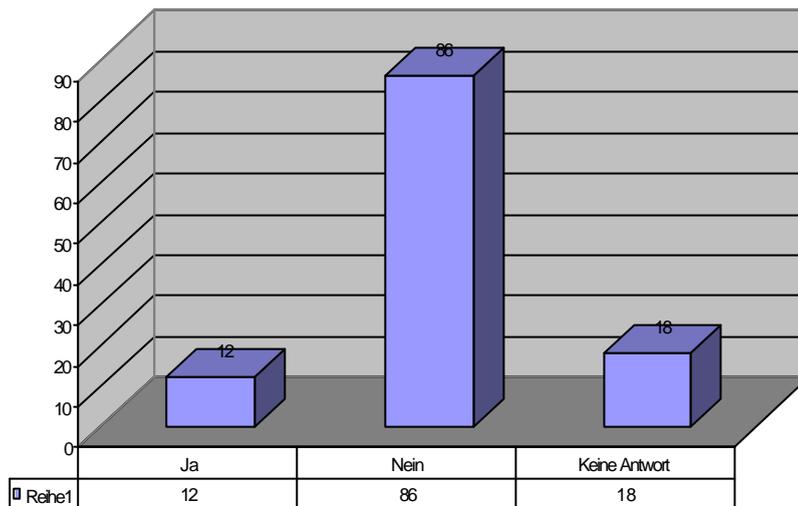
- „Frage ist nicht sinnvoll“
- „Wir kombinieren Win 98 Clients / Linux Server“

---

<sup>75</sup> Die Tabelle listet die zahlenmäßige Verteilung aller gegebenen Original-Antworten auf. Eine Zusammenfassung gleicher Systeme, die in der Beantwortung der Fragen lediglich andere Bezeichnungen erhielten, oder eine auch irgendwie sonst geartete Veränderung der Antworten erfolgt hier zunächst nicht. Ebenso wird an dieser Stelle auf jegliche Interpretation der Daten verzichtet; diese erfolgt in Kap. 7.

## 6.4 Frage 4

Gibt es ein extra Mailing-System / eine Mailing Software?

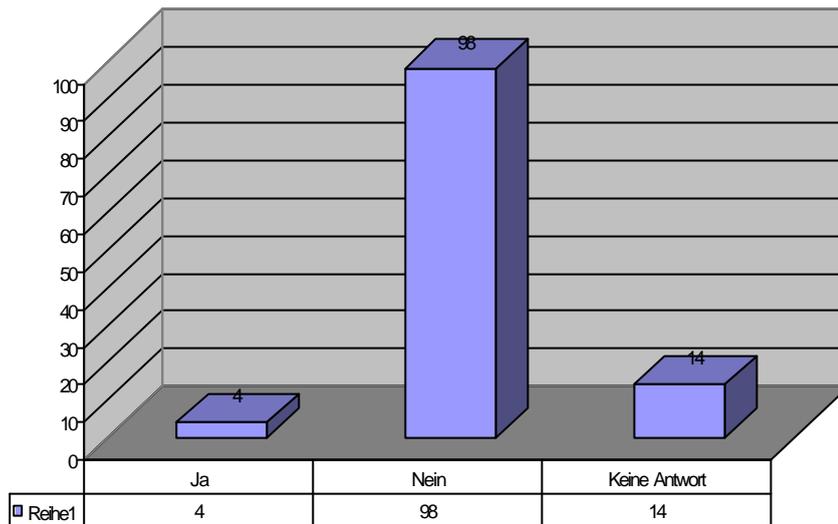


Zusätzliche Anmerkungen:

- „Exchange Server“
- „Sendmail“
- „Outlook“ (3)
- „Exchange“ (2)
- „webbasiert“
- „t-online webmail“
- „e-post.de“
- „mercury mailing systems“
- „pegasos mail clients“
- „netscape communicator“
- „aber nicht betriebsbereit“
- „Outlook Express“ (2)
- „Mac ja – Win nein“
- „t-online“

## 6.5 Frage 5

Ist Ihre Schule mit anderen Schulen vernetzt?



Zusätzliche Anmerkungen:

- „Sekretariat ist mit Stadt und anderen Schulen verbunden“

## 6.6 Frage 6

Welche Strukturen / Merkmale haben das

a. Berechtigungskonzept für unterschiedliche Zugriffsarten?

- Ja: 5 mal
- Keine: 3 mal
- Keine Antwort: 35 mal
- Passwörter: 7 mal
- Hierarchisch: 2 mal
- Win NT-Anmeldung: 3 mal
- Unterschiedliche User haben unterschiedliche Zugriffsarten
- Server-basierte Win-Policy
- Netze sind getrennt
- Einlogscripte, serverbasierte Profile
- Bootmanager NT / Win 95
- Zugriff auf Freigabeebene
- Lesen, ändern, Vollzugriff
- Lokal Vollzugriff, eingeschränkt auf den Server
- Es gibt nur ein Password für den Administrator und eins für das Lehrpersonal
- Passwort für den Server-Rechner, wird vom Lehrer eingegeben
- Klassen-orientiert
- Festlegung der Prog.-Nutzung durch Lehrer
- Noch im Aufbau
- Zugangsberechtigung
- Administrator / Lehrer / Schüler (Sonstige): 4 mal
- Active directory
- Zugangskontrolle / Passwort / Benutzername
- Jeweils Administrator persönliche Kennworte INIS
- Platzbezogen

- Serverabhängige Profile
- Windows 2000
- Schülergruppen / Fortbildungsgruppen / einzelne Lehrkräfte
- Nutzerebene
- Alle Nutzer sind gleichberechtigt

b. Berechtigungskonzept für verschiedene Personen?

- ja: 9 mal
- nein: 1 mal
- keine Antwort: 39 mal
- Passwörter: 3 mal
- Lehrer / Schüler / Admins: 6 mal
- Win NT Anmeldung: 2 mal
- Nur für Admin
- Eingeschränkt – nur Lesen von Dateien
- Log in-Name
- Nur für die Server
- Fehlt – wir sind auf der Suche
- Trennung Schüler / Lehrer- Verzeichnis
- Lehrer-orientiert
- Lehrer / Schüler –Passwort, Benutzername –  
Zugangskontrolle
- Persönliche Konten für alle Benutzer
- Persönlicher Account, Gruppe zugeordnet
- 3 Ebenen
- Lehrer / Schüler
- Serverbasierte Profile: Lehrer, Schüler, Kurse haben unterschiedliche Profile mit verschiedenen Zugriffsrechten
- User, Administratoren, User mit Administratorenrechten
- Serverabhängige Profile
- Individuelle Benutzerkonten

- Anmeldung über Prim.Dom.Contr. mit Anmeldenamen und Passwort für unterschiedliche Berechtigungen
- Freigabe durch Lehrer-PC
- Administrator mit Zugang für alles, Anwender eingeschränkt

c. Datensicherheitskonzept?

- keine Antwort: 41 mal
- backup: 5 mal
- Firewall und Proxyserver: 2 mal
- Wird erarbeitet: 2 mal
- Ja: 4 mal
- Fehlt: 7 mal (wir sind auf der Suche)
- Images / Bandsicherung: 4 mal
- Streamer: 2 mal
- Profile und Protektorkarten
- Schülernetz: novell-gesichert, sonst keine Datensicherheit
- Offenes System
- Images der Clients auf dem Server
- Streamer / Zip / Spiegelplatte
- CD-ROM / Sicherung auf Server
- Abbilder
- Virenschutzprogramm
- Daten auf Server, Wiederherstellung
- Freigabe nach Ordner
- RAID-System
- Spiegelung der Serverplatte
- In Ansätzen (Images sichern)
- Manuell
- Web-washer
- Image-Dateien als Sicherung, pers. Home-Verzeichnis auf Server
- Regelmäßige Sicherung Server

- Backuplösung für die workstations auf Server
- Sehr beschränkter Zugriff durch Schüler
- Separate Festplatte
- Clientkontrolle über Lehrer-Rechner

d. Datenschutzkonzept?

- keine Antwort: 41 mal
- physikalisch getrennte Netze: 3 mal
- wird erarbeitet: 3 mal
- ja: 2 mal
- keines: 5 mal (wir sind auf der Suche)
- Streamer
- Verarbeitung personenbezogener Daten nur in der Verwaltung, diese sind gesondert gesichert
- Homeverzeichnis
- Strikte Trennung zwischen Unterrichtsnetz und Verwaltung
- Virens Scanner und Mini-Firewall zum Internet
- Keine relevanten Daten im Schülernetz
- Mangelhaft; z.B. ständige Eingriffe durch Schüler
- Zugriff von außen nicht gestattet
- Firewall, z.B. Zone alarm, in Planung
- Zugriffe passwortgeschützt
- NAV auf Server
- Kein direktes
- Passwort
- Verschlussene Räume / Schränke – Passwortschutz
- Virenschutz, Datenbackup
- Zugangskontrolle, Anti-Viren-Schutz
- Persönliche Daten (email) bei Provider – kein spezielles Konzept
- Externe Datenträger
- Manuell

- Fileserver mit Kennwortabfrage
- Keine empfindlichen Daten erlaubt – Benutzerordnung
- Persönliche Daten nur im Verwaltungsnetz
- Proxy und Firewall, blacklist
- Keine relevanten Daten
- Noch nicht umgesetzt

a und b:

- wir verwenden ein Schutzprogramm: Win Control 99
- unterschiedliche Lese- Schreibzugriffe für Admin, Lehrer, Schüler
- Registry verändert: kein Zugriff auf Systemsteuerung, Systemdateien, Disketten- und CD-Laufwerke
- Über active-directory

c und d:

- auf Schülerrechnern befinden sich keine Daten, die geschützt werden müssen
- keine, da PC's nur in der Mediothek
- gegenwärtig noch ungelöst

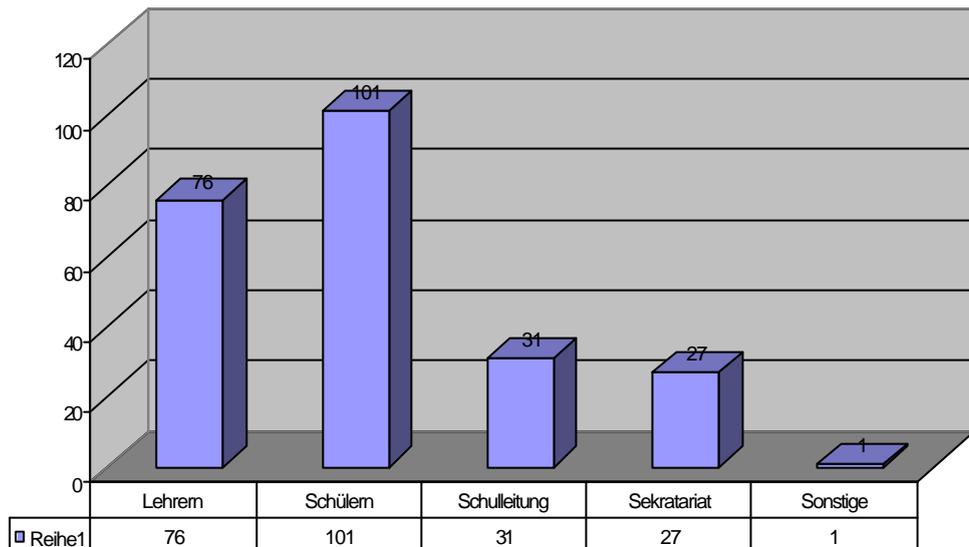
a bis d:

- Fragezeichen: 7
- ohne Strukturen
- Noch im Aufbau
- Netzadministrator vergibt Rechte
- Clients haben nur Zugriff auf Ordner auf dem Linux-Server, die Laufwerke auf den Clients sind gesperrt
- Getrennte Netze: Verwaltungsnetz NT, Unterrichtsnetz NT
- Internet Cafe Linux
- Die Netze sind räumlich getrennt. Die Personen haben unterschiedliche Zugangsberechtigung.

- Datenschutz / Datensicherheit über verschiedene Benutzersysteme (Lehrer / Schüler / Admin)
- Proxy-Server
- Windows-Anmeldung
- Anmeldung in Arbeitsgruppen
- Berechtigungen werden in drei Kategorien unterteilt: Lehrer, Schüler, Administrator
- Siehe Software ANAT: 2
- Hinweis auf INIS: 4
- Die Frage verstehe ich nicht
- Offenes System, da peer-to-peer-Netz; im Netz Dateifreigabe durch Win 95 / 98
- NT 4.0 Policies, Win 3.11 INIS
- Generell nur anonyme Anmeldung für Zugriff auf einen NT-Dateiserver
- Geplant: 2
- Unleserliche Antwort

## 6.7 Frage 7

Von wem wird das Netz hauptsächlich genutzt?

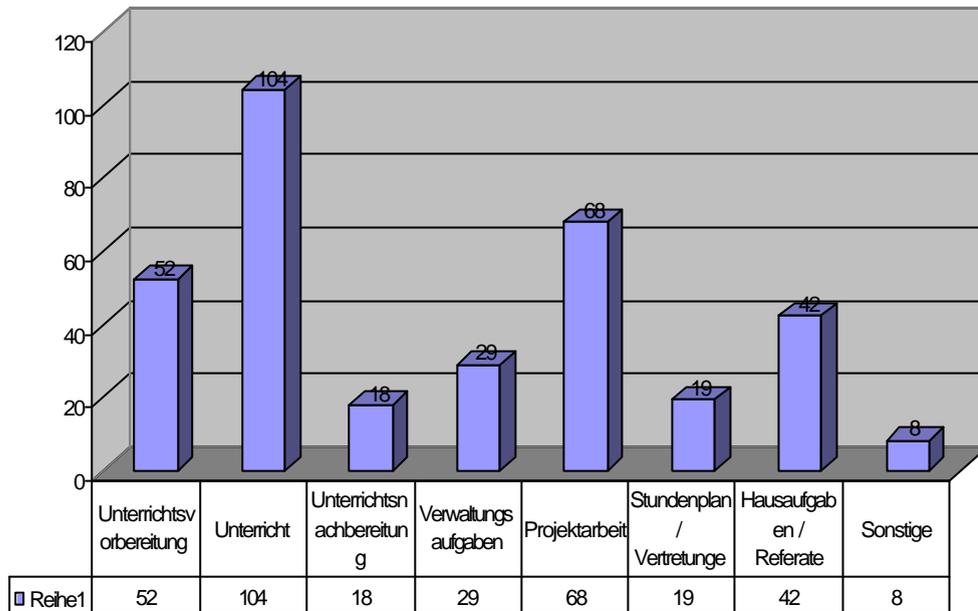


Zusätzliche Anmerkungen:

- „Lehrer zuweilen“
- „eigenes Verwaltungsnetz“
- „internes Verwaltungsnetz“
- „Lehrer bedingt“
- „wir haben nur den ausschließlich für Schüler vorgesehenen [T@school-Zugang](#) der Deutschen Telekom“
- „Schülerfirma step2web“

## 6.8 Frage 8

Zu welchem Zweck wird das Netz bzw. die Teilnetze genutzt?

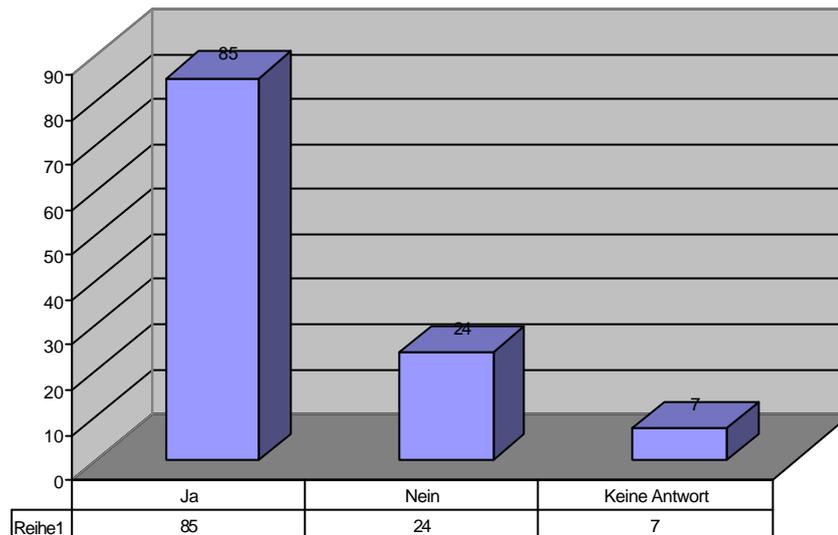


Zusätzliche Anmerkungen:

- „Schulzeitung“
- „Unterrichtsvorbereitung nur bedingt“
- „AG's“
- „Projektarbeit gelegentlich“
- „gar nicht“
- „Internetrecherche“
- „Internet-Schulung“
- „Lehrerfortbildung“
- „Fortbildung“
- „Schulung der Schüler für den Zugang mit Internet“

## 6.9 Frage 9

Sind Sie mit Ihrer Schule auch im Internet vertreten („Home-Page“, „Web-Site“)?

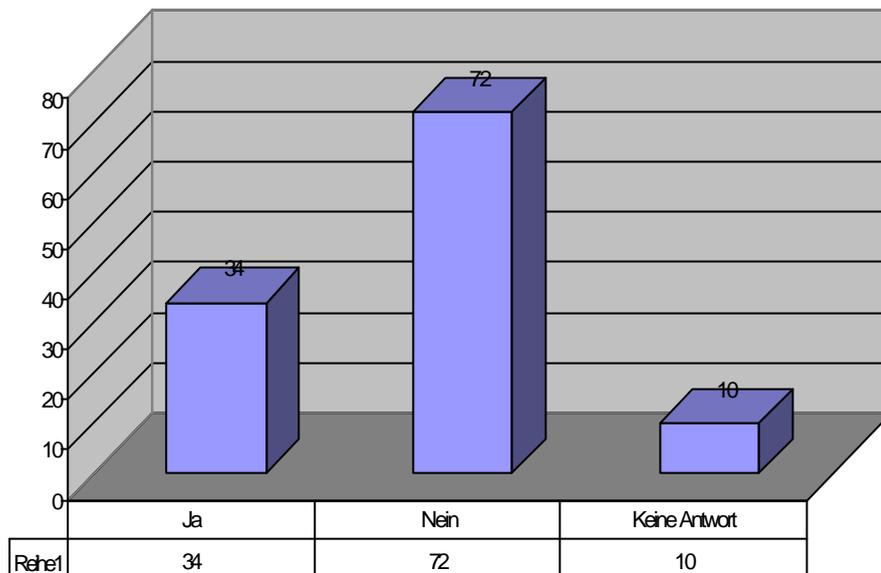


Zusätzliche Anmerkungen:

- „projektiert“ (3)
- „noch nicht“
- „home page“
- „im Aufbau“
- wegen Weggang des Administrators nicht aktualisiert“

## 6.10 Frage 10

Haben Sie Unterstützung zur Pflege des Netzes?

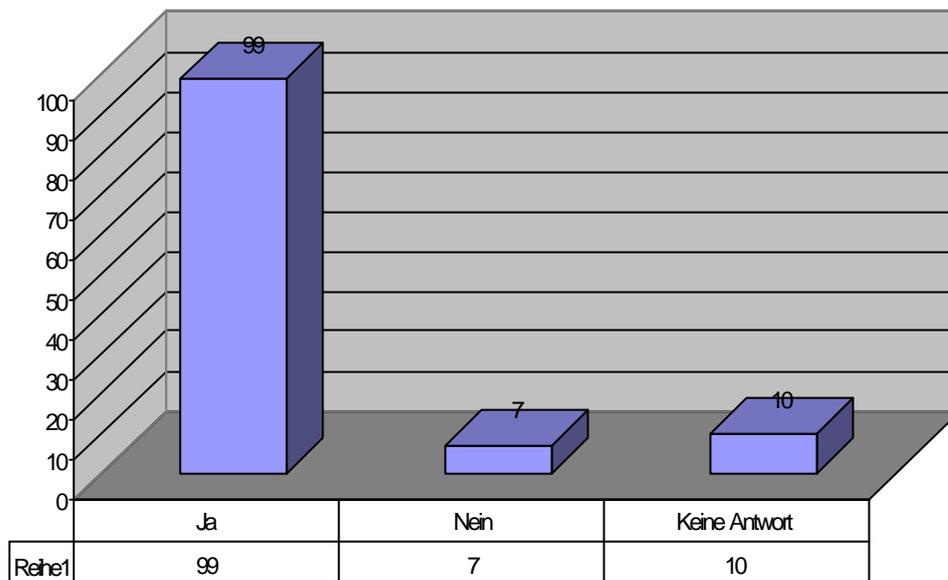


Zusätzliche Anmerkungen:

- „Stadtweite Praktikanten“
- „Sponsoring“
- „demnächst: Schulträger“
- „Firma“
- „Ehemann einer Lehrerin“
- „aber teuer!“
- „außer durch kompetente Schüler“
- „Sohn einer Kollegin hilft“
- „materielle Mittel zum Ausbau, keine für die Wartung und Konfiguration, keine für die Hardware-Wartung“

## 6.11 Frage 11

Haben Sie in Ihrer Schule einen verantwortlichen Netzwerk-Administrator?



Welche Ausbildung, welches Training hat er als Administrator?

- Lehrer (5)
- keine (6)
- Autodidakt (19)
- Selbststudium
- Ohne Ausbildung (3)
- Seminar
- Lehrerfortbildung (4)
- Informatik
- War Softwareingenieur in der Wirtschaft
- Informatik-Fortbildung
- Learning by doing (3)

- Anwenderentwicklung
- Gegenwart bei der Installation
- Schulung und Praxis
- Zertifikatskurs in Informatik
- Eine Lehrkraft betreut das Netz mehr der Not gehorchend, denn als wirkliche Fachfrau – keine Ausbildung!
- Keine spezielle Netzwerkausbildung
- Externe NT-Fortbildung
- 2 x FB á 10 Tage
- Fortbildungsveranstaltungen bei Microsoft und Novell
- Fortbildung Bezirksregierung (2) und Ministerium (3)
- Lehrerfortbildung zu Win NT (2)
- Netwareadmin in einer Firma gewesen
- Praktikum in der freien Wirtschaft (2)
- Studium Informatik (z.Zt.)
- Auf privater Basis, im wesentlichen durch Fachliteratur
- Ehefrau eines Ingenieurs
- TÜV Akademie Rheinland
- Autor verschiedener Computer-Artikel
- Täglicher Umgang mit dem Netzwerk
- Netzbetreuung durch Fachlehrer Mathematik / Physik ohne spezielle Ausbildung für Arbeit mit dem Netz
- 3 Kollegen sind verantwortlich mit Verteilung der Aufgaben: hardware, software, Raumnutzung u.a.
- Autodidakt mit gelegentlichen (mageren) Fortbildungen durch die Behörde
- Teilnahme an MCSE-Kursen

## 6.12 Frage 12

Falls Sie noch kein Netz eingerichtet haben:

Ist eine Vernetzung der Schule in Planung?

Sind Sie an einer Vernetzung interessiert?

Sind Sie an einer Kontaktaufnahme bzw. Beratung interessiert?

	Ja
Planung einer Vernetzung	23
Interesse an einer Vernetzung	19
Interesse an Kontaktaufnahme	31

Zusätzliche Anmerkungen:

- „geplant für den Rest der PCs im Informatik-Raum“
- „neues Netzwerk / Netzwerkerweiterung ab Sommer, Linux / Win 2000 – 2 Teilnetze
- „ein Netzwerk zur Nutzung von Druckern und Scannern ist geplant; dieses soll nicht mit dem Internet-Netzwerk gekoppelt werden. Wir sind an einer Beratung interessiert.“

Welche Gründe sprechen gegen ein Computernetz?

- „Die arbeitsintensive Eingewöhnungsphase und die Kosten.“
- „Nur der hohe Administrationsaufwand neben dem Unterricht (für den Admin).“
- „Datenschutz / Schülerschutz“
- „keine!“

- „Vernetzung aller Rechner (auch der Verwaltungsrechner mit sensiblen Daten) kann zu erheblichen Sicherheitsproblemen führen.“
- „Der Netzwerkadmin. soll wahrscheinlich ein Lehrer sein, der damit neben seiner „normalen“ Tätigkeit den Job eines berufsmäßigen Adm. ausübt. Der Arme! Wie wird das Preis-Leistungs(=Nutzungs)-Verhältnis sein?“

Zusätzlich zur Beantwortung der Fragen sind Zusatzbemerkungen / Freitexteintragungen abgegeben worden. Sie werden hier im unveränderten Originaltext wiedergegeben. Sofern allerdings durch Angaben im Text Rückschlüsse auf den Urheber möglich wären, wurden sie durch den Verfasser verfremdet. Veränderungen dieser Art sind im Einzelfall kenntlich gemacht.<sup>76</sup>

Zum Bereich „technische Umsetzung“:

- „Wir sind zur Zeit im Stadium Planung der Vernetzung der Schule.“
- „Es besteht ein Netz mit 11 Arbeitsplätzen und einem Server, das in den nächsten Monaten in ein Funknetz eingebunden wird. Für die Verwaltung besteht ein Netz von 2 Rechnern, das auch, mit entsprechenden Sicherheits- und Schutzmaßnahmen an das Funknetz angeschlossen werden soll.“
- „Die Schule besitzt 2 physikalisch getrennte Netze. Ein kleines Netz für die Schulleitung / Verwaltung (3 Rechner) und ein „didaktisches“ Netz für den Unterricht (ca. 40 Rechner). Auf dem den Schülern zugänglichen Teil befinden sich keine sensiblen Daten.“

---

<sup>76</sup> Die Einteilung in die Themenkomplexe erfolgte durch Verf.

- „Wir streben an, ein (möglichst Funk) Netzwerk für alle Klassen in den Klassenräumen einzurichten, im Unterricht in Intranet (Wissensdatenbank existiert schon!) und im Internet. Kosten 1. Ausbaustufe 50 – 60 000 DM → Sponsoring?“
- „Im Moment wird jeder Raum angeschlossen.“
- „Im Informatikraum sind alle 17 PC vernetzt. Der nächste Schritt ist die Vernetzung der 4 Verwaltungs-PC, danach sollen in jedem Klassenraum und Lehrerzimmer ein PC stehen, mit Internetzugang und Netzwerkanbindung. Für dieses Vorhaben wollen wir ein Konzept erarbeiten.“
- „Ob Ihnen unser Spezialfall: bisher ein Informatikraum mit 30 Einzelplätzen, aber intendierter Vernetzung, ein Informatikraum mit 6 clients und 1 server, weitere Erkenntnisse liefern kann, weiß ich nicht.“
- „Es gibt in der Schulverwaltung / Lehrerzimmer insges. 5 Rechner unterschiedl. Qualität, die nicht vernetzt sind. Vernetzt sind nur die 10 PC im Computer-Raum.“
- „1. Neues Rahmenkonzept für xyz-Schulen in A-Stadt.<sup>77</sup>
  2. Gesamte Klassen sollen vernetzt werden.
  3. Kleine Pentiums (13iP5, 32 MB RAM, 500 MB HDD, kein CD-Rom) sollen ersetzt werden.
  4. Derzeitiger Zustand nicht zufriedenstellend.“
- „Das Mac-Netz ist wesentlich einfacher und kostengünstiger zu warten, die Software Anat (Apple Administration Toolkit) erfüllt die Erfordernisse eines Schülernetzes bei minimalem Administrationsaufwand. NT ist problematisch, aber eben weiter verbreitet.“
- „Der Proxyserver (Linux) ist über einen 32-Port-Hub 10/100 MBit vernetzt, und zwar über 100 MBit-Kabelverbindung zu den fest installierten Rechnern im PC-Raum und über eine

---

<sup>77</sup> Die Veränderung erfolgte aus datenschutzrechtlichen Gründen. Anm. d. Verf.

Funkverbindung mit 2 Accesspoints zu mobilen Geräten (notebooks) im ganzen Schulgebäude.

Die Arbeitsstationen haben 3 unterschiedliche Arbeitsbereiche als getrennte primäre Partitionen, zu denen der Zugang über ein Bootmanager-Login mit Name und Passwort möglich ist. (I.: Schüler, II.: Lehrerfortbildung, III.: Internet)

Partition I ist so abgesichert (über ein System von Registry-Einträgen), dass Schüler nur mit speziellem Passwort in jeweils ein Anwendungsprogramm kommen. Dabei ist der Zugang zur Systemsteuerung und zu den Laufwerken gesperrt. Auf dem Server sind zwei –Datenlaufwerke eingerichtet, zu denen Schüler Lese- bzw. Schreib-Lese-Zugang haben. Alle Rechnerpartitionen sind als Image-Dateien gesichert und können so bei Störungen / Abstürzen zurückgeschrieben werden.“

- „Es existieren zwei Raumnetze, aber kein Gesamtnetz!
- „Schulnetz befindet sich zur Zeit im Aufbau / in der Erprobung; eine endgültige Strukturierung soll im Sommer erfolgen.“
- „Als pädagogisches Netzwerk ist „master eye“ installiert.“

Zum Bereich „Ausbildung“:

- „Fortbildung und kompetente Ansprechpartner für Administratoren.“
- „Interesse besteht an einer fundierten Ausbildung als Netzwerkadministrator – oder an der Vermittlung entsprechender Fachkräfte.“
- „Dringend geboten: Weiterbildung und Entlastung für Netzwerkbetreuung!! Oder: Struktur Veränderung → Profis für Technik!“
- „Es fehlen niveauvolle Fortbildungen für Lehrer zur Netzwerk-Administration.“

Zum Fragebogen:

- „Der Fragebogen enthält für Schulen ohne interne Vernetzung keine konkreten Hinweise darauf, welche Vernetzung überhaupt sinnvoll ist und worin der Sinn bestehen soll, von Machbarkeit (Geld!) ganz zu schweigen.“
- „Dieser Fragebogen ist teilweise schwierig zu beantworten und schlecht strukturiert.  
Versuchen Sie doch einmal GrafStat2000 für diese Aufgabe einzusetzen. Es wird die Arbeit wesentlich erleichtern und brauchbare Ergebnisse liefern.“
- „Der Fragebogen ist nicht eindeutig. Unsere Schule wird demnächst auf ein neues Netzwerk mit Win 2000 umgestellt.“
- „Ihre Fragen treffen die schulischen Realitäten nicht gut.“

Zum Bereich „Unterstützung“:

- „Die Stadt Hilden hat im Haushalt 2001 ein komplettes IT-Konzept für alle Schulen in Angriff genommen.“
- „Der Internet-Zugang mit zwei Klassenräumen erfordert hohe Stabilität, die mit „selbstgestrickten Lösungen“ nicht zu erreichen sind, auch nicht mit speziellen Schul-Linux-Lösungen. Hier sind professionelle Lösungen mit Zugangsmöglichkeiten der Administratoren zu „know how“ sowie versierte Ansprechpartner für bestehende Probleme gefragt. Speziell für die neuen ADSL-Zugänge gibt es zu wenig Wissen, denn Lehrer sind keine Systeminformatiker, sondern Pädagogen, die sich um Qualität und Einsatzmöglichkeiten von computergestütztem Unterricht kümmern sollten, nicht aber um die technische und konfigurationsmäßige Gestaltung eines stabilen Internetzuganges mit Firewall, Sicherheitsbeschränkungen, Zugriffsbeschränkungen usw.“

- „Ein System für Schulen wäre sinnvoll. Wenn jede Schule für sich alleine bastelt, ist das ungünstig.“
- „Schulen werden mit dem Netz ziemlich allein gelassen.“
- „Ich bin für Rückmeldungen / Hilfen zu praktikablen Netzkonzepten dankbar.“
- „Stadt soll Techniker stellen.“
- „Keine Sicherung vorhanden! Keine technische Hilfe vorhanden!“
- „Alles sehr zeitaufwendig, keine Unterstützung durch den Schulträger etc.“
- „Dringend notwendig: stadtllokale Admin mit Aufgaben Hotline, Pflege und „Gleichschaltung“, Schulung, Installationsunterstützung...“
- „Anbei sende ich Ihnen Ihren Fragebogen zurück.  
Auf die Formulierung „Beauftragter für IuK-Technologien“ aus Ihrem Anschreiben möchte ich noch kurz eingehen:  
Scheinbar besteht bei Ihnen das Missverständnis, die Themen „Internet-Computer – neue Technologien“ würden an den Schulen professionell gehandhabt. Unsere Ausstattung beruht auf Spenden und privater Initiative der Lehrer/Innen und ihrer Angehörigen. Es gibt bei uns keinen IuK-Beauftragten, da weder wir Lehrer über technische Ausbildung noch die Schule über notwendige Mittel für außerschulische Hilfe verfügen, es gibt Ehemänner und Söhne, die in die Schule beordert werden, wenn's mal wieder nicht klappt. Sollten Sie nun annehmen, wir seien die große Ausnahme, weil wir nur eine kleine xyz-Schule sind, dann kann ich aus meinem Erfahrungsaustausch mit Kollegen nur sagen, bis auf die Berufsschulen sieht es fast überall so aus. Die Schulen im Lande sind vollgestopft mit hochmoderner, teurer Technologie, aber für die technische Wartung steht kaum Personal zur Verfügung.  
Wenn Sie Vorschläge zur Gestaltung der Vernetzung von

Schulen entwickeln wollen, scheint es mir ein nicht unwichtiger Hinweis zu sein, dass Sie es auf Seiten der Schulen mit Laien zu tun haben.“

- „Der Staat stellt nur Geld für eine (gute) Hardware / Softwareausstattung zur Verfügung. Wir brauchen viel mehr Zeit und / oder Geld für die anschließende Installation, Pflege, Weiterentwicklung!!“
- „Schulträger und Land NRW tun NICHTS für Administratoren und Netzwerke! Alles nur heiße Luft!“

## 7 Analyse / Auswertung

### 7.1 Fragen 1 und 12

In 88,79 % der zurückgegebenen Fragebogen wird die Aussage getroffen, dass die Schule vernetzt sei. Damit ist der Grad der Vernetzung der betreffenden Schulen unerwartet hoch. Allerdings könnte man den Schluss ziehen, dass gerade diejenigen Schulen, die weder vernetzt sind noch eine Vernetzung planen oder überhaupt ein Interesse daran haben, auch das Ausfüllen und Zurücksenden des Fragebogens ablehnten. Daher könnte der Teilnehmerkreis ohnehin auf diejenigen mit positiver Antwort beschränkt gewesen sein.

Die Antworten lassen zu technischen Fragen teils allerdings so eklatante Unkenntnis erkennen, dass davon auszugehen ist, dass die Beantwortung nicht in allen Fällen von Lehrkräften mit hinreichenden Kenntnissen auf dem Gebiet der Computervernetzung erfolgt ist.

In der detaillierten Betrachtung der Antworten lässt sich feststellen, dass alle diejenigen Schulen, die das Vorhandensein eines Netzes verneint haben, entweder in der Planung einer Vernetzung sind oder zumindest (in einem Fall) Interesse bekunden. **Keine der teilnehmenden Schulen lehnt ein Computernetz ab.** Die einzigen Argumente gegen Computernetze finden sich in den Freitexten der Frage 12 als Hinweise auf Arbeitsintensität und Sicherheitsfragen wieder. Es werden weder Überzeugungen noch Einstellungen als Gegenargumente aufgeführt. **Von der positiven Grundhaltung gegenüber Netzwerken kann also offenbar ausgegangen werden.**

## 7.2 Frage 2

50 der teilnehmenden Schulen geben an, Teilnetze eingerichtet zu haben. In der Betrachtung der weiterhin gegebenen Antworten dieser 50 Schulen zeigt sich, dass in der Mehrheit der Fälle parallel laufende kleine Netze, die physikalisch getrennt betrieben werden, als Teilnetze bezeichnet werden. Echte Teilnetze existieren lediglich in 3 Fällen. Es sind dies diejenigen, die sich auch in den technischen Fragestellungen (Fragen 3 und 4) bzw. in den Freitexten durch besonders detaillierte Angaben auszeichnen. **Die Gestaltung und Funktionenvielfalt von Netzwerken mit Einbeziehung unterschiedlicher Teilnetze scheint bei den meisten Schulen eher unklar.**

## 7.3 Frage 3

Eine prozentuale Verteilung aller Versionsstände zu berechnen, erscheint wenig sinnvoll.

Stattdessen werden die angegebenen Antwortdaten so aggregiert, dass eine sinnvolle Auswertung möglich wird. Es wird daher zusammengefasst zu den Bereichen Novell, Windows und Unix, wobei im Windows-Bereich weiterhin unterschieden wird in „echte Netz- Systeme“ und in sogenannte „Low Cost-Netzsysteme“, also solche, die beispielsweise vom Versionsstand her lediglich für peer-to-peer-Vernetzungen geeignet erscheinen.

Antworten, die offensichtlich nicht die Frage treffen (z.B. peer-to-peer oder TCP/IP als Betriebssystem bezeichnen), bleiben unberücksichtigt. Sie dienen nicht der Zielerreichung dieser Fragestellung, lassen aber den Schluss zu, dass bei einigen Bearbeitern des Fragebogens lediglich marginale Kenntnisse bestehen. Wie mit diesen Kenntnissen Netzwerke be-

treut, gepflegt, administriert werden können, erscheint zumindest fragwürdig.

Die Betrachtung der übrig bleibenden (sinnhaften) Antworten ergibt das folgende Verteilungsbild:

1.	Novell	15
2.	Windows (ohne Versionsangabe)	4
2.11	Win 3.11	1
2.12	Win 95, 98 u.ä.	48
2.21	Win 2000 u.ä.	19
2.22	Win NT (ohne Version)	40
3.	Unix-Produkte / Linux	20
	gesamt	147

Tabelle 3: Verteilung genutzter Betriebssysteme

Von den 147 noch auswertbaren Antworten entfallen daher auf Microsoft-Produkte und Windows als BS 112, die verbleibenden 35 verteilen sich auf Novell und Unix. Damit ist Windows auch hier das am meisten verbreitete System. Dies deckt sich mit den weltweit bekannten Zahlen der Marktanteile von Microsoft-Produkten. Diese legen den Schluss nahe, dass sowohl in allen außerschulischen (somit auch im häuslichen) Bereichen unterschiedliche Windows-Versionen das meistgenutzte Betriebssystem sind. Ihr Einsatz auch in Schulen liegt also nahe.<sup>78</sup> So werden Schüler in

---

<sup>78</sup> Über die Nachteile der unterschiedlichen Windows -Versionsstände und die Unix-Vorteile macht die Literatur teils mit missionarischer Ambition deutliche Aussagen. Das Hochschulrechenzentrum der Universität Wuppertal stellt die Fehlerbelastung und Angreifbarkeit von Microsoft Produkten heraus, vgl. hierzu HRZ- Information des Hochschulrechenzentrums, Nr. 18 / 11. Dezember 2001, BU Wtal sowie Kap. 10 dieser Arbeit, in SAR-NOW, 2000, S. VIII, findet sich ein deutlicher Appell für die Linux-Gemeinde, und auch manch kabarettistischer Kommentar zu MS-Betriebssystemen ist lesens- bzw. hörens wert (gedruckte Version enthält den Text im Anhang, s. 13.3, CD-Version enthält MP3-File, abspielbar mit musicmatch o.ä., zum Start Doppelklick):



killling-my-software.mp3

der Nutzung dessen, was sie von zu Hause kennen bzw. in der Welt außerhalb der Schule vorfinden, sicherer.<sup>79</sup>

Der Hinweis, Unix und seine Derivate erfordere einen erheblich geringeren Pflegeaufwand und sei sicherer und stabiler, ist gut nachvollziehbar. Darüber hinaus sind aktuelle Bestrebungen unterschiedlicher Firmen (wie z.B. SuSe, IBM pp.) zunehmend erfolgreicher, das Betriebssystem auf dem Markt zu etablieren. Da damit eine Open Source-Software zur Verfügung steht, wird Linux durch die finanziellen Vorteile auch für Schulen immer erstrebenswerter. Seit die Stadt München in Erwägung gezogen hat, die gesamte PC-Welt ihrer Verwaltung mit Linux auszustatten, was lediglich durch massive Preispolitik durch Microsoft verhindert werden konnte<sup>80</sup>, ist auch die Signalwirkung einer derartigen Entscheidung für andere kommunale Verwaltungen oder auch gesamte Landesverwaltungen in ihren Konsequenzen zu beobachten. Ob und wie hier Stellung bezogen werden muss, auf welche Weisen man Alternativen finden bzw. bereits bestehende Systeme nutzen und verbinden könnte, soll hier nicht weiter betrachtet werden. Dazu ist eine detaillierte Sicht auf die Leistungsmerkmale und Gegebenheiten erforderlich, was den Rahmen dieser Arbeit sprengen würde.

Für die hier anzustellenden weiteren Betrachtungen gilt als weiteres Befragungsergebnis:

---

<sup>79</sup> SARNOW versucht, die Argumente für Microsoft-Produkte und Windows zugunsten von Linux zu widerlegen; der Vorwurf der Ideologie wirkt jedoch durch allzu deutliche eigene Ausprägung gezwungen, Lebenswirklichkeit und Schulrealität werden von ihm als unvereinbar angesehen:

SARNOW, K.: Linux in der Schule, SuSE GmbH, Nürnberg 2000, S. VII:

*Im privaten Bereich mag jeder Lehrer oder Schüler sein geliebtes und mit ideologischer Verbhrtheit verteidigtes Betriebssystem zu pflegen. In der Schule ist mangels Geld Vernunft und Sachkenntnis gefragt.*

*Die Kritik an Linux hat sich meistens um das Argument „Die Lehrer benutzen zu Hause das System \*\*\* und wollen das auch in der Schule haben“ herum entzündet. Diese Argumentation kann nicht akzeptiert werden. „Schule“ ist nicht „zu Hause“. Beide Umgebungen unterscheiden sich signifikant voneinander, und der Versuch, dies zu übersehen, beschert den Betroffenen viel Ärger.*

<sup>80</sup> Vgl. [http://portale.web.de/Computer/Betriebssysteme/?msg\\_id=3123578](http://portale.web.de/Computer/Betriebssysteme/?msg_id=3123578), Stand 28.05.2003, s. Anlage 2

**Für Schulnetze sind bislang als meistverbreitete Betriebssysteme unterschiedliche Windows-Versionen in Gebrauch.**

#### **7.4 Frage 4**

In einem funktionierenden Schulnetz böte sich die Nutzung eines Mailing-Systems an. Auf diese Weise können Nachrichten an jeden Angehörigen der Schule zügig, klar und nachvollziehbar (z.B. durch Priorisierungen, Quittungen oder ähnliche Optionen) übermittelt werden. Nur 12 der beteiligten Schulen geben allerdings an, ein solches System zu nutzen. Von diesen wiederum geben einige solche Systeme an, die für die Nutzung von e-mail-accounts dienen, nicht aber für interne Netze (z.B. t-online). Nur in Einzelfällen wird auf Exchange-Server, Outlook (als MS-kompatible) oder ähnliches verwiesen.

**Eine Nutzung schulinterner Vernetzung als Kommunikationsmittel wird also nur in Einzelfällen betrieben.**

Es bietet sich daher an, an anderer Stelle erneut diese Frage aufzugreifen und – passend zum Konzept der Betriebssysteme – Kommunikationssoftware für ein Mailing-Konzept in den Schulen erstellen zu lassen. Zuständig für die Entwicklung dieser Konzepte kann nicht jede einzelne Schule für sich sein; hier muss eine umfassende, übergreifende Regelung gefunden werden (s. hierzu Kap. 11).

## 7.5 Frage 5

Nur vier Schulen geben an, mit anderen Schulen vernetzt zu sein. Drei dieser vier Schulen haben in der Beantwortung der anderen Fragen die Begrifflichkeiten des Netzes nicht eindeutig erkannt, häufig mit der Möglichkeit des Internetzuganges verwechselt. Es ist daher davon auszugehen, dass nur eine der vier Schulen tatsächlich mit anderen vernetzt ist. Träger dieser Schule ist die Stadt Hilden, die ein umspannendes Netzwerk aller Schulen ihrer Trägerschaft plant.

Die Möglichkeit, die sich mit der Vernetzung aller Schulen in Form eines Intranets zur Zusammenarbeit miteinander bieten würden, die technischen Möglichkeiten der heutigen Zeit, bleiben so völlig außen vor. Dies allerdings erscheint nur zu verständlich, legt man zu Grunde, dass die Administration eines Netzes in einer Schule mit einer mittleren Schülerzahl (ca. 500 Schüler) der in einem betrieblichen Netz eines mittelgroßen Betriebes gleich kommt (s. hierzu <http://www.initiative21.de>, vom 20.07.01) und dass diese Administration von Lehrern und Lehrerinnen ganz nebenbei erledigt werden müsste.

In den außerschulischen Bereichen der Landesverwaltung wird die komplette Vernetzung aller Verwaltungszweige, die Integration sämtlicher bisher bestehender Netze in ein Landesverwaltungsnetz (LVN) angestrebt. Nur auf diese Weise kann ungehinderte Zusammenarbeit funktionieren, kann Wissens- und Informationsmanagement effizient betrieben werden.

Schulen als Teil öffentlicher Verwaltung sind in dieses Verwaltungsnetz zu integrieren, ungeachtet der Frage, welchem Schulträger sie unterstehen. Verschiedene Zuständigkeiten dürfen im Sinne der Verwaltungsökonomie und zum Nutzen der SchülerInnen sowie zur Entlastung von Lehrern und Lehrerinnen nicht dazu führen, dass der Einsatz moderner IuK-Technik am Zuständigkeitsgerangel scheitert.

Dazu bedürfte es unmittelbar verschiedener Schritte innerhalb der zu beteiligenden Ministerien aller Verwaltungszweige, also auch innerhalb des Ministeriums für Schule, Jugend und Kinder:

- Einrichten eines zuständigen Referates
- Übernahme der Zuständigkeit
- Erarbeitung eines entsprechenden umspannenden Netzkonzeptes
- sukzessive Umsetzung der Netzstrategie
- Übernahme technischen Supports
- Gestaltung von Fortbildungsmaßnahmen

usw.

Dem entgegen stehen die Vermutungen einiger Schulen, die aus den angefügten Freitexten hervorgehen und die erahnen lassen, dass die fehlende Flexibilität der Aufsichtsbehörden eine unmittelbare Reaktion verhindert. Was aber in anderen Bereichen der Verwaltung möglich ist, sollte auch im schulischen Bereich nicht unmöglich gemacht werden.

## 7.6 Frage 6

Keine andere Frage des gesamten Bogens hat zu so vielen Fragezeichen bei den Bearbeitern geführt wie diese. Das Erfordernis zur Einbeziehung dieser Themenfelder in die konzeptionelle Planung eines Netzwerkes scheint bislang nicht erkannt, Kenntnisse über Datenschutz und Datensicherheit fehlen vielfach. Diejenigen Schulen, die versucht haben, Frage 6 zu beantworten, haben durch ihre Antworten zum größten Teil ihr Unwissen über die Probleme von Datenschutz und Datensicherheit dokumentiert. Nur zwei (sic!) der gesamten Fragebögen zeigen, dass der Bearbeiter die Begrifflichkeiten erkennt und ihre Bedeutung einschätzen kann. Nur diese beiden haben dezidierte Vorstellungen zu den Konzepten an ihren Schulen. Dort, wo wenigstens diffuse Vorstellungen von Gefährdungsgraden bestehen, hat man einfach physikalische Trennung einzelner Netze voneinander vorgenommen, nicht aber über Alternativen nachgedacht bzw. Kenntnisse auf den entsprechenden Gebieten erworben. Dass dies den Betroffenen nicht anzulasten ist (für sie ist dieses wiederum eine der ohnehin zahlreichen zusätzlichen Belastungen), ist offenkundig. Gerade in der heutigen Zeit, in der Viren- und Wormattacken im und aus dem Web, Hackerangriffe und Computermanipulationen für Schlagzeilen sorgen, können Sicherheitsaspekte nicht außer Acht gelassen werden, sie müssen vielmehr ins Zentrum der Betrachtungen rücken.

Da also gerade in diesem Bereich erhebliche Defizite zu bestehen scheinen, wird sich der zweite Teil dieser Arbeit (Kap. 8 ff) mit genau diesen allgemeinen Fragen zur Sicherheit von Schulnetzen und zum Bereich Datenschutz befassen und versuchen,

- das erforderliche Basiswissen zu vermitteln, um Schulen die selbständige Erarbeitung und Umsetzung von sicheren Konzepten zu ermöglichen (Kap. 8, 9, 10)

- ein denkbare Konzept zur Einrichtung eines funktionierenden umfassenden Schulnetzes zu skizzieren (Kap. 7, S. 108 sowie Kap. 11).<sup>81</sup>

## 7.7 Fragen 7 und 8

**Die Nutzer bestehender Netze in Schulen sind in erster Linie die Schüler, gefolgt von Lehrern.** Schulleitung und Sekretariat nutzen das Netz nur in rund einem Viertel der Fälle. Dabei ist zu beachten, dass es sich hier um die Nutzung des Internets, damit des www, handelt; ein internes Netzwerk in Form eines Intranets ist zunächst nicht in der Betrachtung. Dies liegt einerseits an der bereits genannten begrifflichen Unbestimmtheit (die Befragten definieren den Begriff „Netz“ in der Mehrheit der Fälle offenbar als Internetzugang), andererseits auch am grundsätzlichen Fehlen eines funktionierenden Intranets. Bei einer Vollvernetzung der Verwaltung einschließlich der Schulen in Form eines Landesverwaltungsnetzes (vgl. Kap. 7.5) würde dies anders werden müssen, online-Kommunikation im schulischen Intranet würde möglich, Einmal erfassung und Mehrfachverwendung von Daten und Informationen jeglicher Art würden möglich, der Verwaltungsaufwand teils minimiert.

Damit würde auch eine gleichmäßige Auslastung der Nutzungsmöglichkeiten erreicht werden. Während zur Zeit noch rund 90 % der Nutzungen im Zusammenhang mit dem Unterricht stehen und nur rund ein Viertel für Verwaltungsaufgaben entfällt,<sup>82</sup> könnte sich bei umfassender Vernet-

---

<sup>81</sup> Eine detailliertere Darstellung, die über eine Skizze hinausginge, kann im Rahmen dieser Arbeit nicht erfolgen; sie könnte bestenfalls Gegenstand einer weiteren Aufgabe und Betrachtung werden.

<sup>82</sup> Die umfangreiche Nutzung des Netzes im Unterrichtsgeschehen sagt lediglich etwas darüber aus, dass die Nutzung größtenteils für den Unterricht und im Unterricht erfolgt. Diese Aussage überrascht nicht, wenn man bedenkt, dass ohnehin die Mehrheit der schulischen Vorgänge solche des Unterrichtsgeschehens sind. Interessant wäre an dieser Stelle die Erhebung eines weiteren Datums, das jedoch nicht Gegenstand des Fragebogens war: Welches Potential ist innerhalb der Schulen bislang ungenutzt vorhanden, auf das für zukünftige Nutzungen zusätzlich zurückgegriffen werden könnte?

zung eine Vollnutzung erzielen lassen, die auch eine Kommunikation zwischen Nutzern ermöglicht, damit sowohl dem Unterrichtsgeschehen als auch der Verwaltungstätigkeit neue Möglichkeiten eröffnet.<sup>83</sup>

Zur Zeit dürfte die erhebliche Nutzung im Unterricht mit der Tatsache zusammenhängen, dass in den meisten Schulen das Netz noch im Informatik-Raum besteht und für Informatik-Unterricht genutzt wird und für Fachunterricht nur in Ausnahmefällen. Eine umfassende PC-Nutzung scheidet allein wegen der fehlenden technischen Ausstattung in den meisten Fällen aus. Nur dort, wo getrennte Verwaltungsnetze bestehen, werden auch Verwaltungsaufgaben im Netz abgewickelt.

Interessant ist an dieser Stelle die Feststellung, dass das Netz zwar in rund 44 % der Fälle für Unterrichtsvorbereitung genutzt wird, für Unterrichtsnachbereitung jedoch nur in rund 15 % der Fälle. Hier stellt sich die Frage, ob wiederum Begrifflichkeiten unklar angewandt wurden (wird Unterrichtsvorbereitung mit Internetrecherche betrieben, die für die Nachbereitung nicht mehr erforderlich ist?) oder ob tatsächlich Unterrichtsnachbereitungen im Netz nicht erfolgen. Dies aber würde die Möglichkeiten eines Netzwerkes nicht ausschöpfen. Da mögliche Ursachen hier aber nur spekulativ betrachtet werden können und nicht eigentlich Gegenstand der Arbeit sein sollen, soll auf diese Frage hier nicht näher eingegangen werden.

---

<sup>83</sup> Vgl. hierzu GRÄTZ, unter [www.goethe.de](http://www.goethe.de)

## 7.8 Frage 9

Rund 73 % der Schulen geben an, im Internet präsent zu sein. Die stichprobenartige Suche nach den entsprechenden Sites ergibt, dass manche Schulen hier ein wenig „hochstapeln“, andere mit äußerst professionell gestalteten Seiten aufwarten können. Insgesamt lässt sich aus der hohen Anzahl positiver Antworten schließen, dass **die Schulen die Bedeutung des Internets in der heutigen Zeit, den positiven Effekt einer Web-Präsenz anerkannt haben und daher versuchen, sich selbst entsprechend zu präsentieren.**

## 7.9 Fragen 10 und 11

Rund 62 % der beteiligten Schulen geben an, keine Hilfe und Unterstützung zu erhalten. In 85 % gibt es einen verantwortlichen Administrator. Diese beiden korrespondierenden Ergebnisse weisen auf einen erheblichen Missstand in der Vernetzung der Schulen hin:

Es ist politischer Wille, Schulen mit Netzwerk arbeiten zu lassen, in der Umsetzung der Vorgaben zur Erreichung dieses politischen Zieles sind die Schulen aber in der Mehrheit der Fälle auf sich gestellt.<sup>84</sup> Ohne das

---

<sup>84</sup> vgl. hierzu: Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000

*Eine Schlüsselposition in diesem Spannungsfeld fällt der Kollegin oder dem Kollegen einer Schule zu, der freiwillig oder per Aufgabenzuweisung durch die Schulleitung die Betreuung der EDV betreiben bzw. vorantreiben darf. Doch dieses augenscheinlich reizvoll und zukunftssträchtige Betätigungsfeld erweist sich für betroffene schnell als nicht enden wollender „Kampf gegen Windmühlen“, der sich ohne Wenn und Aber weit in die Freizeit erstreckt, die Unterrichtsarbeit nicht unwesentliche tangiert und für die Aktiven wenig Dank nach sich zieht.*

*Im Vergleich mit Funktionen wie dem Beratungslehrer oder einem Fachbetreuer, der in lang angelegten Lehrerfortbildungen stufenweise an seine Aufgaben herangeführt wird, erfährt der SystembetreuerIn keine vergleichbare Förderung. Vielmehr bleibt es weitgehend ihm überlassen, sich in neue Betriebssysteme, Soft-*

Engagement einzelner ist der Einsatz von Netzwerken in Schulen nicht zu erreichen. Wenn Sponsoren gefunden werden, die die Hardwareausstattung finanzieren, stehen allzu häufig diese Geräte im Keller, bis sich ein Lehrer findet, der die Konfiguration und Installation zusätzlich zu seinen eigentlichen Aufgaben übernimmt, ohne eine auch irgendwie geartete Entlastung zu erfahren. Hier wird der Dienstherr seiner Fürsorgepflicht nicht gerecht.

Ohne die selbstlose Eigeninitiative der Betreffenden sind Vernetzung, Fortbildung, Arbeit im Netz usw. nicht möglich. Es bedarf dringend der Einrichtung einer zentralen Dienststelle zur Übernahme dieser Aufgaben. In den Schulen sind teilweise autodidaktisch fundiert aus- und fortgebildete Fachleute vorhanden, auf deren know-how man zurückgreifen und das man in den Dienst aller Schulen stellen sollte. Nicht jede Schule, jede Kommune oder jeder Schulträger muss für sich das Rad neu erfinden.

---

*und Hardware autodidaktisch einzuarbeiten. Bei den vergleichsweise wenigen EDV-Fortbildungen von EDV-Idealisten mit vollem Unterrichtsauftrag“, der unzureichenden, halbherzigen Unterstützung der vorgesetzten Dienststellen sowie den ungenügenden finanziellen bzw. technischen Ausstattung sind dies Rahmenbedingungen, die künftigen Erfordernissen der hochkomplexen Informations- und Telekommunikationstechnologie derzeit nicht entsprechen.*

(Vorwort an den Leser)

*Als problematisch erweist sich dabei, dass es sich bei den schulischen Systembetreuern i.d.R. um Autodidakten handelt, denen die Systembetreuung als dienstliche Zusatzaufgabe angetragen wurde. In diese Zusatzaufgabe hat sich diese Lehrerguppe dann meist im Selbststudium und als „Einzelkämpfer“ nach dem Prinzip Versuch und Irrtum eingearbeitet und so bestehende Schulinstallationen ohne Unterstützung von außen begründet. Dies hat zur Folge, dass ich im schulischen Umfeld keine homogene Installationsstruktur wiederfindet, sondern dann eine Vielzahl einzelner, von Lehrern entwickelter Nischenlösungen das Bild prägt. Dies ist unter anderem eine der Hauptursachen für das viel zitierte Dilemma der zeitlichen Überlastung der Systembetreuer, da ähnliche Arbeiten und Entwicklungen im Alleingang vielfach mit identischer Problemstellung und Zielsetzung ausgeführt werden.*

Teil 2-2, Seite 1

Daher gilt: an dieser Stelle ist Zentralisierung das einzige probate Mittel zur Erreichung einer zügigen, umfassenden Netzwerktopologie in der Schulwelt des Landes NRW.

### **7.10 Zusammenfassung der Auswertungsergebnisse**

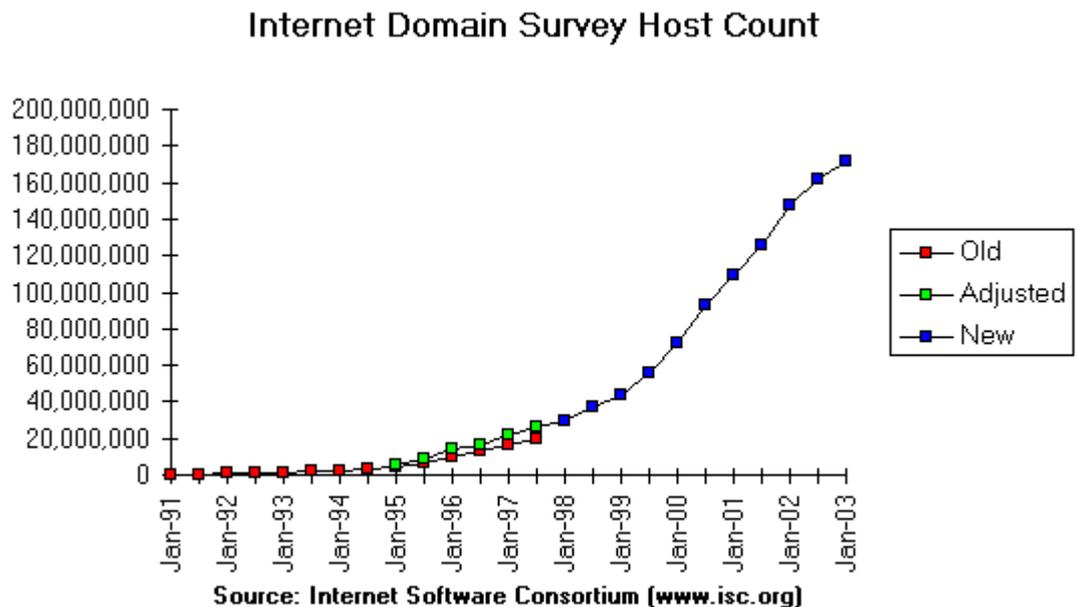
- Keine der teilnehmenden Schulen lehnt ein Computernetz ab.
- Die Gestaltung von Netzwerken mit Einbeziehung unterschiedlicher Teilnetze scheint bei den meisten Schulen eher unklar.
- Unterschiedliche Windows Versionen sind bislang als Betriebssysteme die für Schulnetze am weitesten verbreiteten.
- Eine Nutzung des schulinternen Netzes als Kommunikationsmittel wird nur in Einzelfällen betrieben.
- Die Möglichkeit, die sich mit der Vernetzung aller Schulen in Form eines Intranets zur Zusammenarbeit miteinander bieten würden, die netztechnischen Möglichkeiten der heutigen Zeit, bleiben außen vor.
- Das Erfordernis zur Einbeziehung der Themenfelder Datenschutz und Datensicherheit in die konzeptionelle Planung eines Netzwerkes scheint bislang nicht erkannt, Kenntnisse über Datenschutz und Datensicherheit fehlen vielfach.
- Die Nutzer bestehender Netze in Schulen sind in erster Linie die Schüler, gefolgt von Lehrern.
- Die Schulen haben die Bedeutung des Internets in der heutigen Zeit, den positiven Effekt einer Web-Präsenz anerkannt und versuchen daher, sich selbst entsprechend zu präsentieren.
- Es ist politischer Wille, Schulen mit Netzwerk arbeiten zu lassen, in der Umsetzung der Vorgaben zur Erreichung dieses politischen Zieles sind die Schulen aber in der Mehrheit der Fälle auf sich gestellt.

Da also offenbar die Notwendigkeit zur Nutzung moderner Technik und damit die Einbeziehung von Netzwerken in den schulischen Alltag von allen Beteiligten aus den unterschiedlichsten Gründen bejaht wird, ist von dem Erfordernis auszugehen, dass geeignete Netzwerkgestaltungen zu finden und zu erläutern sind. Dabei soll sich diese Arbeit nicht über die bereits in Kap. 2 gemachten Aussagen hinaus mit der technischen Umsetzung beschäftigen, die bereits in der Standardliteratur vielfach sehr detailliert beschrieben wird (vgl. Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000 sowie COMER1(998), LARISCH (2000) usw.).

Vielmehr soll hier zunächst der Sicherheitsbereich betrachtet werden, um klare Begrifflichkeiten hinsichtlich Datenschutz und Datensicherheit zu schaffen. Es sollen die Erfordernisse an Netzwerke, die sich daraus ergeben, dargestellt und daraus resultierend ein Vorschlag erläutert werden, wie schulische Netzwerke unter diesen Prämissen aussehen könnten.

## 8 Datenschutz / Datensicherheit und Internet

Die Anzahl der im Internet auf unterschiedlichen Wegen miteinander kommunizierenden Rechner ist nur zu vermuten; es ist davon auszugehen, dass es sich um Millionen einzelner PC handelt, teils sind diese bereits in internen Vernetzungen zusammengeschlossen. Diese Millionen verschiedener Rechner kommunizieren miteinander durch die Nutzung verschiedener Hosts. Die Anzahl der vorhandenen Hosts ist in den vergangenen Jahren ebenfalls sprunghaft angestiegen, wie die folgende Abbildung zeigt:



**Abbildung 9: Entwicklung der Anzahl von Hosts 1991 bis 2003**

Quelle: [www.isc.org](http://www.isc.org), Abfrage vom 04.11.2003, 12.52 Uhr<sup>85</sup>

Eine weltweite Kommunikation ist damit möglich, durch das Entstehen der virtuellen Welt als „Parallelwelt“ sind alle Lebensbereiche auch in diese Virtualität verlagert worden, womit Kommunikation aber auch in vie-

---

<sup>85</sup> Unter derselben Adresse findet sich eine tabellarische Aufstellung der Host-Zahlen von 1981 (213) bis 2003 (171.638.297). Es ist davon auszugehen, dass die Zahl der PCs noch erheblich höher sein dürfte.

len Bereichen unkontrollierbar geworden ist. Während man in der realen Welt dem Dialogpartner in aller Regel beim Gespräch in die Augen sehen kann oder zumindest die Stimmmodulation im Gesprächsverlauf verfolgen kann, ist in der virtuellen Dialogwelt noch nicht einmal sicher, dass man tatsächlich mit dem vermuteten Gegenüber spricht, dass dieser Kommunikationspartner tatsächlich der ist, für den er sich ausgibt, ob er vor einem Rechner in einem anderen Kontinent sitzt oder im Haus nebenan.

Während zu Beginn des Internet-Zeitalters die Gefahren innerhalb des Netzes eher gering geschätzt wurden, nahmen in den letzten Jahren auch mit der rasanten Steigerung der Anzahl von Usern die bekannt gewordenen Fälle der Attacken und Hackings ebenso zu wie die Zahl derer, die die PC-Welt zur Abwicklung ihrer Geschäfte nutzen. Damit muss sich auch der Privatmann (dessen Bedürfnisse andere sind als die der Verwaltung und Behörden und damit auch der Schulen, s. hierzu Kap. 9.4) heutzutage Gedanken darüber machen, wie er unberechtigte Zugriffe von seinem PC abwehren kann<sup>86</sup>, über den er die Bankgeschäfte im online-Verfahren abwickelt, real-time-Börsengeschäfte erledigt und ähnliches.

Gerade die in der jüngsten Vergangenheit in Umlauf gebrachten Würmer „Lovesan“<sup>87</sup> und „Sobig“ bis „Sobig F“<sup>88</sup> haben die Angreifbarkeit

---

<sup>86</sup> Auch für Laien gut verständliche Erläuterungen und Handlungsanweisungen hierzu finden sich in RRZN – Regionales Rechenzentrum für Niedersachsen / Universität Hannover: Computersicherheit im Internet für Anwender. Juni 2001 sowie in JANSSEN, A.: Vorsicht... Viren, Hacker, Firewalls; Sicherheit am PC. O.O. 2002 (KnowWare Nr. 170)

<sup>87</sup> Lovesan sollte einen der Microsoft-Server attackieren, was durch Microsoft jedoch noch rechtzeitig verhindert werden konnte. Eine Vielzahl von privaten PC (Schätzungen sprechen von bis zu 200.000 PC) wurden infiziert, was sich durch ständiges Herunterfahren der Rechner nach dem Einloggen ins Internet äußerte. Vgl. hierzu: [www.techchannel.de](http://www.techchannel.de), News vom 15.08.2003, s. Anlage 3

<sup>88</sup> „Sobig F“ ist eine Weiterentwicklung des Sobig-Wurms, der sich durch e-Mails verbreitet. Sobald die Anlage einer dieser Mails geöffnet wird, wird auf dem betreffenden Rechner ein Trojaner installiert, womit der Rechner für jeden Datenzugriff von außen offen ist. Einziges Gegenmittel: infizierte Anhänge isolieren und ungeöffnet löschen. Dazu bedarf es einer aktuellen, gut funktionierenden Sicherheitssoftware, s. hierzu Kap. 10 sowie [web.de](http://web.de) Portale > Internet vom 25.08.2003, s. Anlage 4

innerhalb des Systems ebenso verdeutlicht wie das Erfordernis, dass auch jeder private PC entsprechende Sicherheitsvorkehrungen benötigt<sup>89</sup>, um nicht einerseits selbst von den zerstörerischen Würmern, Trojanern oder Viren befallen zu werden und um andererseits nicht auch eine wesentliche, aber unrühmliche Rolle in deren weiterer Verbreitung spielen zu müssen.

Schwierig ist diese Absicherung besonders im Bereich der Datenmissbräuche, da hier nicht – wie bei herkömmlichen Diebstahlsdelikten – die weggenommene Sache wirklich „weg“ ist, sondern schlicht und einfach eingesehen wurde, kopiert (damit dupliziert) und dann genutzt werden konnte. Während der Geschädigte die Wegnahme einer realen Sache in aller Regel problemlos bemerkt, wird die Einsichtnahme und Nutzung von Daten erst dann festgestellt, wenn es zu „Sekundärschädigungen“ gekommen ist, also z.B. zu einer Abhebung vom Konto des Geschädigten oder zu einer geschäftlichen Transaktion zu seinen Lasten.

Zwar hat der Gesetzgeber auf derartige Veränderungen in der „Landschaft der Straftaten“ bereits vor geraumer Zeit reagiert, indem zusätzliche Straftatbestände eingearbeitet wurden (vgl. hierzu § 263 a StGB - Computerbetrug -, § 303 a StGB – Datenveränderung -, § 303 b StGB – Computersabotage -).<sup>90</sup> Diese Strafandrohungen greifen aber erst dann, wenn es zumindest zum unmittelbaren Ansetzen zur Verwirklichung eines der Tatbestände gekommen ist (§ 22 StGB; der Versuch ist in allen drei Fällen strafbar!), es also zu einem feststellbaren An- oder Eingriff gekommen ist. Auch hier gilt, dass Prävention die sinnvollere Alternative ist vor repressiven Maßnahmen.

---

<sup>89</sup> S. hierzu HRZ – Informationszentrum des Hochschulrechenzentrums der Bergischen Universität Wuppertal, Nr. 18 / 11. Dezember 2001

<sup>90</sup> Zur näheren Erläuterung der Tatbestandsmerkmale bzw. der Abgrenzung zu den übrigen Straftatbeständen der Deliktsgruppe s. gängige Strafrechtskommentare wie TRÖNDLE / FISCHER, LACKNER / KÜHL oder SCHÖNKE / SCHRÖDER. Für SCHÖNKE / SCHRÖDER ist zu beachten, dass das 6. Strafrechtsänderungsgesetz, das allerdings den hier angesprochenen Bereich nicht tangiert, von 1998 noch nicht eingearbeitet wurde: letzte Auflage von 1997.

Nicht erst die Wegnahme, Nutzung oder Veränderung von Daten muss also verhindert werden, zu schützen ist bereits gegen die unbefugte Einsichtnahme in jeglichen Datenverkehr, die die weiteren Schritte erst ermöglicht. Und das in einem Informations- und Kommunikationsmedium, das nachgerade davon lebt und seine besondere Bedeutung daraus erlangt, dass es Datenverkehr und Datenfluss ungehindert ermöglicht, „lediglich“ an den Schaltstellen der Datenübermittlung durch Protokollierung Kommunikationswege und Zugriffe registriert. Protokolle aber gibt es nur über einmal realisierte Bewegungen, sie sind also rein retrospektiv. Eine präventive Maßnahme wird nur durch besondere Sicherungssoftware oder Maßnahmen der Netzgestaltung in Intranets erreicht (s. hierzu Kap. 10).

Es geht also darum, Zugriffe zu verhindern oder zu erschweren, um die Datensicherheit zu gewährleisten und um zu verhindern, dass entstandene Daten Rückschlüsse auf konkrete Personen zulassen.

Die Vielfalt der technischen Möglichkeiten, ungehinderte und unautorisierte Zugriffe auf eigene Daten zu verhindern, wie z.B. Kryptierungen, Verschlüsselungen, Firewalls u.ä., sind durch die User gezielt einzusetzen, um das eigene Recht auf informationelle Selbstbestimmung (RiS, s. Kap. 9.2) aktiv auszuüben. Das aber setzt auch voraus, dass der einzelne User über das Vorhandensein und die Nutzungsmöglichkeiten derartiger technischer Instrumente informiert ist und auch in der Lage, sie sicher einzusetzen. Ohne eine derartige technische Kenntnis und Kompetenz in der Umsetzung gelingt das aktive Gestalten des Rechts auf informationelle Selbstbestimmung nur den wenigen „Freaks“. Ziel muss also im Zeitalter der grenzenlosen Internet-Kommunikation sein, die Kompetenzen einzelner auch auf diesem Gebiet zu fördern; hier liegt eine Möglichkeit für neue, zusätzliche Thematiken im schulischen Unterricht. Es besteht gleichsam eine Notwendigkeit, in schulische Inhalte diejenigen Anforderungen hinsichtlich Datenschutz und Datensicherheit einzubeziehen, die durch den täglichen Umgang mit der Technik und aktuelle Entwicklungen erforderlich werden, wie sie auch in Kap. 9 und 10 aufgezeigt werden.

Und nicht zuletzt dient auch das Internet bereits als Plattform für Straftaten, als eine Art „virtueller Tatort“, bei dem im eigentlich rechtlichen Sinne (§ 9 StGB) kein Tatort festgeschrieben oder festgestellt werden kann. Dies wiederum erschwert die Möglichkeiten, Verstöße zu verfolgen und zu ahnden. Die genaue lokale Herkunft strafbarer Internet-Inhalte (an die die Zuständigkeit einer Ermittlungsbehörde und eines Gerichtes geknüpft ist) ist ebenso schwierig zu ermitteln wie der tatsächliche Urheber verbotener Inhalte. Das Aufspüren strafbarer Inhalte im Internet (z.B. kinderpornografische Inhalte, Aufrufe oder Verabredungen zu Verbrechenstatbeständen) erfordern spezielle Softwareeinsätze. Die Ermittlung der Urheberschaft derartiger Inhalte ist darüber hinaus nur mit Hilfe weiterer Softwarelösungen möglich. Software-Entwickler unternehmen bereits seit geraumer Zeit, teils in Zusammenarbeit mit den Ermittlungsbehörden, alle Anstrengungen, diese Lücke zu schließen.<sup>91</sup> Die Selbstregulierung der Internet-User (sog. netiquette aus den Anfangszeiten des Internet) ist an ihre Grenzen gestoßen<sup>92</sup>, weitergehende Regularien aber sind außer denen des Bundesdatenschutzgesetzes bislang nicht erlassen. Und diese sind vielfach unbekannt, oder es existiert lediglich eine mehr oder minder diffuse Vorstellung von den Bestimmungen.

Eine von manchen Datenschützern geforderte Herstellung absoluter „Unbeobachtbarkeit“ aber wäre das andere Extrem: Eine niemals und unter keinen Umständen nachvollziehbare Kommunikation zwischen Personen kann und darf es auch nicht geben. Sofern nur und ausschließlich der Einzelne über das Maß der Offenheit seiner Kommunikation entscheiden kann, werden Sicherheitsbedürfnisse unerfüllt bleiben. Einmal mehr ist hier – durch politische Entscheidung – das Spannungsfeld zwischen Freiheit und Sicherheit des Einzelnen zu bedenken und möglichst weitgehend auszugleichen; gänzlich aufheben lässt es sich auf Grund der konträren Inte-

---

<sup>91</sup> Die existierenden Software-Lösungen sind wegen ihrer Bedeutung als Verschlusssache zu behandeln; daher wird an dieser Stelle auf weitere Ausführungen verzichtet.

<sup>92</sup> Vgl. hierzu BfD, 16. Tätigkeitsbericht, 1997

ressen nicht. Man denke nur an die Ereignisse der jüngsten Vergangenheit im internationalen Terrorismus, aber auch an die bereits weit verbreiteten Strukturen der Organisierten Kriminalität<sup>93</sup> und stelle sich vor, dass jegliche Kommunikation, ob über Internet, Telefon, Fax oder wie auch immer, unbeobachtbar, nicht nachvollziehbar, nicht nachweisbar und nicht rückverfolgbar wäre, eine Ermittlung und Verfolgung möglicher Straftäter wäre unmöglich. Der allgemein bekannte Ausspruch „Datenschutz ist Täterschutz“ bekäme eine Daseinsberechtigung zum Nachteil der Gesamtgesellschaft.

Datenschutz hat also gerade durch die Möglichkeiten des Internets wesentliche Bedeutung gewonnen; gäbe es ihn gar nicht, wären der User und seine jeweiligen Aktivitäten inklusive der Internet-Kommunikation gläsern. Würde er aber als ausschließlicher Anspruch in den Vordergrund gestellt, gäbe es keine Möglichkeiten staatlicher Interventionen mehr. Nur das „gesunde“ Mittelmaß kann der richtige Weg sein.

Aber nicht nur im Internet und seiner grenzenlosen Kommunikation sind Datenschutz und Datensicherheit von grundlegender Bedeutung. Auch in den Bereichen, in denen es losgelöst vom World Wide Web zur Feststellung von Personendaten im weitesten Sinne kommen kann, müssen die Anforderungen berücksichtigt werden. Dazu ist zunächst einmal Klarheit darüber zu erlangen, was Datenschutz und Datensicherheit überhaupt bedeuten und welchen Stellenwert sie in den unterschiedlichen Bereichen alltäglichen gesellschaftlichen Lebens, damit auch schulischen Lebens, erlangt haben.

---

<sup>93</sup> Der Begriff „Organisierte Kriminalität“ (OK) umfasst sowohl Organisationen mit mafiösen Strukturen als auch jedwede Form der Kriminalität, die die Anforderungen der Definition erfüllen: OK ist „...die „von Gewinn- und Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Zeit arbeitsteilig

- unter Verwendung gewerblicher oder geschäftsmäßiger Strukturen,  
- unter Anwendung von Gewalt und anderer zur Einschüchterung geeigneter Mittel oder

- unter Einflussnahme auf Politik, Medien, Öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.“ Die Zeit, Nr. 37 / 93

## 9 Datenschutz

Das Themenfeld des Datenschutzes kann hier nur in seinen grundsätzlichen Aussagen aufgegriffen werden, eine umfassende Darstellung des Datenschutzbereiches ist in dieser Arbeit auf grund der weitreichenden Bedeutung für alle Lebensbereiche nicht möglich, sie würde den Rahmen der Arbeit sprengen. Daher soll hier lediglich einen Abriss zu den für das vorliegende Thema wesentlichen Kernbereichen geboten werden.

### 9.1 Grundsätzliche Inhalte des Datenschutzes

Unter dem Begriff Datenschutz versteht man (landläufig) „...Maßnahmen zum Schutz gespeicherter oder übertragener Daten von natürlichen Personen gegen Verfälschung oder unberechtigte Benutzung...“.<sup>94</sup> Weiter gehen die Erläuterungen zum Begriff in der Fachliteratur, da nicht Definitionen versucht werden, sondern Erläuterungen zu den Kernbereichen des Gesetzes dargelegt werden.<sup>95</sup>

---

<sup>94</sup> *Der Brockhaus in einem Band*. 9., vollständig überarbeitete und aktualisierte Auflage. Mannheim: Bibliographisches Institut & F.A. Brockhaus 2002.

<sup>95</sup> So TETSCH / TEMME, 1998, S. 172:

Der Begriff „...umfasst als Rechtsbegriff alle Regelungen, die unmittelbar den Umgang staatlicher und privater Stellen und Personen mit fremden Daten betreffen, insbesondere die

- Befugnisse der datenverarbeitenden Stellen zur Erhebung, Speicherung, Veränderung, Nutzung und Übermittlung
- Rechte der Betroffenen auf Berichtigung, Sperrung und Löschung der Daten, auf Auskunft und Schadensersatz.

Schutzbereich des Bundesdatenschutzgesetzes sind also Daten natürlicher Personen. Als Datum im Sinne dieser Regelung gilt jedes personenbezogene Datum, also eine wie auch immer geartete Information über die Verhältnisse einer bestimmten oder bestimmbarer Person.<sup>96</sup> Damit wird deutlich, dass nicht nur der allgemeine Begriff eines „Datums“ von den Regelungen des Gesetzes umfasst ist, sondern jedwede Information, die sich direkt oder indirekt auf konkrete Personen bezieht oder beziehen lässt oder die so gestaltet ist, dass man eine konkrete Person über dieses Datum ermitteln kann, also auch Bilder, Videos, Stimmufzeichnungen, daktyloskopisches und DNA-Material u.ä.

Jedes wie auch immer geartete Datum, also jede Information, ist geschützt von dem bereits erwähnten Recht auf informationelle Selbstbestimmung als Ergebnis des allgemeinen Persönlichkeitsrechts, das die Privatsphäre Einzelner schützt, so dass jeder das Recht hat, über die Preisgabe seiner persönlichen Daten und deren Verwendung selbst bestimmen zu dürfen.<sup>97</sup> Schutzzweck des Gesetzes, das konkret festschreibt, wer unter welchen Voraussetzungen welche Daten erheben, speichern und weitergeben darf, ist die Bewahrung von Daten vor Veränderlichkeit und unberechtigter Benutzung als einen Bereich des allgemeinen Persönlichkeits-schutzes.

Diese Formulierung indiziert, dass es auch eine berechtigte Nutzung (oder Verfälschung) entsprechender Daten geben kann.

Berechtigt ist die Nutzung der persönlichen Daten dann, wenn einer von mehreren Erlaubnis- oder Gesetzesvorbehalten gegeben ist:

---

<sup>96</sup> Legaldefinition in § 3 Abs. 1 BDSG sowie den Ländergesetzen, für NRW gilt § 3 Abs. 1 DSG NW

<sup>97</sup> Bundesverfassungsgerichtsentscheid vom 15.12.1983 über die Verfassungsmäßigkeit des „Gesetzes über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung“, sog. Volkszählungsgesetz – VZG -, BVerfGE 65, 1; s. hierzu SCHWABE, J.: Entscheidungen des Bundesverfassungsgerichts; Studienauswahl, Hamburg 1994, S. 38 ff, sowie TETSCH / TEMME (1998), S. 151 ff

- Erlaubnis zur Nutzung der Daten liegt immer dann vor, wenn
- der betroffene Dateninhaber seine persönliche Einwilligung erteilt
  - ein Gesetz/ eine Verordnung die Nutzung zulässt.

Das heißt, dass der jeweilige Dateninhaber seine Einwilligung geben kann, was dann zur berechtigten Nutzung seiner Daten durch andere führt. Diese Einwilligung kann auf unterschiedliche Arten erteilt werden; denkbar ist die Erlaubnis in verbaler, schriftlicher Form oder durch konkludentes Handeln (wer z.B. ein videoüberwachtes Einkaufszentrum betritt, bei dem an den Eingängen auf die Überwachung hingewiesen wird, erklärt durch das Betreten an sich in Form konkludenten Handelns sein Einverständnis, s. hierzu Kap. 9.2). Grundsätzlich ist die Verarbeitung von Daten zweckgebunden, das heißt die Daten dürfen nur für den für die Erhebung maßgeblichen Zweck verarbeitet werden. Ausnahmen bestehen dann, wenn durch Ermächtigungen die Verwendung (= Speicherung, Verarbeitung oder Weitergabe) des Datenmaterials, auch wenn es sich um nur ein einziges Datum handelt, erlaubt und damit gerechtfertigt ist. Derartige Rechtsgrundlagen für Eingriffe in das RiS finden sich z.B. in der Strafprozessordnung für die Fälle einer Strafverfolgungsmaßnahme, in den Polizeigesetzen der Länder für Maßnahmen der Polizei zur Gefahrenabwehr usw. (s. hierzu TETSCH / TEMME, Bd. 1, 1998).

Verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen ist immer diejenige öffentlich rechtliche Stelle, die die Daten verarbeitet, also sie im rechtlichen Sinne verwendet.<sup>98</sup> An Hand dieser Definition lässt sich erkennen, dass auch jede Schule datenverarbeitende und daher datenverantwortliche Stelle ist: Schülerdaten, die durch das Sekretariat einer Schule verarbeitet werden, obliegen der Verantwortlichkeit genau dieser Schule, sind also entsprechend zu handhaben, zu pflegen und zu schützen (s. hierzu Kap. 9.3).

---

<sup>98</sup> § 3 Abs. 7 BDSG sowie § 3 Abs. 3 DSG NW

Dabei ist zu beachten, dass unter dem Stichwort „personenbezogenes Datum“ nicht nur diejenigen Daten als sensibel anzusehen sind, die konkret mit der Person verbunden sind, also Name, Vorname, Geburtsdatum und –ort, Anschrift, Beruf usw., sondern auch alle diejenigen Einzelangaben über die zur Person gehörenden Verhältnisse sachlicher Art, die wiederum der bestimmten Person zugeordnet werden können, also z.B. solche Daten wie Ort und Zeitpunkt des letzten Wocheneinkaufs, die, wenn auch nur indirekt, Rückschlüsse auf persönliche Verhältnisse zulassen würden.

Klassisch ist die Erhebung von Daten mit anschließender Speicherung durch automatisierte Verfahren, also ADV- oder EDV-gestützte Datenspeicherung und -verarbeitung. So entstehen durch das Sammeln personengebundener Daten Dateien<sup>99</sup> im Sinne des Gesetzes. Sie könnten automatisiert ausgelesen, ausgewertet, umorganisiert und nach neuen Kriterien neu geordnet werden. Jede Datei, die diese Voraussetzungen erfüllt, unterliegt wiederum den besonderen Bestimmungen des Datenschutzgesetzes.<sup>100</sup> Hierunter sind also auch die im schulischen Bereich geführten Dateien zu verstehen (s. Kap. 9.3).

## **9.2 Entwicklung und Struktur des Datenschutzgesetzes**

Datenschutz als einer der wesentlichen Bereiche des Schutzgutes der Persönlichkeit ist bereits seit vielen Jahren in der Diskussion. Nicht erst mit Schaffung der technischen Möglichkeiten zu Datenerhebung und Datenabgleich wurde über die daraus resultierenden technischen Möglichkeiten zum Missbrauch derartiger Daten diskutiert. Der Schutz der persönli-

---

<sup>99</sup> Zu den möglichen Formen der Speicherung – auch dateilose Speicherung – vgl. TETSCH / TEMME (1998), S. 309 sowie AUERNHAMMER, H.: Bundesdatenschutzgesetz - Kommentar; München 1993

<sup>100</sup> § 3 Abs. 5, 6 DSG NW sowie die Regelungen zu Datenverarbeitung, Verbunddateien u.ä. aus §§ 4 ff DSG NW

chen Rechte ist insbesondere in den USA bereits seit Mitte der 60er Jahre des letzten Jahrhunderts ein Thema.<sup>101</sup>

Auch in der Bundesrepublik entbrannte eine heftige öffentliche Diskussion um die Datenschutzproblematik, die mit dem Vorhaben zur Volkszählung, die im Jahre 1983 mit so genannten „klassischen“ Mitteln vorgesehen war, ihren Höhepunkt fand<sup>102</sup> und spätestens zu diesem Zeitpunkt auch in den Blickpunkt jedes einzelnen Bürgers gerückt wurde. Die Bedeutung der persönlichen Daten wurde schmerzlich deutlich, nicht nur denen, die bislang Befürchtungen hegten, die Bundesrepublik könne sich zu einem Überwachungsstaat mit Orwells „Big Brother“-Mentalität entwickeln, sondern auch denen, die erst jetzt eine wenn auch zuweilen noch nebulöse Vorstellung darüber erlangten, was sich überhaupt unter der Begrifflichkeit des „persönlichen Datums“ verbirgt.

Parallel zur Diskussion über den Datenschutz wurde die technische Entwicklung von Möglichkeiten zu Datenerhebung und Datenabgleich durch die stetige Fortentwicklung der IuK-Technologie vorangetrieben; beide – Datenschutz und Computertechnik – entwickeln sich gleichsam parallel weiter, wobei die Anforderungen der jeweils einen Seite notwendige Konsequenzen der jeweils anderen bedingten und nach wie vor bedingen. Die Interessen des Menschen werden dabei je nach Position des Betrachters mehr oder minder in das Zentrum gerückt. Sein Recht auf informationelle Selbstbestimmung (RiS), das als „quasi-Grundrecht“ garantieren soll, dass jeder Mensch über seine Daten selbst zu befinden habe<sup>103</sup> und nur

---

<sup>101</sup> S. hierzu KAMLAH: Right to Privacy; Das Allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen, Köln 1969

<sup>102</sup> SIMITIS, S.: Die Informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung; NJW 1984

<sup>103</sup> vgl. TETSCH / TEMME, S. 152: „...Vor dem Umgang staatlicher Sicherheitsbehörden mit personenbezogenen Daten (pbD) ist der einzelne grundrechtlich durch das Allgemeine Persönlichkeitsrecht des ART 2 Abs. 1 i.V.m. 1 Abs. 1 GG geschützt...“

unter engen rechtlichen Voraussetzungen (Gesetzesvorbehalt)<sup>104</sup> dieser Grundsatz durchbrochen werden darf (s. Kap. 9.1), ist bis heute nicht eindeutig formuliert. Es wird noch immer als Ergebnis des Volkszählungsurteils von 1983 sowie aus Art. 1 und 2 GG gesehen und fand bislang keinen Einzug in die Verfassung. Dennoch wird diesem RiS in jeder Minute und in jeder Lebenssituation Rechnung getragen, wenn über Daten von Personen entschieden wird.

Im föderalistischen System der Bundesrepublik ist auch der Datenschutz entsprechend organisiert. Das Bundesdatenschutzgesetz (BDSG) wird in den Ländern durch die jeweiligen Länderdatenschutzgesetze (DSG) konkretisiert; sie unterscheiden sich inhaltlich kaum. Vertreten werden die Interessen der Dateninhaber (also der Angehörigen der Gesellschaft) durch den Bundesbeauftragten für den Datenschutz, die jeweiligen Beauftragten in den Ländern und weitere Datenschutzbeauftragte in unterschiedlichen Ebenen (s.u.). Ihnen obliegt auch die Beobachtung der aktuellen Entwicklungen sowohl technischer als auch tatsächlicher Art, auf die sie durch jeweilig angemessene Maßnahmen, Erörterungen, Diskussionen auch eventuell über notwendige Gesetzesänderungen / -anpassungen zu reagieren haben.<sup>105</sup> So entstanden in der Vergangenheit die verschiedenen Veränderungen innerhalb des Bundesdatenschutzgesetzes auch auf Grund der Erforderlichkeiten, die die technische Weiterentwicklung gesetzt haben. Die bereits seit geraumer Zeit geführte Diskussion um die Struktur und Bedeutung des Internets kann innerhalb der durch die Datenschutzbeauftragten vertretenen Notwendigkeiten zu einem Wertewandel führen, der derzeit in seinen Auswirkungen noch nicht absehbar ist. Über die unterschiedlichen Auffassungen der Aufgaben von Datenschutzbeauftragten im Netz sei ver-

---

<sup>104</sup> vgl. TETSCH / TEMME, S. 154: „... Da der einzelne gegen informationelle Maßnahmen grundsätzlich geschützt ist, bedarf der Staat für Eingriffe in das Grundrecht einer verfassungsmäßigen gesetzlichen Grundlage, aus der bereichsspezifisch die Voraussetzungen und Grenzen klar erkennbar sind und die dem Grundsatz der Verhältnismäßigkeit entspricht...“

<sup>105</sup> §§ 4 f, g BDSG sowie BDSG, Zweiter Abschnitt, Dritter Unterabschnitt

wiesen auf die Darstellung von LUTTERBECK, in LfdD 1998. Er stellt heraus, dass die noch Mitte der 90er Jahre durch den damaligen Bundesbeauftragten für den Datenschutz vertretene Auffassung, das Internet sei eine Art Datenautobahn, für die man Verkehrsregeln aufstellen müsse, deren Einhaltung durch die jeweiligen Beauftragten zu überwachen sei.

Nach seiner (und der überwiegenden heutigen) Meinung aber ist auf „...die Eigenständigkeit des durch das Internet geschaffenen Raumes gegenüber der sonstigen, auch durch die Rechtsordnung gebildeten Welt...“ (S. 24, a.a.O.) abzustellen, es sei – so zitiert er den Supreme Court der USA – „...nicht vergleichbar mit den alten Medien – Briefpost, Buch, Presse, Telefon, und Fax, Foto, Film, tonträger, Funk und Fernsehen. Das Gericht lehnt es also ab, das Internet im Wege der Analogie zu bewerten und sagt damit, dass die alten Rechtsinstrumente für das neue Medium Internet überwiegend untauglich sind. Das Internet sei nichts anderes als freie Rede, die sich wie auf einem Marktplatz entfalten könne und müsse...“ (S 25, a.a.O). Diese Auffassung hat sich heute auch außerhalb der Gemeinde der User zunehmend durchgesetzt (im Gegensatz zu der noch 1996 von LUTTERBECK dargestellten Gegenmeinung) und führt zu einer veränderten Einstellung zur Umsetzung datenschützender Maßnahmen, die auch dem Wandel der Gesellschaft zur Informationsgesellschaft Genüge tun muss. Es geht darum, durch konzeptionelle, innovative Arbeit auch auf dem Gebiet der Rechtsentwicklung als Datenschutzbeauftragte mitzugestalten und damit dem Einzelnen, dessen Nutzen die Arbeit sein soll, Instrumentarien zum eigenen Schutz an die Hand zu geben. Gestaltet werden diese Instrumentarien von den Beauftragten, Richtschnur aber müssen Bedürfnisse der Nutzer (die permanent zu erheben sind) und technische Voraussetzungen sein.

Sowohl im Bund als auch in den Ländern ist diese gestaltende überwachende und regulierende Zuständigkeit für den Datenschutz den Innen-

ministerien bzw. Innensensoren übertragen worden, bei denen die jeweiligen Datenschutzbeauftragten organisatorisch angesiedelt sind.<sup>106</sup>

In allen Verwaltungsbehörden werden Datenschutzbeauftragte installiert, die in den durch Zuständigkeitsverordnung übertragenen Bereichen Vetorecht ausüben können und – um von etwaigen Beeinflussungen verschont zu sein – direkten Zugang zu den jeweiligen Behördenleitern haben. In Firmen und Betrieben werden Datenschutzbeauftragte eingesetzt, die sowohl den betrieblichen Datenschutz als auch den der Kunden sichern und gewährleisten sollen. Gerade im Medium Internet werden zunehmend Datenschutzfragen durch die dort vertretenen Firmen diskutiert. Jeder, der online Einkäufe tätigt, an Versteigerungen teilnimmt, Bank- oder Verwaltungsgeschäfte tätigt, wird mehr oder minder umfassend über derartige Regelungen informiert. Ein gutes Beispiel für verständliche, umfassende Information über Datenschutz findet sich in der Internet-Präsentation der Firma Intersport (s. Anlage 5); dort wird der Besucher über die Inhalte des Datenschutzes, den Schutzbereich und den Schutzzweck allgemeinverständlich informiert. Wie viele der Nutzer diese Seiten tatsächlich lesen, wie viele im Gegensatz dazu so, wie es vielfach üblich ist, einfach auf die Schaltfläche klicken zur Bestätigung, dass sie die Bestimmungen (ähnlich wie Allgemeine Geschäftsbedingungen, sog. AGBs) gelesen hätten, ist nicht bekannt. Zu wünschen ist aber, dass die Inhalte tatsächlich allgemein bekannt und geläufig sind.

Mit dem Zusammenschluss Europas entstand die Notwendigkeit, das jeweilige nationale Datenschutzrecht auch auf europäischer Ebene abzugleichen. Zusätzlich zu den Einigungsschwierigkeiten innerhalb des bun-

---

<sup>106</sup> Die Datenschutzbeauftragten des Bundes und der Länder sehen gerade in dieser organisatorischen Anbindung ein systemimmanentes Problem: durch die gleichzeitige Zuständigkeit für innere Sicherheit und Datenschutz wird die Gestaltung des Datenschutzes oft als von Strafverfolgungs- und Sicherheitsbehörden unzulässig beeinflusstes Ergebnis angesehen. Auf der anderen Seite fühlen sich Strafverfolgungsbehörden, zumindest deren Angehörige im operativen Dienst, oft durch die Bestimmungen des Datenschutzes unzulässig in der täglichen Arbeit eingengt.

des deutschen Föderalsystems sind nun auch weitere Kompromisse mit den anderen EU-Mitgliedsstaaten zu formulieren. Die um die betreffende Richtlinie 95 / 46 <sup>107</sup> entbrannte öffentliche Diskussion, die sich teilweise als ein bilateraler politischer Schlagabtausch mit lediglich parlamentarisch ausgelebter nationaler Aversion äußerten (z.B. die in den Medien dargestellte Diskussion zwischen Italien und Spanien), zeigte deutlich, welche unterschiedlichen Einschätzungen das allgemeine Persönlichkeitsrecht in den verschiedenen Mitgliedsstaaten erfährt.

Die Wechselwirkungen zwischen der EU-Richtlinie und den nationalen Bestimmungen war einerseits Problem für die Umsetzung innerhalb der Mitgliedsstaaten (da es zu einer Angleichung nationaler Bestimmungen und Gesetze im erforderlichen Maße kommen musste), andererseits auch Chance für Innovation und Anpassung an europäische und technische Gegebenheiten. Die Chance, den einzelnen User durch Information über technischen Selbstschutz in die Lage zu versetzen, seine Interessen selbst wahrzunehmen, scheint allerdings nicht ausreichend umgesetzt worden zu sein; die notwendigen Informationen und Bedingungen sind nicht wirklich transparent gemacht worden und nur einem interessierten kleinen Leserkreis, der sich aktiv um entsprechende Informationsbeschaffungen bemüht, zugänglich.

Ergebnis der europäischen Bemühungen ist die bereits erwähnte Richtlinie 95/46, die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Schutz des freien Datenverkehrs“<sup>108</sup>, die den Datenschutz innerhalb Europas, mögliche Datentransfers zwischen den Mitgliedsländern u.ä. regelt (Auszüge s. Anlage 6). Da-

---

<sup>107</sup> Die gesamte EU-Richtlinie wurde durch den Berliner Beauftragten für Datenschutz eingestellt ins Internet und ist abzurufen unter <http://www.datenschutz-berlin.de/infomat/heft24/dde.htm>

<sup>108</sup> Sie wird ergänzt durch die Richtlinie über die „Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation von 1997, vgl. hierzu Gerling: Nachholbedarf, EG-Richtlinien zum Datenschutz; in: C't 1999, Heft 6, S. 316

bei wird deutlich, dass hier versucht wurde, einerseits den Schutz der Persönlichkeit zu gewährleisten, andererseits auch den Austausch von Datenmaterial zu ermöglichen. Ohne derartigen Datenaustausch sind weder ungehinderter Handel (der Datenverkehr erfordert) zwischen den Mitgliedsstaaten möglich noch ungehinderte Reisen durch ein Europa ohne Grenzen. In Wechselwirkung stehen die Erfordernisse, z.B. bei Ausschreibungen in bestimmter Größenordnung europaweite Bewerbungen zuzulassen, die nicht ohne Datenverkehr auch sensibler Daten möglich wären. Ein in allen Lebensbereichen funktionierendes Europa kann es also nur mit geregelterm Datenschutz und Datenaustausch geben. Eine Neuerung gegenüber nationalem Recht hält die europäische Richtlinie dort bereit, wo sie den Zugriff auf Dateien zulässt, die nicht staatlicherseits geführt wurden, wo sie also die nationale strikte Trennung zwischen öffentlichen und privaten vorgehaltenen Datensammlungen aufhebt.

Auch die europäischen Regelungen sind keine Insellösungen, Europa wiederum ist eingebettet in internationale Gegebenheiten, Gesetze und Verordnungen. So hat die Richtlinie Regelungen vorgesehen, wie Datenaustauschmöglichkeiten mit außereuropäischen Ländern zu gestalten sind. Aktuelle Diskussionen erfolgen insbesondere nach den terroristischen Anschlägen im September 2001 und der Folgezeit. US-amerikanische Forderungen nach Datenerhebungen und Datenübertragungen, z.B. bzgl. Passagierlisten u.ä. (Airline Passenger Data Transfer) müssen mit nationalem und europäischen Datenschutzrecht abgeglichen werden und u.U. Auswirkungen auf Gesetzesänderungen haben; die Vermeidung politischer Verwicklungen aufgrund von rigiden gesetzlichen Einschränkungen ist Wegweiser und Ursache auch für nationale Schutzbestimmungen.

Ganz praktische, für jeden Bürger in bestimmten Lebenssituationen spürbare Auswirkungen finden die politischen Entscheidungen auf europäischer Ebene in den Regelungen des Schengener Abkommens und des darauf aufbauenden Schengener Durchführungs-Übereinkommens

(SDÜ)<sup>109</sup> und in der damit vorgenommenen Gestaltung des Schengener Informations Systems (SIS) sowie in den Datenarchivierungen innerhalb der Europol.<sup>110</sup>

Das SIS ermöglicht es, europaweit Fahndungs-, Sach- und Personendaten zu speichern und dem polizeilichen Zugriff zur Verfügung zu stellen. Allerdings ist die Nutzung des SIS als Datenpool an bestimmte Voraussetzungen geknüpft, eben auf Grund der gültigen Datenschutzbestimmungen der beteiligten Nationen und der EU-Richtlinie. Für den Bürger ist die Folge aus dem SIS spürbar dort, wo er innerhalb Europas grenzenlos reisen kann, andererseits aber auch grenzenlos recherchierbar ist, sofern eine Datenerhebung und Speicherung zulässig ist (so z.B. wenn er Halter eines hochwertigen Fahrzeuges ist, das entwendet wurde – seine Halterdaten werden europaweit im SIS gespeichert werden).

Europol ist eine Organisation, die in bestimmten Deliktsfeldern, die ihnen per Auftrag zugeschrieben werden, Daten aus den Datenpools der Mitgliedstaaten des Maastrichter Vertrages und dem SIS sammelt, eigene Daten erhebt, analysiert anschließend durch Datenauswertung zu Empfehlungen für die Kriminalitätsbekämpfung in den Mitgliedsländern gelangt. Auch wenn der Name darauf hindeutet, handelt es sich nicht um eine wirklich polizeiliche Institution, da ihr keinerlei Exekutivbefugnisse zustehen. Europol ist also rein strategische Planungsinstanz, die einerseits den Datenschutzbestimmungen der Mitgliedsländer, andererseits denen der EU unterliegt.

---

<sup>109</sup> STURM, J.: Das Schengener Durchführungsübereinkommen – SDÜ; Kriminalistik 1995, S. 162 ff

<sup>110</sup> STORBECK, J.: EUROPOL – Sachstand und Ausblick. Die Polizei 1993, S. 229 ff

### 9.3 Bedeutung des Datenschutzes in der Gesellschaft

Wie die beiden vorangegangenen Beispiele bereits zeigen, gibt es Datenschutzproblematiken im täglichen Leben, in jeder Minute des Tages. Nicht nur dann, wenn man von einem Land innereuropäisch oder außereuropäisch ins andere reist, auch schon dann, wenn man innerhalb seiner Stadt sich von A nach B bewegt, gibt es Datenerhebungen und Registrierungen, die den Datenschutzrichtlinien unterliegen. Einige Beispiele:

- Wer ein Einkaufszentrum, eine Bank, eine Tankstelle, ein Parkhaus, bestimmte Restaurants oder viele Geschäfte betritt, ist sich darüber im Klaren, dass er videoüberwacht wird. Während noch zu Beginn dieser Überwachungsmöglichkeiten ein Schild am Eingang auf das Vorhandensein der Kameras hinwies und der jeweilige Kunde dann durch das Betreten der Örtlichkeit sein Einverständnis durch konkludentes Handeln erklärte, gehört heute auch die Videoüberwachung ohne vorherigen Hinweis, z.B. in Banken, zum alltäglichen Leben und gilt als sozialüblich. Jeder ist sich darüber im Klaren, dass er hier beobachtet wird, dass die Aufnahmen bestimmte Zeit aufbewahrt und im Notfall als Beweismittel herbeigezogen werden können.
- Die bei den kommunalen Stellen vorgehaltenen Personaldaten sind problemlos durch Vernetzung innerhalb der Kommunalverwaltungen von einem Amt zum nächsten zu übertragen und – nach einmaliger Datenerhebung mehrfach nutzbar. Zusätzlich wird erwogen, die Daten auch unter den verschiedenen Kompetenzbereichen auszutauschen, um möglichen halblegalen oder illegalen Handlungen vorzubeugen. So wird z.B. diskutiert, ob die Möglichkeit besteht, zwischen verschiedenen Kommunen Daten zu transferieren. Es wird angestrebt, den Anmeldungen von Kraftfahrzeugen eine Abfrage beim Finanzamt vorzuschalten, ob der betreffende Halter bislang seinen steuerlichen Verpflichtungen

nachgekommen ist oder nicht und ggf. die Neuanmeldung eines Fahrzeuges erst nach Entrichten der Steuerschulden zu vollziehen. Ebenso wird die bislang unterbliebene Abfrage, ob ein potentieller Fahrzeughalter auch Sozialhilfeempfänger ist, diskutiert. Alle diese Maßnahmen würden zur einer Aufweichung des Datenschutzes und damit eventuell zu einer Kriminalisierung des betroffenen Bürgers führen, andererseits möglicherweise aber zu einer Teilsanierung der maroden Haushalte. Ob man nun für oder gegen entsprechende Verfahren ist, ist eher eine ideologisch-moralische Frage, die hier nicht abschließend diskutiert werden soll. Für den Bürger ist sie eine wesentliche, die weitreichende Konsequenzen für das Individuum haben kann.

- Datenschutz im Kundenverkehr ist ebenfalls eine Variante, die jedem Bürger bei jedem Rechtsgeschäft mehr oder weniger deutlich wird. Während bei Käufen mit schriftlichen Verträgen sowie bei Rechtsgeschäften im Internet die Übertragung von Daten allgemein bekannt ist, wird sie bei Direktzahlungskäufen eher weniger deutlich. Hier werden Personendaten erst dann konkret erhoben, wenn es zum Beispiel zu einem Umtausch mit Kostenrückstattung gekommen ist. Wozu dies von Bedeutung ist, können die wenigsten Verkäufer/Innen wirklich erklären. Auf die Frage, warum bei Auszahlung Daten erhoben werden, bei Einnahmen diese aber scheinbar unwichtig sind, finden sie zumeist keine Antwort. Eine Aufklärung der Bevölkerung hierüber hat ebenfalls nie stattgefunden.

- Bei jedem Arztbesuch wird der Großteil der Bevölkerung, noch bevor es auch nur zu einer Beratung kommen kann, nach der „Patientenkarte“ befragt. Während diese zur Zeit noch Informationen über die Krankenkasse, Versicherungsleistungen und Patientenkerndaten enthält, sehen die Planungen für zukünftige Verwendungen eine Vernetzung der Arztpraxen vor. Bei Einlesen der

Patientenkarte werden automatisch bisherige Daten abgerufen: Anamnese, Therapie und Medikation sind allen angeschlossenen Praxen verfügbar. Auf diese Weise werden zwar Kosten reduziert und Behandlungen können aufeinander aufbauen, da bei einem Arztwechsel nicht wieder bei Null begonnen werden muss, es wird dem Patienten aber auch die Möglichkeit genommen, unvoreingenommene Ärzte konsultieren zu können. Eine derartige Verwendung der Krankenkassenkarten käme den derzeitigen Bemühungen der Bundesregierung zur Kostenreduzierung im Gesundheitssektor zu Gute, würde aber Patientendatenschutz gefährden.

Nimmt man alle (und damit weit mehr als die hier exemplarisch aufgeführten) Möglichkeiten zusammen, Daten über Personen zu sammeln, so kann – bei einem Abgleich der verschiedenen Datenquellen - ein lückenloses Lebens- und Bewegungsbild einer Person entstehen. In den Brennpunkt des öffentlichen Interesses rücken derartige Fragen immer erst dann, wenn eine neue Überwachungsmöglichkeit hinzugekommen ist oder hinzukommen soll; so berichten die lokalen Fernseh- und Radiosender in jüngster Zeit:

- Die Busse des ÖPNV im Verkehrsverbund Rhein-Ruhr (VRR) werden seit einiger Zeit teilweise videoüberwacht, worauf man durch Schilder in den Bussen jeweils hingewiesen wird. Eine gründliche, eventuell kontroverse öffentliche Diskussion im Vorfeld dazu hat es nicht gegeben. Ziel soll sein der Schutz der Fahrgäste und Prävention gegen Sachbeschädigungen in den Fahrzeugen.
- Die Taxis der Stadt Remscheid sollen, nach einigen Raubüberfällen auf Taxifahrer, videoüberwacht werden. Die Betreiber erklären, dass dies sowohl dem Schutz der Fahrer als auch dem der Fahrgäste dienen soll; die meisten Fahrgäste haben keinerlei Probleme mit dieser Art der Überwachung. Dennoch meldet die

Landesbeauftragte für den Datenschutz erhebliche Bedenken an. Das mediale Interesse an der Diskussion wächst, eine Entscheidung gibt es noch nicht (Stand Juli 2003).

- Zum Vergleich mit diesen beiden Berichten wurde darüber berichtet, dass Parks in England videoüberwacht werden sollen ebenso wie die Stadtgebiete einiger weniger Innenstädte. Dazu ist es erforderlich mehr Überwachungspersonal einzustellen, das per Monitorüberwachung die sicherheitsrelevanten Bereiche beobachtet. Berichte darüber gibt es im deutschen Fernsehen, leichte Proteste unter der englischen Bevölkerung, die Maßnahme wird dennoch umgesetzt.

Eine völlig andere Datenschutz und Überwachungsmentalität findet sich teilweise im außereuropäischen Ausland. Während die Meldegesetze in den USA den Datentransfer von einem Bundesland in das andere kaum zulassen, der Umzug in ein anderes Bundesland häufig wegen fehlender Meldeverpflichtungen die Person unauffindbar verschwinden lässt, ist tägliche Überwachung in allen Lebenslagen in manchen Städten normal. Man denke nur an diejenigen Städte wie z.B. New York, in denen das Konzept der zero-tolerance (Ergebnis der broken-windows-theory<sup>111</sup>) verfolgt wird. Dies sind Städte, in denen auch im öffentlichen Raum jeder Schritt überwacht und aufgezeichnet wird. (Anm. d. Verf.: Kriminalität wirklich reduziert wurde damit wohl nicht, sie wurde lediglich qualitativ verändert bzw. zu Lasten angrenzender Behörden verdrängt.)

Die gesellschaftliche Bedeutung des Datenschutzes wird, wie diese Beispiele zeigen, bestimmt von politischen, gesellschaftlichen und technischen Rahmenbedingungen. Die allgemeinen Betrachtungen der Datenschutzproblematik gilt – wie bereits beschrieben – für alle Lebensbereiche.

---

<sup>111</sup> WILSON / KELLING (1992); s. hierzu KELLING, G.L. / COLES, C.M.: Fixing Broken Windows; Restoring Order and Reducing Crime in our Communities; Touchstone 1998, sowie WILSON, J.Q. / HERRNSTEIN, R.J.: Crime & Human Nature, The Definitive Study of the causes of Crime; Free Press 1998

Da Schule und Unterricht einen wesentlichen Teil des täglichen Lebens ausmachen, machen sie auch dort nicht Halt, vielmehr gibt es gerade im schulischen Bereich besondere Aspekte zu beachten.

## **9.4 Bedeutung des Datenschutzes in der Schule**

Die bisherigen Beispiele haben gezeigt, dass unter dem Begriff „sensible Daten“ erheblich mehr Angaben zu subsumieren sind, als der Bürger gemeinhin glaubt; darüber hinaus legen die Ergebnisse der Befragung in Schulen den Schluss nahe, dass auch dort Unklarheit zu diesen Fragen besteht (s. Kap. 7). Also nicht nur die harten Daten wie Namen, Vorname, Geburtsdatum und Anschrift gehören dazu, auch aus anderen Daten lassen sich, sobald Querbeziehungen zwischen verschiedenen Daten und vielleicht auch Datenquellen hergestellt werden, Informationen zur Person konstruieren. Betrachtet man die Bedeutung des Datenschutzes in Schulen, ist in mehreren Dimensionen zu prüfen, wie Datenschutz praktiziert werden sollte.

### **9.4.1 Schulinterner Datenschutz**

Schulen dürfen als Teil der Verwaltung die von ihnen benötigten Daten automatisiert zweckgebunden zur Erfüllung ihrer Aufgaben verarbeiten, sie unterliegen somit den Bestimmungen des Bundesdatenschutzgesetzes. In jeder Schule gibt es Dateien, in denen die Schülerdaten, wie z.B. Namen, Vornamen, Adressen, Telefonnummern registriert sind. Bei Abfragen von Daten derjenigen Personen, die im Schule / Schüler-Rechtsverhältnis eine Bedeutung haben (Erziehungsberechtigte, Pfleger, Kontaktpersonen wie Großeltern o.ä.), haben diese in der Regel ihre Erreichbarkeiten selbst angegeben, so dass von ihrem jeweiligen Einverständnis zur automatisierten Verarbeitung der Daten auszugehen ist. Fraglich ist, ob es bislang zu entsprechenden Rückfragen bei diesen Personen gekommen ist. Das würde bedeuten, dass bei jeder in einer Schule erstellten Adressenliste, in der

Personaldaten im weiteren Sinne aufgeführt werden, mit den Betroffenen Rücksprache zu halten ist. Und diese Rücksprache ist durch die Schule zu halten, denn sie ist diejenige Stelle, die für die ordnungsgemäße Erhebung, Speicherung und Verarbeitung der Daten zuständig und verantwortlich ist (s. Kap. 9.1, § 3 BDSG sowie § 3 Abs. 3 DSG NW). Die Schule kann sich also nicht darauf verlassen, dass die Großeltern eines Schülers / einer Schülerin damit einverstanden sind, dass ihre Erreichbarkeit in der Schule hinterlegt wird. Sie muss vielmehr dort nachfragen und das Einverständnis einholen. Ob dies bislang wirklich so geschehen ist, erscheint fraglich. Es liegt eher die Vermutung nahe, dass bisher das jeweilige Einverständnis entgegen der gesetzlichen Anforderungen stillschweigend vorausgesetzt wurde,

Diese und alle anderen in den Schulen vorgehaltenen „Verwaltungsdaten“ dürfen nicht anders als zu administrativen Aufgaben verwendet werden oder weitergegeben werden. Die Speichermedien, auf denen sie abgelegt sind, dürfen nicht zur Speicherung anderer Daten verwendet werden<sup>112</sup>. Das heißt jedoch nicht, dass auch dieser Rechner nicht auch für andere Anwendungen genutzt werden darf.

Es kann außerdem davon ausgegangen werden, dass eine Vielzahl von Lehrern auch auf einem privaten PC über Daten verfügt und dort Notenlisten, Schülerdaten etc. bearbeitet und verwaltet. Damit werden teil-administrative Aufgaben aus dem schulischen Bereich nach Hause verlagert. Es ist fraglich, ob diese „Lehrer-PC“ tatsächlich nur für dienstliche und schulische Datenverarbeitung genutzt werden. Vielmehr kann davon ausgegangen werden, dass dieselben PC auch über Internet-Zugänge verfügen, eventuell von der gesamten Familie genutzt werden usw. Die sensiblen Daten sind also sowohl von Familienmitgliedern des Lehrers als auch durch Zugriffe aus dem Netz heraus einsehbar und manipulierbar, sofern

---

<sup>112</sup> Konsequenz aus § 4 Abs. 6 DSG NW; zu weiteren Maßnahmen technischer und organisatorischer Art vgl. Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000, Teil 2-3

nicht ausschließende Softwarelösungen gefunden und installiert sind (s. hierzu Kap. 10). Hier werden automatisierte Datenverarbeitungswege genutzt, die dem Datenschutzgesetz unterliegen müssten, aufgrund der privaten Gestaltung aber außerhalb jedes Kontrollbereiches liegen. Erst, wenn es zu Datenmissbräuchen gekommen ist, werden derartige Gesetzesmissachtungen bekannt und straf- und / oder disziplinarrechtlich verfolgt.

Aber nicht nur Schüler, auch Lehrerdatenschutz ist Bestandteil schulischen Datenschutzes. Eine Datei, die Aufschluss gibt über die persönlichen Daten, aber auch über die durch den einzelnen Lehrer erteilten Unterrichtsstunden, über seine Krankheitstage und Ausfallzeiten, über die von ihm gestellten Klassenarbeiten und deren jeweilige Ergebnisse u.ä., unterliegt denselben Kriterien. Sie kann – vergleicht man sie mit den Datenmaterialien anderer, evtl. außerhalb der Schule geführter Dateien - Aufschluss über Arbeitsmoral, Schüler-Lehrer-Verhältnis und –Interaktion und nicht zuletzt über die persönlichen Verhältnisse geben.

#### **9.4.2 Schulischer Datenschutz und Vernetzung**

Die Initiative des Landes, alle Schulen ans Netz zu bringen, greift immer tiefer. Zunehmend sind auch Schulen nicht nur, wie in Kap. 6 beschrieben, mit einem einzigen Stand-alone-Rechner als Zugang in das Internet ausgestattet, zunehmend werden auch interne Vernetzungen und schulische Intranets angestrebt und die Schule durch eine eigene Homepage vertreten. Damit gewinnt der Datenschutz außerhalb der bereits beschriebenen Bereiche zunehmend Bedeutung. Es entsteht ein neues Spannungsfeld zwischen den Interessen der Schule, die sich auf ihrer Site so positiv und werbewirksam wie möglich darstellen will, andererseits aber auch die Rechte der Einzelnen berücksichtigen und entsprechend handeln muss.

Im Zusammenhang mit der Betrachtung, was schulischen Datenschutz im Netz (Internet wie Intranet) ausmacht, steht zuvorderst also die Frage, wie dieses Spannungsfeld aufgelöst und auch in einer ansprechenden Internet-Präsentation den Belangen des Datenschutzes genüge getan werden kann. Jedes ins Netz eingestellte Datum „gehört“ irgendjemandem. Es ist also auch in allen Fällen das Einverständnis des jeweiligen Dateninhabers einzuholen, und es sei an dieser Stelle erneut darauf hingewiesen, dass das **alle** Formen von Daten betrifft, auch Bilder, Videomitschnitte, selbst Stimmtaufzeichnungen.<sup>113</sup> Derartige Einverständniserklärungen sind an Vorgaben gebunden, die ihre Rechtswirksamkeit bedingen: Eine Einwilligung muss vom Betroffenen in Kenntnis aller Umstände der Veröffentlichung und der Dateninhalte freiwillig gegeben worden sein, sie ist für jedes Datum einzuholen, schriftlich zu fixieren und kann jederzeit widerrufen werden.<sup>114</sup> Die Kenntnis aller Umstände aber wiederum setzt voraus, dass insbesondere der Verfügende sich über die Sensibilität des Datums, über den Informationsgehalt und die Konsequenzen bewusst ist; hier wiederum ist insbesondere für Schüler ein erhebliches Informationsbedürfnis vorhanden. Die Implementierung derartiger neuer Unterrichtsinhalte ist daher dringend geboten.

Das hat zur Konsequenz, dass die Präsentation einer Schule permanenter Thematisierung im Unterricht und mit dieser einhergehend ständige technische Betreuung und Überarbeitung durch den webmaster bedarf und nicht „nebenbei“ von einem der Lehrer oder Schüler erledigt werden kann. Jedes wirklich zur Veröffentlichung geeignete und interessante Ereignis ist mit Schüler- oder Lehrerdaten verknüpft; die jeweilige Veröffentlichung von Texten oder Bildern, sofern Personen abgebildet oder Rückschlüsse auf sie möglich sind, verlangt also nach dem schriftlichen Einverständnis der Be-

---

<sup>113</sup> Auch wenn es nicht eine direkte Zuordnungsmöglichkeit zu konkreten Personen gibt, so ist durch besondere Methoden z.B. auch die Zuordnung einer Stimme durchaus möglich; verwiesen sei hier auf die in der Öffentlichkeit bekanntgewordenen Fälle der Identifikation von Straftätern insbesondere in Erpressungsfällen über Tonbandmitschnitte, z.B. Dagobert-Fall.

<sup>114</sup> § 4 DSG NW

troffenen. Die Veröffentlichung von Fotos aus dem Unterrichtsgeschehen kann auf diese Weise im ungünstigsten Fall das Einholen von mehr als 20 Einverständniserklärungen, bei nicht voll geschäftsfähigen Schülern noch zusätzlich die der Erziehungsberechtigten, erforderlich machen. Der Verwaltungsaufwand zur Darstellung einer Schule im Internet mit aussagekräftigen Texten und Bildern ist also weit größer als bei oberflächlicher Rechtsbetrachtung zu vermuten wäre.

Eine diesen rechtlichen Anforderungen entsprechende Vorgehensweise ist bisher in vielen Schulen eher lasch und ohne wirkliche Sachkenntnis getragen gehandhabt worden, wie sporadische und mehr zufällige Rückfragen bei Lehrkräften gezeigt haben.

Die bisherigen Aussagen beziehen sich ausschließlich auf die Erhebung, Speicherung, Darstellung von Daten und das Bemühen, das Recht des Einzelnen zu schützen. Darüber hinaus aber hat die Schule (ebenso wie jede andere Institution, jedes Unternehmen) Sorge dafür zu tragen, dass es keine unberechtigten Datenzugriffe bzw. Datenveränderungen gibt. Die Darstellung / Speicherung der Daten sind rechtmäßig nach den Maßgaben des Datenschutzes, unautorisierte Zugriffe, ungewollte Datenverluste oder –veränderungen und andere Manipulationen sind im Rahmen eines geeigneten Datensicherheitskonzeptes zu verhindern.

## 10 Datensicherheit

Datensicherung als eine Umsetzung von Datensicherheitsbemühungen steht im engen Zusammenhang mit Datenschutz. Die oberflächliche Auslegung der Begriffsunterschiede legt als Interpretation nahe, Datenschutz sei die rechtliche Komponente, Datensicherheit bzw. Datensicherung die technische Umsetzung derselben. Dieser Interpretation wurde in den letzten Jahren geraume Zeit gefolgt. Mittlerweile ist die Betrachtung jedoch durch die ständige Weiterentwicklung der Rechtsposition und der technischen Gegebenheiten differenzierter geworden.<sup>115</sup>

Die Datensicherung soll mehreren Zielen gleichzeitig dienen und unterschiedliche Angriffsmöglichkeiten gleichermaßen abwehren: Sie schützt den Bestand von Daten ebenso wie den der Datenträger, Programme, Hardware vor jeglichem manipulativen Zugriff, also sowohl vor unberechtigter Einsichtnahme als auch vor Beschädigung oder Zerstörung, Kopie, Verlust usw. Hier aber kann Datensicherung nur einen Teilaspekt aufgreifen; zwar werden durch regelmäßige Sicherung der Totalverlust oder eine Beschädigung in den Konsequenzen aufgefangen, eine unberechtigte Einsichtnahme kann sie jedoch nicht verhindern.

Es bietet sich daher für die weitere Darstellung an, eine Einteilung vorzunehmen, die Kern- und Spezialbereiche betrachtet:

---

<sup>115</sup> Vgl. hierzu TETSCH / TEMME (1998), S. 172:  
*„... Der Begriff der Datensicherung hat zwei Bedeutungsinhalte. Zunächst lag der Hauptzweck in der Erreichung von Datensicherheit i.S. Schutz vor Verlust oder Beschädigung gespeicherter Daten. Dieser technisch orientierte Inhalt blieb bis heute auch so erhalten. Daneben trat aber der rechtliche Inhalt, der sich auf Fragen des sicheren, i.S. eines gesetzmäßigen Umganges mit den Daten konzentriert...“*

## 10.1 Kernbereiche der Datensicherheitsproblematik

TRAEGER <sup>116</sup> nimmt eine Einteilung in vier Kategorien vor:

*Folgende Formen der Sicherheit lassen sich im Bereich der EDV abgrenzen:*

1. *Datensicherheit* (Anm.d.Verf.: im engeren Sinne)
2. *Zugriffssicherheit*
3. *Authentikation*
4. *Vertraulichkeit*

Diese Einteilung fokussiert den Bereich der Datensicherheit im weiteren Sinne auf das Objekt, also die Daten an sich. Im weiteren Verlauf stellt TRAEGER technische Möglichkeiten vor, die von ihm formulierten vier Sicherheitsformen zu erreichen. So soll Datensicherheit durch die Realisierung eines Datensicherungskonzeptes, etwa durch ständige Sicherungen, backup-Systeme o.ä. erzielt werden. Auf diese Weise wird allerdings wieder lediglich die Ausfallsicherheit garantiert; im Falle eines Datenverlustes oder einer Datenmanipulation können die ursprünglichen Daten durch die redundante Speicherung wiederhergestellt werden. Dies ist ein Verfahren, das jeder PC-Nutzer kennt; kaum jemand, der nicht schon durch einen Absturz des Systems Daten verloren hat, von denen keine Sicherungskopie gefertigt wurde. Sicherungskopien reduzieren aber wiederum lediglich die Folgen einer Störung, sie verhindern nicht die Störung selbst. Ein Systemausfall kann nur durch Redundanz verhindert werden, was aber das System erheblich verteuert und wartungsintensiver macht.

Die durch TRAEGER als zweiter Bereich genannte Zugriffssicherheit kann über das Sperren und Setzen von Berechtigungen und die nähere Definition ihres jeweiligen Umfangs erreicht werden. Damit können Zugriffe verhindert oder erlaubt werden; darüber hinaus sind erfolgte Zugriffe zu

---

<sup>116</sup> TRAEGER (2001), S. 459 ff

protokollieren (was der retrospektiven Erfassung entspricht, s. hierzu Kap. 8).

Hier sind die Unterschiede in den Betriebssystemen<sup>117</sup> zu beachten, bereits VOR einer Entscheidung für das eine oder andere System ist also das Augenmerk darauf zu richten, welche Berechtigungsvarianten man haben möchte.

Unter Authentikation versteht TRAEGER die „*Echtheit der Identität*“ (S. 461). Identität im Zusammenhang mit Daten ist jedoch nicht nur zu beziehen auf Mail-Absender, IP-Adressen oder ähnliche „Absenderdaten“. Eine weitere Betrachtung sollte erfolgen hinsichtlich der Echtheit der Identität derjenigen Personen, die das Datenmaterial nutzen, bearbeiten, versenden usw. Wenn Mitarbeiter ihre Logins an andere weitergeben, ist die Identität des Sachbearbeiters nicht mehr zu kontrollieren. Nicht nur technische Konsequenzen sind hier also zu beachten, auch die Personalseite muss in die Überlegungen einbezogen werden.

Der letzte durch TRAEGER definierte Bereich soll analog zur Vertraulichkeit des gesprochenen Wortes die Vertraulichkeit der Kommunikation unter Nutzung der luK garantieren. Vertraulichkeit von Kommunikation, bei der die Dialogpartner räumlich entfernt voneinander sind, kann jedoch wiederum nicht nur durch technische Abwehrmechanismen erreicht werden. Sie bilden natürlich einen wesentlichen Teilbereich der erforderlichen Maßnahmen, sind aber alleine nicht umfassend genug.

Auch hier wird also die Sicherheit von Daten in zwar nicht unwesentliche Bereiche gegliedert und jeder Bereich einer Lösung zugeführt, ein Gesamt-Sicherheitspaket wird aber noch nicht geschnürt.

---

<sup>117</sup> Während bei Windows NT Zugriffserlaubnisse gesetzt werden müssen, da zunächst die Daten gesperrt sind, sind andere Systeme grundsätzlich offen und müssen gezielt für Zugriffe gesperrt werden. Der jeweilige Aufwand ist – bezogen auf den Sicherheitserfolg – gänzlich unterschiedlich, die erforderlichen Kenntnisse ebenso.

Eine solche Betrachtung nur von Teilbereichen des Themenkomplexes ist eines der wesentlichen Kennzeichen der Diskussion über Datensicherheit auch in der Literatur. Viele Publikationen<sup>118</sup> beziehen sich zwar auf die Gefahren, die sich aus dem Internet und seiner Nutzung ergeben; Gefahren, die aus dem eigenen Herrschaftsbereich resultieren, also z.B. durch eigenes Personal hervorgerufene Datenveränderungen, -zugriffe oder – Manipulationen jeglicher Art, werden häufig außerhalb des Betrachtungshorizontes gelassen, da es nicht zu der erforderlichen Vernetzung unterschiedlicher Ansprüche und Denkansätze kommt und eine Betrachtung von Wechselwirkungen auf Grund der Komplexität in der Regel ausbleibt. Ebenso wenig werden alltägliche, banale Möglichkeiten unberechtigter Datenzugriffe außer Acht gelassen, so z.B. wird nur selten darüber nachgedacht, ob Monitore auch für Unberechtigte einsehbar sind und damit ein Ausspionieren von Daten möglich wird.

Dabei sind gerade solche Gefahren diejenigen, die – zusätzlich zu den die gesamte PC-Welt betreffenden Viren, Würmern, Trojanern u.ä. – die Sicherheit von privaten und öffentlichen Netzen ebenso nachhaltig beeinträchtigen können. Ihnen also gilt es mindestens gleich hohe Aufmerksamkeit zu schenken. Darüber hinaus kann – wie bereits erörtert wurde – Datensicherheit nicht isoliert betrachtet werden; sie muss immer mit den Anforderungen des Datenschutzes in Einklang gebracht werden.<sup>119</sup>

---

<sup>118</sup> So A CAMPO, M.: PC-Sicherheit. Bonn 2001-2002; JANOWICZ, K.: Sicherheit im Internet. O'Reillys Internet-Bibliothek, Köln 2002 u.a., anders BERNSTEIN, H. (2001), der im Gegensatz dazu auch die Sicherheit von Einzelplatzsystemen u.ä. betrachtet.

<sup>119</sup> Eine detaillierte Darstellung der technischen Möglichkeiten einschließlich dezidierter Umsetzungsvorschläge finden sich bei BERNSTEIN, H. (2001). Dort werden sowohl Schutzkonzepte für PC-Arbeitsplätze als auch die Vorgehensweise für Risikoanalysen dargestellt, deren Anwendbarkeit auch für den schulischen Bereich gegeben ist. Für die private Anwendung empfiehlt sich A CAMPO, M.: PC Sicherheit; Bonn 2001-2002

Eine weit ausgedehntere Erörterung der Problematik findet sich in dem sehr umfassenden und umfangreichen<sup>120</sup> IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es betrachtet alle sicherheitsrelevanten Bereiche von IT-Systemen und bezieht auch die vordergründig nicht betroffenen Felder wie Peripheriegeräte, Telefonanlagen, bauliche Strukturen, Personalfragen und so weiter mit ein:

*„...Das vorliegende IT-Grundschutzhandbuch enthält Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche IT-Konfigurationen, die typischerweise im heutigen IT-Einsatz anzutreffen sind...“<sup>121</sup>*

Aus den im Grundschutzhandbuch aufgeführten wesentlichen Bereichen sollen hier nur einige wenige exemplarisch dargestellt werden, die für die konkreten Betrachtungen innerhalb schulischer Datensicherheit von besonderer Bedeutung erscheinen (Kap. 10.3). Die darüber hinaus im Handbuch unter Kapitel 1.4 zu findenden Inhalte werden als Anlage 7 beigefügt. Dabei handelt es sich um 47 (!) Betrachtungsfelder<sup>122</sup>, deren isolierte Darstellung allerdings nicht möglich erscheint; jede Entscheidung und Veränderung in einem der Felder hat Konsequenzen in anderen Bereichen, muss also jeweils auch dort betrachtet und im Bezug auf die Entstehung von jeweiligen Wechselwirkungen und Spannungsfeldern entschieden werden.

---

<sup>120</sup> Das Gesamtwerk ist mehr als 1700 Seiten stark!

<sup>121</sup> Aus: BSI: IT Grundschutzhandbuch, Stand Oktober 2000, Seite 2

<sup>122</sup> Hingewiesen sei darauf, dass auch auf unterschiedliche Betriebssysteme auch verschiedener Hersteller eingegangen wird, wobei es sich in erster Linie um netztaugliche Systeme handelt. Die Befragung der Schulen hat ergeben, dass nicht immer Klarheit über die Netztauglichkeit unterschiedlicher Betriebssysteme zu bestehen scheint; die Frage „Mit welchem Betriebssystem arbeiten Sie im Netz?“ (Frage3) erbrachte teilweise Antworten, die widersprüchlich erschienen. Vgl. hierzu Auswertung Frage 3, Kap. 6.3.

### 10.1.1 IT-Sicherheitsmanagement

Ein geeignetes IT-Sicherheitsmanagement kann, da es Steuerungs- und Lenkungsfunction im weiteren Aufbau eines sicheren Systems haben soll, notwendigerweise nur am Anfang einer jeglichen technischen Umsetzung stehen. Im BSI-Grundschutzhandbuch<sup>123</sup> werden die erforderlichen Schritte in diesem Zusammenhang ebenso deutlich und checklistenartig dargelegt wie die erforderlichen Ressourcen jeglicher Art. Das indiziert auch, dass es keine realisierbare IT-Sicherheit gibt ohne den Einsatz von Ressourcen, ohne Man-Power. Vergleicht man dieses Erfordernis mit den Ergebnissen der Umfrage, so stellt sich das Problem, dass bislang in nordrhein-westfälischen Schulen offenkundig auf die Freiwilligkeit der Lehrer und Lehrerinnen, ja sogar ihrer Verwandten gesetzt wird, um in den Schulen entsprechende Sicherheitsprozesse zu erwirken.<sup>124</sup> Gerade die Bedeutung von Datenschutz und Datensicherheit im gesamten IT-Bereich macht aber genau diese Vorgehensweise zu einer fragwürdigen Gestaltung des Prozesses; der hier enthaltenen Bedeutung wird man nicht dadurch gerecht, dass Sicherheit quasi dem Zufall und dem Engagement einzelner zur zusätzlichen Arbeit überlassen bleibt. Vielmehr muss die enorme Wichtigkeit dadurch unterstrichen werden, dass Personal und Mittel zur Verfügung gestellt werden, die den Prozess vorbereiten, initiieren und steuern.

### 10.1.2 Organisation

Das Sicherheitsmanagement kann nur dann zielgerichtet und erfolgreich sein, wenn die Zuständigkeiten für die Konzeptumsetzung eindeutig festgelegt und verteilt werden. Sowohl zeitliche Abläufe als auch personelle Besetzung, sowohl grundlegende Entscheidungen über die Rolle und Aufgabe der Administratoren und der einzelnen User, sowohl der Umgang mit

---

<sup>123</sup> Darüber hinaus s. ERTL, A. W.: Das globale Dorf. München 1996

<sup>124</sup> s. hierzu Ergebnisse der Fragen 10 und 11 sowie Freitexte zu Frage 12

der Hardware als auch zulässiger bzw. unzulässiger Softwareeinsatz müssen geregelt und organisiert werden. So ist z.B. von Anfang an festzuschreiben, wer für das Installieren neuer Anwendungen zuständig ist, um einen „Wildwuchs“ von unterschiedlichen Softwareausstattungen der Clients zu verhindern. Das wiederum setzt voraus, dass bereits zu Beginn des Prozesses die Bedarfe umfassend erhoben und Abläufe abgebildet wurden, die mit der Umsetzung des Konzeptes optimiert zu organisieren sind.

### 10.1.3 Personal

Vordergründig und ganz zu Beginn ist über die Zuständigkeit der Projektbeteiligten zu entscheiden, die – unter Beachtung der in 10.1.1 bereits ausgeführten Grundsätze der Anbindung des Prozesses an eine möglichst hohe Kompetenz- und Entscheidungsebene hinaus – das Sicherheitsmanagement initialisieren<sup>125</sup>, umsetzen, begleiten und regelmäßig evaluieren. Im Detail aber geht die Bedeutung von Personalfragen innerhalb des Projektes darüber weit hinaus: Datensicherheit ist in höchstem Masse abhängig vom Verhalten derjenigen, die sich in dem betreffenden IT-System bewegen. Mitarbeiter müssen so geschult sein, dass sie die ihnen durch den PC zur Verfügung gestellten Möglichkeiten auch nutzen können<sup>126</sup> und sich tatsächlich an die erarbeiteten Regularien halten, sich nicht aus unter-

---

<sup>125</sup> Zu den Anforderungsprofilen geeigneten Personals wie zur Besetzung entsprechender Funktionen und deren Aufgabenzuschnitt s. GESELLSCHAFT FÜR INFORMATIK (GI): Empfehlungen zur Planung und Betreuung von Rechnersystemen an Schulen; Beilage zu LOG IN 21 (2001) Heft 1

<sup>126</sup> s. hierzu LARISCH, D. (2000), S. 27:

*Der typische Netz-PC-Benutzer ist ein Anwender, der innerhalb eines Firmennetzes mit Windows arbeitet und sich beispielsweise ausschließlich mit Texterfassung beschäftigt. Für solche Benutzer ist die Flexibilität eines konventionellen PCs geradezu übertrieben, in der jeder nur erdenkliche Anspruch befriedigt werden muss (Anm. d. Verf.: wodurch wiederum durch mangelnde Kenntnisse des Users neue Gefahrensituation geschaffen werden). Die sogenannten Power-User mit speicherintensiven Grafikanwendungen werden diese mit Sicherheit nicht auf einem NC oder Net-PC einsetzen, sondern auch weiterhin den sogenannten Fat-Client dem Thin-Client vorziehen.*

schiedlichen Gründen darüber hinwegsetzen. Ein Mitarbeiter, der sich aus Bequemlichkeit nicht an die Vertretungsregelungen hält, einem anderen „der Einfachheit halber“ das eigene Login überlässt, eigene (womöglich noch von zu Hause mitgebrachte, nicht gescannte) Software installiert, durch Unkenntnis wegen mangelnder Schulung das System sperrt, konterkariert das Sicherheitsmanagement damit nicht nur in Teilbereichen. Dem ist durch geeignete Maßnahmen vorzubeugen: Schulung der Mitarbeiter, regelmäßige Hinweise auf Sicherheitsstandards, Verfahrensweisen in Abwesenheits-, Vertretungsfällen u.ä.

#### **10.1.4 Datensicherungskonzept**

Innerhalb der eng überschaubaren schulischen Bereiche kann Datensicherung auf relativ einfache Weise durch Wechselfestplatten oder Sicherungskopien erreicht werden, die jeweils auf externen Datenträgern erfolgen kann, die sicher aufzubewahren sind. Je komplexer die IT-Strukturen, je größer der Vernetzungsgrad, je umfangreicher das Gesamtsystem und der Datenbestand, desto größer ist der Bedarf an fundierter Datensicherung. Wird also ein Vernetzungskonzept umgesetzt, wie es in Kap. 11 ansatzweise dargestellt wird, ist diesem Bereich bereits von Beginn an wesentliche Aufmerksamkeit zu widmen.

#### **10.1.5 Bauliche Maßnahmen, Ausstattung**

Datensicherung und Datenverarbeitung sind so zu gestalten, dass sie unberechtigtem Zugriff entzogen werden. So sind bauliche Veränderungen u.U. dort erforderlich, wo Räume offenem, unkontrolliertem Zugang unterliegen, eine reine physikalische Trennung von Netzen genügt hier nicht. Es kann Abhilfe geschaffen werden durch Türen, Schließanlagen, geeignete Großschränke für die Aufnahme von Datenträgern und ähnliches. Zu berücksichtigen sind weiterhin die Erfordernisse, die für einen störungsfreien

Betrieb sorgen, so z.B. eine Unterbrechungsfreie Stromversorgung (USV), Klimatisierung von Räumen mit hoher Wärmebelastung wie Serverräumen, aber auch diejenigen Erfordernisse, die im Notfall zur Schadensbegrenzung genutzt werden können, wie z.B. Feuerlöscher o.ä.

#### **10.1.6 Computer-Virenschutzkonzept, Firewall, E-Mail-Verkehr**

Viren können sowohl aus dem Internet in das eigene Netz gelangen als auch durch Nutzung verseuchter Datenträger innerhalb des eigenen Systems. Geeignete Maßnahmen hierzu setzen wiederum in unterschiedlichen Bereichen an. Nur ein funktionierendes, ineinander greifendes Konzept ist in der Lage, alle Felder abzudecken. Ein gutes Virenprogramm<sup>127</sup>, das aus E-Mails verseuchte Anhänge filtert und isoliert, eine Firewall, die – manuell oder konfiguriert – Zugriffe unterbindet und eine gute Mitarbeiter-schulung und Information über Gefahren und Abwehrmechanismen müssen gleichzeitig eingesetzt werden. Eine entsprechende Konzipierung der Vernetzung einschließlich aller ihrer Bestandteile (z.B. zugehörige Software pp.) ist also bereits frühzeitig in das Management einzubeziehen. Auch die Zusammenfassung von Teilnetzen innerhalb eines Gesamt-Intranets und dessen Öffnung ins Internet wird erst so sicher möglich. Anzahl von Schnittstellen, Gefährdungsgrade u.ä. sind dabei – je Rechnerstation – einzeln zu betrachten.<sup>128</sup>

---

<sup>127</sup> Zu den Arbeits- und Wirkungsweisen unterschiedlicher Attacken aus dem Internet, von Viren, Würmern oder Trojanern, vgl. A CAMPO, 2001-2002, S. 91 ff sowie ECKERT, C.: IT-Sicherheit; Konzept – Verfahren - Protokolle. Oldenbourg 2001, Kap. 2

<sup>128</sup> So ist z.B. vorzusehen, die Schulverwaltungsdaten strikt vom Internet zu trennen; hier erscheint lediglich eine physikalische Trennung zielführend. Das aber hat zur Konsequenz, dass Rechner, die zur Verarbeitung von Schüler- und Lehrerdaten genutzt werden, KEINEN Internet-Zugang erhalten dürfen.

### 10.1.7 Häuslicher Arbeitsplatz, Tragbarer PC

Häusliche Arbeitsplätze gehören zwar in Schulen im eigentlichen Sinne des Begriffes nicht zur Regel; die in den meisten Lehrerhaushalten stehenden privaten PCs können allerdings als häusliche Arbeitsplätze betrachtet werden. Sie werden auch für Unterrichtsvorbereitung und -nachbereitung, für die Korrektur von Arbeiten, die Verwaltung von Notenlisten (daher mit hochsensiblen Daten belegt) u.ä. genutzt und sind daher in das Sicherheitskonzept einzubeziehen. Es ist also zwingend darauf zu achten, dass auch solche privat genutzten PCs ebenso wie Laptops in geeigneter Weise geschützt und gesichert werden. Der durch die ganze Familie genutzte PC, der gleichzeitig zur Verwaltung von Schülerdaten (im weitesten Sinne, s. Kap. 9) genutzt wird, entspricht nicht einem geeigneten Sicherheitsmanagement; ebenso wenig der dienstlich genutzte Laptop, der weder durch geeignete Maßnahmen gegen Diebstahl noch durch Verschlüsselung, Kennworte o.ä. vor unberechtigten Zugriffen auf den Datenbestand geschützt ist.<sup>129</sup> Private und dienstliche Nutzung ein und desselben Gerätes sind zwar möglich, unterliegen aber besonders weitreichenden Anforderungen, die formuliert, dargestellt und den betroffenen Usern verdeutlicht werden müssen.

---

<sup>129</sup> S. hierzu ECKERT, C.: Zur Sicherheit mobiler persönlicher Endgeräte – eine Bestandsaufnahme; in: HORSTER (2001), S. 204 – 217; ECKERT weitet noch aus auf die Einbindung von Geräten wie PDAs (Personal Digital Assistant), Organizer oder auch Handys, die ebenfalls in eine umfassende Betrachtung mit einbezogen werden müssen. Ihr Nutzung dürfte zukünftig mit den Möglichkeiten des UMTS noch zunehmen, eine zukunftsorientierte Betrachtung der Sicherheitsproblematik kann sie also nicht außer Acht lassen. Gefahren, die sich gerade daraus ergeben, dass derartige Endgeräte physisch die Firewall umgehen und durch direktes Andocken im Netz zu weiteren Risiken führen schildert PINS DORF, U.: in: HORSTER (2001), S. 218 -226: David gegen Goliath; Palmtops als Bedrohung für Firewalls

### 10.1.8 Behandlung von Sicherheitsvorfällen

Auch das beste Konzept kann nicht verhindern, dass es zuweilen dennoch zu einem Ausfall, einem Schaden, einem Sicherheitsvorfall kommt. Dieses Szenario darf in der Entwicklung des Konzeptes nicht außer Acht gelassen werden; vielmehr muss bereits im Vorfeld versucht werden, jede mögliche Schadenskonstellation zu antizipieren und jeweils entsprechende Reaktionsmöglichkeiten und –mechanismen vorzusehen, zu beschreiben und einzuüben. Eine u.U. erforderliche Wiederherstellung des Gesamtsystems wird – sofern es gelingt, entsprechende Mechanismen vorzuhalten – dann zügig vonstatten gehen, die Verfügbarkeit der Funktionalitäten wird in kurzer Zeit wieder gewährleistet sein.

Keines der genannten Elemente kann für sich genommen und isoliert betrachtet werden, es bestehen Korrelationen zwischen den Bereichen und eine enge Verzahnung der Elemente, die nur bei gleichzeitiger Untersuchung der Wechselwirkungen zu einem optimalen Sicherheitserfolg führen wird. So sind z.B. die externen Datenträger (s. 10.1.4) so aufzubewahren, dass sie fremdem Zugriff entzogen werden. Mitarbeiter müssen also über das Erfordernis aufgeklärt werden, diese Datenträger unter Verschluss zu halten (Wechselwirkung zu 10.1.3). Dann müssen wiederum geeignete Möglichkeiten zur Verfügung gestellt werden, die Datenträger verschlossen aufzubewahren, also durch bauliche Veränderungen oder geeignete Schränke (Wechselwirkung zu 10.1.5) eine sichere Unterbringung zu gewährleisten.

Für alle diese Komponenten (und viele weitere mehr) hält das BSI-Grundschutzhandbuch die wesentlichen Aussagen vor; *„...Damit kann für die überwiegende Zahl der IT-Systeme der bislang arbeitsintensive Prozess der Erstellung eines IT-Sicherheitskonzepts erheblich vereinfacht werden, da aufwendige und oft komplexe Analysen von Bedrohungen und Eintrittswahrscheinlichkeiten entfallen. Mit Verwendung des Handbuchs*

*bedarf es lediglich eines Abgleichs des Maßnahmen-Solls mit dem Maßnahmen-Ist, um Sicherheitsdefizite zu ermitteln und passende Sicherheitsmaßnahmen zu identifizieren...*“ (IT-Grundschutzhandbuch, Stand Oktober 2000, Vorwort D. Henze)

Ob und wie das konkrete Sicherheitsmanagement konzipiert und umgesetzt werden kann, ist abhängig von den Umgebungsbedingungen, so z.B. Anzahl der eingebundenen Rechner, lokale Ausdehnung, bauliche Strukturen usw.

Grund- und Kernanforderungen, wie sie in annähernd jeder Darstellung zur Problematik in der Literatur<sup>130</sup> formuliert werden, bilden nur die geeignete Basis; eine wirklich umfassende Betrachtung mit dem Ziel einer Umsetzung muss jedoch über derartige Überlegungen weit hinausgehen und Bedrohungen und Grundschutz für jeden einzelnen Bereich erheben.

## **10.2 Erhebung des Grundschutzes**

Eine Erhebung des Grundschutzes setzt eine umfassende Inventur aller vorhandenen IT-Komponenten einschließlich zugehöriger Rahmendaten (wie z.B. Versionsstand o.ä.) voraus. Dabei kann keine Beschränkung auf die genutzten PC vorgenommen werden, stattdessen sind **alle** der Kommunikation dienenden Bestandteile einschließlich der Subsysteme, der Telefone, der Faxgeräte, der Peripheriegeräte sowie der genutzten Software zu erfassen. Sofern diese einer wie auch immer gearteten Verarbeitung von Daten dient, es sich also um eine Datei handelt, sind die zugehörigen Datei- und Verfahrensbeschreibungen (s. DSG NW und BSI Grundschutzhandbuch) beizulegen. Für jedes einzelne so erfasste Gerät und jede Anwendung sowie jede Datei bestehen konkrete Schädigungsmög-

---

<sup>130</sup> Vgl. hierzu z.B. zum modularen Netzaufbau DROSTE, in: HORSTER (2001), S. 1 – 11; zur Anonymisierung zum Schutz der Privatsphäre ECKERT, C. / PIRCHER, A.: Anonym im Internet, Probleme und Lösungen; in: HORSTER (2001), S. 13 – 25; zur Installation von Firewall-Systemen POHLMANN, N.: Möglichkeiten und Grenzen von Firewall-Systemen. in: HORSTER (2001), S. 26 – 46;

lichkeiten und konkrete Chancen des Zuganges ins Gesamtnetz (so z.B. das ganz simple Ausspionieren über das Abhören von Telefonen, das Mit-hören oder Mitlesen von gesprochener oder geschriebener Kommunikation oder ähnliches).

Für jedes dieser Geräte und jede dieser Anwendungen ist im Anschluss daran zu prüfen, welche Konsequenzen ein Ausfall, eine Schädigung oder ein unerlaubter Zugriff haben können<sup>131</sup>. Die daraus resultierenden Folgen können sich qualitativ unterschiedlich darstellen (vgl. hierzu BSI-Grundschutzhandbuch, Kapitel 2). Daher ist für jeden Posten in der Inventarliste ein qualitativer Schutzbedarf zu formulieren. Es ist ein Unterschied für die Priorität innerhalb des Sicherheitskonzeptes, ob der Ausfall eines Gerätes „nur“ verhindert, dass ein Mitarbeiter seiner Arbeit weiterhin nachgehen kann, oder ob dieser Ausfall zur Konsequenz hat, dass das gesamte System gefährdet oder für Zugriffe offen gelegt wird.

Daraus lässt sich erkennen, dass auch die Topologie und Architektur des bestehenden oder des geplanten Netzes ebenso dringend in die Überlegungen einbezogen werden müssen<sup>132</sup> wie die Frage, ob das geplante Netz sich herkömmlicher Übertragungsmedien bedient oder als Funk-LAN aufgebaut werden soll.

Der so erhobene Geräte- und Anwendungsbestand, verknüpft mit den Aussagen über die Konsequenzen eines möglichen Ausfalles, stellt die Ist-Beschreibung dar.

---

<sup>131</sup> Die festgestellten Schutzbedarfskategorien können sich nach den Schäden richten, die durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit der Anwendungen bzw. der Komponenten entstehen; zu weiteren Details s. BSI IT Grundschutzhandbuch, S. 40. Dort werden auch der Verstoß gegen Gesetze / Vorschriften / Verträge und die Beeinträchtigung des informationellen Selbstbestimmungsrechtes als wesentliche Konsequenzen erläutert.

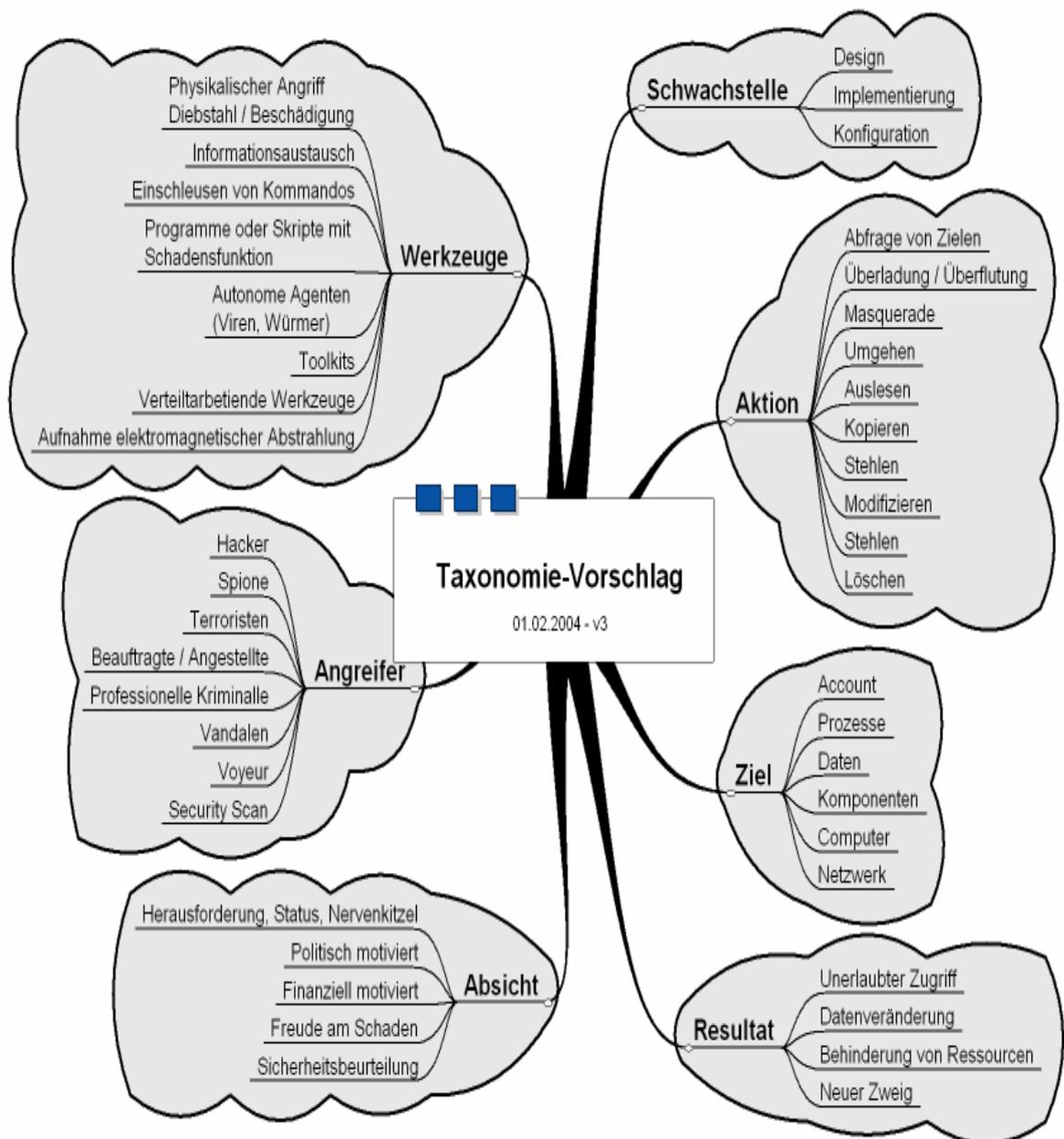
<sup>132</sup> S. hierzu Kap. 2.2.3, in dem z.B. die Konsequenzen des Ausfalles EINES Rechners z.B. in einer Ring-Topologie erkennbar werden.

In einer Planungsphase für Vernetzungen von Firmen, Behörden, Schulen usw. muss dieser Ist-Zustand abgeglichen werden mit den Plänen der Gesamtvernetzung. Nur wenn das Gesamtkonzept unter Einbeziehung der gegenwärtigen Gegebenheiten erstellt wird, ist beides entsprechend zukunftsorientiert und sicher.

Auch in den übrigen genannten Betrachtungsfeldern (s. Kap. 10.1) müssen entsprechende Erhebungen des Ist-Zustandes durchgeführt werden. Damit ist es also auch erforderlich, den Ausbildungsstand des Personals, bestehende Regelungen innerhalb der personellen Besetzungen, bauliche Gegebenheiten usw. zu betrachten und mit den Wunschvorstellungen für eine zukünftige Vernetzung abzugleichen. Daraus ergeben sich die Hinweise darauf, welche weiteren organisatorischen Maßnahmen noch zu treffen sind, wo es z.B. zu Umsetzungen, Umzügen, Umbauten oder ähnlichem kommen muss, um den Anforderungen gerecht zu werden.

In engem Zusammenhang mit der Erhebung des Ist-Zustandes muss aber auch eine Analyse potentieller Störfälle erfolgen, die die Gegebenheiten schulischen Datenschutzes und schulischen IT-Einsatzes berücksichtigt.

Die Vielzahl möglicher Störfälle bzw. Attacken beruht auf einer ebenso facettenreichen Motivationsstruktur und hat damit auch ganz verschiedenartige Konsequenzen zu verzeichnen. Eine einheitliche Taxonomie existiert bislang nicht, wurde u.a. von BUSCH, C. und WOLTHUSEN, S., Fraunhofer Institut, WS 2002 / 2003 versucht sowie von DITTMANN, J., Uni Magdeburg 2003. Nach deren Skript richtet sich weitgehend die nachfolgende Darstellung:



**Abbildung 10: Struktur potentieller Schadensereignisse.**

Mind-Map erstellt durch Verf.

Viele von diesen möglichen Störungen und Angriffen sind für den schulischen Bereich irrelevant. Mögliche Motive dürften hier anders gelagert sein:

- Während die Industrie mit der Entwicklung des Internets einen neuen Dienstleistungs- und Servicebereich nutzt, der durch professionelle Hackings die Sicherheitsvorkehrungen jeweiliger Auftraggeber zu überwinden versucht und damit Lücken aufdeckt, dürfte dies für den schulischen Bereich eher nachrangig sein. (Professionelle) Hacker befassen sich nicht mit einer einzelnen Schule, um ihre Sicherheitstechnik auszutesten, es sei denn, sie haben einen wie auch immer gearteten Bezug zu eben dieser Schule. Hochkomplexe Sicherheitssysteme zu überwinden erfordert ein hohes technisches Detailwissen; Schüler, die ein solches Wissen erlangt haben, dürften in der Schule als „Fachmann“ bereits bekannt sein und sich daher der Tatsache bewusst sein, dass sie relativ leicht zu ermitteln sind. Nicht bekannt allerdings ist natürlich, wie oft sich bereits Personen im Datennetz einer Institution bewegt haben, ohne dass dies überhaupt erkannt werden konnte und bekannt geworden ist; und das kann natürlich auch in Schulen der Fall sein.
- Angriffe auf vernetzte Computersysteme durch Zugriffe von außen, also über den Internet-Zugang, sollen in aller Regel wie auch immer geartete sensible Daten als „Beute“ oder Resultat hervorbringen, die dem Angreifer von Nutzen sein können. Dazu zählen z.B. Bankverbindungen innerhalb des online-Bankings, persönliche Daten, die zur Information über ein potentielles Opfer für andere Straftaten dienen können usw. Im schulischen Nutzungsbereich sind derartige Zugriffe, die eher der allgemeinen kriminellen

Energie einzelner Straftäter zuzuordnen sind, vermutlich eher selten.<sup>133</sup>

- Die allgemeinen Attacken, die sich aus dem Internet heraus auf einzelne Rechner und Systeme erstrecken (so die bereits mehrfach erwähnten Viren, Würmer oder Trojaner), sollen nicht in erster Linie die erreichten Rechner und Systeme schädigen, sie sind häufig nach bisherigen Erkenntnissen Ergebnis einer Strategie von Microsoft-Gegnern, die die Lücken in der Sicherheit von Microsoft-Produkten immer wieder erneut unter Beweis zu stellen versuchen. So ist zu beobachten, dass viele Sicherheits-Updates des Konzerns kurz darauf zu erneuten Attacken führen. In dieser Hinsicht scheinen sich Microsoft-Gegner weltweit in einem Wettstreit zu befinden, der letztlich zu einer Gefährdung von unzähligen Systemen führt.

Schulische Systeme dürften, legt man die Vielfalt möglicher System-schädigungen auf der Basis des Schemas Abb. 10 und der vorangegangenen Ausführungen zu Grunde, eher anderen Gefahren ausgesetzt sein, die anderen Motivlagen entspringen. Daraus jeweils resultierende mögliche Konsequenzen gilt es in den Auswirkungen für jede Schule festzustellen. Ebenso sind die möglichen entsprechenden Gegenmaßnahmen für die schulischen Bereiche zu planen:

Terroristische Anschläge auf schulische Systeme sind ebenso wenig zu erwarten wie voyeuristische; allerdings kann es durchaus zu bestimmten „Spionageformen“ im weiteren Sinne kommen, wenn z.B. versucht wird, in

---

<sup>133</sup> Eine Statistik über erfolgte Zugriffe, etwa analog einer Kriminalstatistik, existiert zur Zeit nicht, daher sind hier nur Mutmaßungen möglich; das Dunkelfeld ist ebenfalls in keiner Weise erforscht, da es bislang keine Untersuchungen hierzu gibt.

Schüler- oder Lehrerdaten, Notenübersichten o.ä. Einblick zu nehmen<sup>134</sup>. In einem funktionierenden System werden sie dies jedoch nicht von zu Hause aus über das Internet tun, sondern die Gelegenheit nutzen, dies aus dem schulischen Netz heraus und damit mit weniger Entdeckungsrisiko zu tun. Simple Einsichtnahme (z.B. in Form eines „über-die-Schulter-Sehens“) und damit ein Eingriff in die Vertraulichkeit der Daten ist nur eine der möglichen Varianten. Es gilt also, schulische Netze nicht nur gegen den Angriff von außen zu schützen, sondern sie auch im innerschulischen Betrieb so einzurichten, dass Schüleraktivitäten innerhalb der Schule keinerlei Schäden anrichten können.

Bislang ist lediglich von mehr oder minder vorsätzlichen Angriffen auf das System ausgegangen worden, die also den Begriff des „Angriffs“ tatsächlich erfüllen. Diejenigen Störungen, die fahrlässig verursacht werden, sind allerdings auch diejenigen, die zumeist sehr schnell festgestellt werden und die damit auch bekannt sind. Mitarbeiter des Sekretariats, die die Diskette mit ihrem Lieblingskartenspiel von zu Hause mitbringen und im Diskettenlaufwerk des Netzrechners lesen lassen und installieren, Lehrer, die die zu Hause geschriebenen Stundenverläufe, Arbeitsblätter, Folien pp. im Schulrechner ausdrucken, dazu die Disketten von zu Hause mitbringen und nicht durch Virens Scanner überprüft haben, sind keine Seltenheit. Derartigen alltäglichen und vollkommen normalen Vorgängen innerhalb des Systems muss ebenfalls Rechnung getragen werden, um mögliche Schäden zu verhindern.

Dies alles wird sich bei optimalem Verlauf durch die Feststellung der verschiedenen Schutzbedarfskategorien herauskristallisieren, sich sodann

---

<sup>134</sup> Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000, Teil 4-2: „...Bei Manipulationen oder Sabotageakten von Schülern fehlt i.d.R. das Bewusstsein, dass durch ihr vorsätzliches oder fahrlässiges Handeln ein beträchtlicher materieller Schaden entstehen kann. Vielmehr wird ein derartiges Verhalten als zeitgemäßer Schülerstreich oder als Profilierungsmöglichkeit, was das eigene Computerwissen angeht, gesehen...“

hinsichtlich eines Rankings möglicher Störungen priorisieren lassen. Ergebnis wird eine Liste zur Umsetzung von Maßnahmen sein.

### 10.3 Maßnahmen zur Erreichung eines Grundschutzes

Eine derartige Prioritätenliste kann hier nicht abschließend formuliert werden, da sie für die jeweiligen Gegebenheiten innerhalb eines konkreten Systems erarbeitet werden muss und sich immer auf die Basisdaten des Ist-Zustandes beziehen muss.

Lediglich einige allgemeingültige Grundaussagen zur Umsetzung können hier dargelegt werden, die für die einzelnen Systeme ausbaubar und unter Zuhilfenahme des BSI-Grundschutz-handbuches zu optimieren sind:

- Installierte Sicherheitssysteme sollten ohne großen Aufwand und mit möglichst geringem Bekanntheitsgrad installiert werden können; je bekannter und auffälliger ein System geschützt ist, desto mehr zieht es die Interessen gerade derjenigen Schüler an, die ihr Wissen und ihre Fähigkeiten testen, sich mit dem Sicherheitskonzept messen und das System knacken wollen.<sup>135</sup>
- Der innerhalb der Lehrerschaft und der Bediensteten der Schulverwaltungen und Sekretariate gänzlich unterschiedliche Ausbildungsstand hinsichtlich Computer, deren Nutzung und Möglichkeit erfordert es, eine optimale Sicherheit so zu erreichen, dass

---

<sup>135</sup> Handbuch Praxis Schul-EDV; Systembetreuung – Schulnetze; Stadtbergen 2000, Teil 4-2: „...Die Bekanntgabe von Sicherheitsmaßnahmen gegenüber Schülern hat mitunter die Folge, dass seitens des Systembetreuers oder Fachlehrers eine vermeidbare Wettbewerbssituation hervorgerufen wird. Folge dieses „Kräftemessens“ ist i.d.R., dass die absichtliche Manipulationen seitens der Schüler sich häufen. Die Erfahrung zeigt: Je unauffälliger Schutzmaßnahmen ein- bzw. durchgeführt werden, umso geringer ist der Anreiz für die Schüler, sich gegen diese Maßnahmen zu sträuben...“

auch zufällige Störungen ausgeschlossen werden. Dies wiederum erfordert, dass nicht nur administrative Möglichkeiten genutzt werden sollten, auch die Aus- und Fortbildung der User ist vonnöten ebenso wie bereits genannte bauliche oder organisatorische Maßnahmen im Einzelfall. So kann z.B. bereits die Ausrichtung des Monitors dazu führen, dass Daten ausgelesen werden können (kann man durchs Fenster oder von der Tür aus mitlesen, sich auch hinter einen Schreibtisch stellen o.ä.), eine simple Drehung des Monitors oder andere Position der Möbel kann bereits die Vertraulichkeit der Daten schützen.<sup>136</sup>

- Die einfachste, aber nicht komfortabelste Lösung zur Erreichung der Sicherheit ist eine strikte physikalische Trennung unterschiedlich genutzter Bereiche, wie sie auch nach den Ergebnissen der Befragung durch manche Schulen bereits realisiert wird (s. hierzu Kap. 6 ). Weniger komfortabel und mit höherem Anspruch an das Sicherheitsempfinden des Nutzers, dennoch rein technisch möglich ist es, innerhalb eines Rechners durch verschiedene Karten den Zugriff auf verschiedene Teilnetze zuzulassen, was jedoch jeweils eine erneute Anmeldung, bei Wechselsteckkarten zusätzlich einen jeweiligen Kartenwechsel erfordert.
- Die Auffassungen über die erforderlichen Sicherheitsstandards innerhalb der Schulen gehen in der Realität und in der Literatur weit auseinander. Während teilweise eher vordergründig an materielle Schäden gedacht wird, die Bedeutung des Schulnetzes für einen effizienten Computereinsatz im Unterricht höher bewertet wird als der Sicherheitsaspekt (so BERNSTEIN (2001), Teil 4-2, S. 1), sind gerade die Datensicherheitsmaßnahmen zur Realisierung des Datenschutzes im besonderen Interesse der Datenschutzbe-

---

<sup>136</sup> vgl. BERNSTEIN, H.: PC Sicherheit, Berlin und Offenbach 2001, S. 5: „...Häufig sind triviale Ursachen, wie Nichtsichern von Dateien, der schlampige Umgang mit Disketten und anderen Speichermedien, Gestaltung der Zugriffsrechte, Verschlüsselung von Informationen, die fatale Folgen haben.“

auftragten und können nicht weit genug gehen. Zu realisieren ist also quasi der Spagat zwischen Verbot und Sicherheit, die Auflösung des Spannungsverhältnisses zwischen Liberalität und Einschränkung.<sup>137</sup>

Wie die bisherigen Erörterungen verdeutlichen, sind Datenschutz und Datensicherheit in allen erforderlichen Aspekten schwer erreichbare Ziele, die sowohl Personal und Know How als auch Mittel und Zeit benötigen und binden und nie zu einem tatsächlichen Abschluss gelangen werden. Die Feststellung des Ist-Zustandes im Rahmen eines Managements ist eine Momentaufnahme; allein die Beschaffung neuer Geräte verändert sie wieder, neue Software erfordert neue Betrachtungen, neu eingestellte Lehrer/innen benötigen neue Einweisungen, haben neue Ideen und Vorschläge usw.. Demzufolge ist das Erreichen einer möglichst optimalen Sicherheit ein immerwährender Prozess, der nur von dauernder Rückkopplung und ständiger Evaluation lebt; ein Optimum als statischer Zustand kann hier nicht erreicht werden.

Das aber bedeutet auch, dass für jede einzelne Schule diese Daueraufgabe für sich gelöst werden muss. Der hierfür notwendige wirtschaftliche und personelle Aufwand aber steht in keinem Verhältnis zu den Erfordernissen. Darüber hinaus hat sich in der Vergangenheit herausgestellt, dass die Administration großer Systeme auch hinsichtlich des zu realisierenden Sicherheitsstandards wirtschaftlicher ist als eine Aufspaltung in viele kleine Teilsysteme.<sup>138</sup>

Dieser Erkenntnis könnte man gerecht werden, würde man den Weg in ein großes Schulsystem finden, das mit den heutigen Strukturen nicht mehr vergleichbar ist und eingebettet wird in ein Gesamtsystem der Verwaltung, so dass dem Prinzip der Wirtschaftlichkeit der Administration

---

<sup>137</sup> s. Kap. 8

<sup>138</sup> vgl. BERNSTEIN, H., 2001

ebenso gefolgt werden kann wie dem der Einmalerfassung und Mehrfachnutzung von Daten unter optimaler Datensicherheit. Das allerdings erfordert einen Umdenkungsprozess nicht primär bei den Usern in den Schulen, sondern vielmehr bei den Planern und Installateuren der Netzwerke.

## **11 Auswirkungen und Konsequenzen: Ein „neues Netzverständnis“**

Die Befragung hat ergeben, dass alle teilnehmenden Schulen die Auffassung vertreten, die Nutzung von IT und Netzwerken sei sinnvoll. Allerdings sind weitere Ergebnisse, dass die Schulen mit der Vorbereitung, Gestaltung und Betreuung ihrer Technik allein gelassen werden und daher vom Know-how Einzelner abhängig sind, ganz zu schweigen vom Problem der Kostenentwicklung und -deckung.

Um hier ein allgemeingültiges und sinnvolles, die festgestellten Schwierigkeiten ausräumendes Konzept zu entwickeln, ist es erforderlich, eine neue Denkweise zu gewinnen und in eine Planung einzutreten, die zwar einerseits den dimensional Rahmen bisheriger Planungen sprengt, andererseits aber zukunftssträftig scheint und die Möglichkeit mitbringt, entsprechende Ausbaustadien zu erhalten, die auch noch für eine Zeitspanne von z.B. 10 Jahren tragfähig sein werden.

Bereits vor einigen Jahren im ausgehenden 20. Jahrhundert haben fast alle Bereiche öffentlicher Verwaltung (ausgenommen Justiz) neue Steuerungsprozesse auf mehreren Ebenen eingeleitet. In allen Behörden gehören seither Begriffe wie „Produktsteuerung“, „Output- und Outcome-Orientierung“, „Kennzahlen“ und „Kosten-Leistungs-Rechnung“ zum täglichen Leben der Beschäftigten. Softwareentwickler konkurrieren um die Aufträge, angepasste Programme für die Behörden zur Verfügung zu stellen. Nur Schulen scheinen sich aus diesem Prozess bislang ausgenommen zu haben, wenngleich sie Teil der öffentlichen Verwaltung sind.

Das Ziel in der Nutzung moderner Technologie kann nicht sein, einzelne, zwar zweckgerichtete, aber in der Nutzungsdimension eingeschränkte Lösungen zu entwickeln, das Ziel muss vielmehr sein, eine umfassende gemeinsame Lösung zu finden, die auch eine an rechtlichen Vorgaben ori-

enterte lückenlose Kommunikation innerhalb der verschiedenen Verwaltungsbereiche ermöglicht.

Dazu muss ein Gesamtkonzept entwickelt werden, dessen stufenweiser Ausbau – ob bottom up oder top down sei dahingestellt – landesweit umzusetzen ist, das also auch ein landesweites Konzept erfordert und daher folgerichtig nur im Ministerium angesiedelt werden kann. Für die Umsetzung in der Praxis bietet sich das Vorgehen vom Allgemeingültigen im Großen zum Speziellen im Kleinen an (top down: Ministerium zuerst, einzelne Schulen zuletzt). In der Folge wird eine mögliche Umsetzung eines landesweit gültigen Konzeptes vorgestellt.

### **11.1 Schaffung eines „allgemeinen Verwaltungsnetzes“**

Eine Anbindung in einem der Ministerien ist dann nicht mehr ausreichend, wenn auch die Vernetzung der verschiedenen Verwaltungszweige miteinander erreicht werden soll, da die Grenzen ministerieller Entscheidungskompetenzen partiell überschritten werden. In einer solchen Ausdehnung des Netzes kann nur noch die Landesregierung als richtige Entscheidungsebene angesehen werden. Eine derartige Netzdimension aber macht Sinn, da unterschiedliche Bereiche auch unterschiedliche Daten vorhalten, die jedoch wiederum für andere bedeutsam sein können:

- Finanzämter halten Daten über Personen, Einkünfte, Eigentum, Kraftfahrzeuge usw. vor,
- Arbeitsämter u.a. über Beschäftigungsverhältnisse, Qualifikationen allgemeiner und spezieller Art,
- Schulen über Schülerdaten incl. Daten über Erziehungsberechtigte (und damit indirekt über familiäre Situationen), Unterrichtsgegenstände, besondere Leistungen und Fähigkeiten u.v.m,

- Polizeibehörden über kriminelle Machenschaften mehr oder minder schwerwiegender Art einschließlich vieler personengebundener Dateien unterschiedlicher Inhalte
- und andere Behörden haben viele andere Daten und Datenbestände mit z.T. anderen Kennzeichen.

Jede dieser Institutionen hält ihr Wissen für sich und im eigenen Bereich. Zuweilen ist auch innerhalb der Behörden selbst ein Datentransfer bzw. eine Auskunft über vorgehaltene Daten aus rechtlichen Gründen nicht möglich<sup>139</sup>, was – wenn man sich die Gefahren eines ungehinderten Datenaustausches vor Augen führt – auch durchaus sinnvoll ist. Das aber hat zur Folge, dass unterschiedliche Datensammlungen teils mit gleicher Grundaussage oder mit ähnlicher Zielrichtung parallel betrieben werden; der Grundsatz der Einmalerhebung zur Mehrfachnutzung, der ein effektives und effizientes Nutzen der technologischen Möglichkeiten bedeutet, ist daher nicht zu realisieren.

Eine Vernetzung, die sämtliche Bereiche öffentlicher Verwaltung innerhalb des Landes miteinander verbindet, innerhalb dieses Gesamtnetzes aber Teilbereiche für Spezialdaten vorhält, würde diesem Ideal näher kommen.

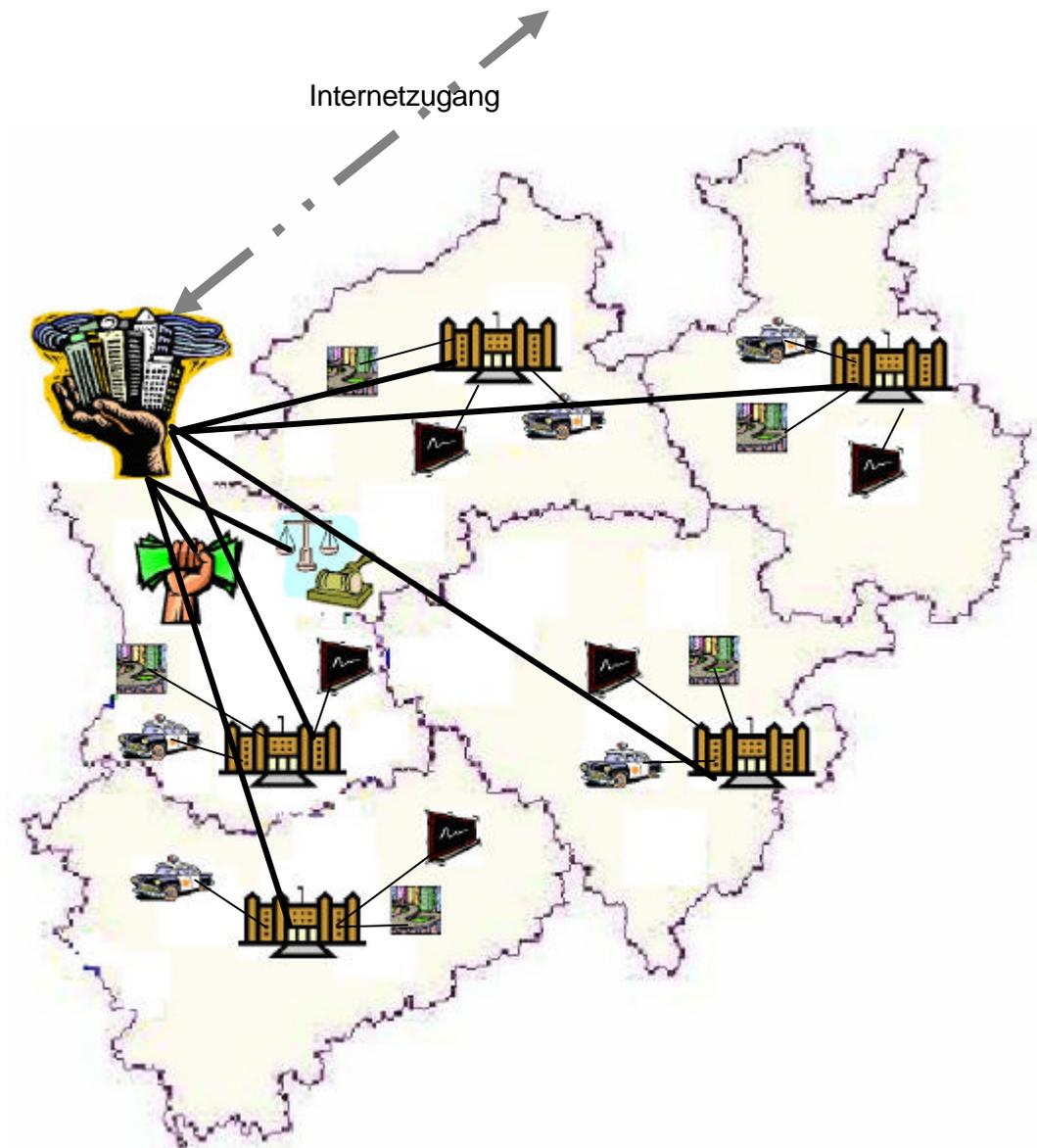
Das „Allgemeine Verwaltungsnetz“ NRW würde zuständigkeitsübergreifend, über ministerielle Grenzen hinweg, sämtliche Hierarchieebenen und Sparten der Verwaltung abbilden und lückenlos die unterschiedlichen Verwaltungszweige miteinander verbinden, aber auch gewährleisten, dass an den erforderlichen Grenzen „Zugangssperren“ errichtet sind.

Die folgende Skizze stellt vereinfacht ein solches Netz dar:<sup>140</sup>

---

<sup>139</sup> Als Beispiel sei erneut verwiesen auf die aus Datenschutzgründen nicht mögliche Kopplung des Schulverwaltungsnetzes mit dem Internet.

<sup>140</sup> Detaildarstellungen in der Skizze richten sich nicht auf die untere oder mittlere Netzebene von Justiz und Finanzwesen. Da diese auf Grund ihrer Organigram-



**Abbildung 11: Skizze eines umfassenden Landesverwaltungsnetzes**

Nordrhein-Westfalen wird in fünf mittlere Netzebenen gegliedert, die organisatorisch den Bezirksregierungen zugeschrieben werden. Zusätzlich werden die nicht den Bezirksregierungen zugeordneten Verwaltungsbereiche wie Finanzministerium (mit seinen Oberfinanzdirektionen und Finanzämtern, LBV usw.) und Justizministerium (mit allen zugeordneten Justizbereichen aller Ebenen, also z.B. vom Schiedsmann bis zum OLG / OVG, Staatsanwaltschaften usw.) in diese obere Netzebene NRW bei der Landesregierung einbezogen.

Zum Aufbau und den einzelnen Komponenten s. nachfolgende Abbildungen (Abb. erstellt durch Verf.)

me wiederum einen sehr detaillierten Teilaufbau erfordern, wird hier lediglich die symbolische Darstellung der ministeriellen Ebene gewählt, ohne die Darstellung auf die Bezirksregierungsebenen herunterzubrechen.

Die inhaltliche Gestaltung eines derartigen Netzwerkes muss darauf ausgerichtet sein, alle Bereiche der Verwaltung abdecken zu können. Das bedeutet, dass sich dieses umfassende Netz aus einer Vielzahl von Komponenten zusammensetzt, die sich teils überschneiden, teils auf Grund der ganz unterschiedlichen Ansprüche an Sicherheit auch gegenseitig ausschließen. Die Komponenten setzen sich in unterschiedlichen Ebenen aus verschiedenen Bausteinen zusammen. Die „untere Netzebene“ wird gebildet aus den einzelnen Behörden / den einzelnen Schulen.

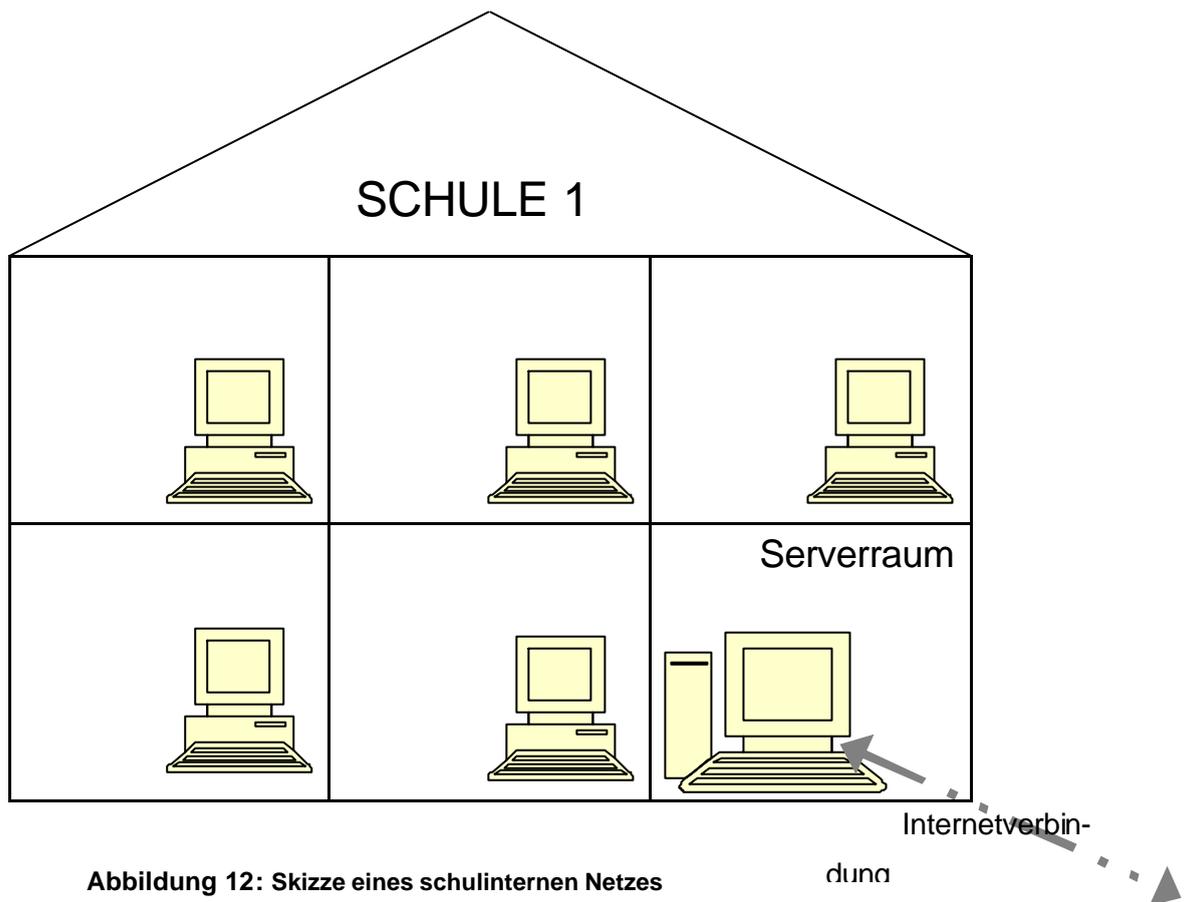
## **11.2 Schule – die kleinste Einheit des Verwaltungsnetzes**

Jede Schule erhält ihr eigenes schulinternes Netz, in das alle vorhandenen PCs eingebunden werden. Hierzu bietet sich eine Client-Server-Struktur an (s. Abb. 4, S. 33). Für die Pflege und Wartung, aber auch für die Sicherheit (Setzen und Streichen von Berechtigungen pp.) ist der Administrator der jeweiligen Schule zuständig. Seine Arbeit endet dort, wo Belange des eigenen Verbundes überschritten werden und solche der gesamten unteren Netzebene oder gar die mittlere oder die obere Netzebene betroffen sind (s. S. 179 ff).

Wo auch immer in der Schule sich ein Schüler oder ein Lehrer an einen Rechner setzt: er findet immer seine eigene Benutzeroberfläche, seine eigenen Berechtigungen vor und kann von jedem schulischen PC aus seine Arbeiten erledigen. Jede seiner Bewegungen im Schulnetz wird entsprechend dem Datenschutzkonzept registriert. Welche Wege die von ihm bewegten Datenpakete dabei nehmen, ist für den Einzelnen nicht von Belang, wesentlich für ihn sind nur eine komfortable Nutzungsmöglichkeit und schnelle PC-Leistung.

Jeder PC bietet ebenfalls – z.B. über Proxy-Server im eigenen Haus oder in der nächsthöheren oder oberen Netzebene - den Zugang ins Internet. Eine physikalische Trennung ist damit nur noch in hochgradig gefähr-

deten Bereichen (z.B. polizeilicher, sicherheitsrelevanter Daten) angezeigt; auch die Abkopplung des schulischen Verwaltungsnetzes vom restlichen schulischen Netz ist nicht mehr erforderlich: Sicherheitsaspekte werden durchaus durch logische Vorgaben erfüllt.



**Abbildung 12: Skizze eines schulinternen Netztes**

Jeder Raum innerhalb der Schule ist mit einer angemessenen (also bedarfsorientierten) Anzahl PCs ausgestattet, mindestens aber mit einem Rechner. Alle PCs sind miteinander vernetzt. In einem separaten Serverraum werden alle Administrationaufgaben wahrgenommen, die erforderlichen Server vorgehalten und der Zugang zum Internet realisiert.  
(Abb. erstellt durch Verf.)

Wie jeder andere Teil öffentlicher Verwaltung auch sind **alle** Schulen miteinander zu verbinden und durch Eingliederung in die Untere Netzebene in das Verwaltungs-Intranet einzubinden. Das hat zur Folge, dass Daten von Schülern und Lehrern nicht in den einzelnen Schulen vorgehalten werden, sondern zentral beim Schulträger (mittlere Netzebene) oder dem Ministerium (landesweite obere Netzebene) auf dem dortigen Server liegen.

Zugriffe der einzelnen Schulen sind über das Intranet auf diese Datenpools möglich (s. auch Abb. 13).<sup>141</sup>

Hier bietet sich erneut an, Windows NT als Betriebssystem zu wählen, da – abgesehen von der Tatsache, dass viele Schulen bereits damit arbeiten – in diesem System zunächst alle Berechtigungen gesperrt sind, sie gezielt geöffnet werden müssen, was dem Sicherheitsaspekt entgegen kommt.

Über die Berechtigungen, die nur durch die jeweiligen Administratoren gesetzt werden können, kann immer nur derjenige verändernd auf die Daten zugreifen, der gleichzeitig der aktuelle Datenbesitzer ist, also z.B. diejenige Schule, die der Schüler zur Zeit besucht. Schulwechsel, Abschlüsse u.ä. verlangen damit Veränderungen in den Berechtigungen, die durch die zentralisiert angesiedelten Administratoren vollzogen werden. Das wiederum bedeutet für die Schulen, dass der Administrationsaufwand für sie erheblich reduziert, wenn nicht gegen Null geführt wird. Gerade der große finanzielle und personelle Aufwand der Netzadministration und die Tatsache, dass derartige Arbeiten von Lehrkräften zusätzlich übernommen werden müssen, hatte bei der Befragung der Schulen zu vielen kritischen Anmerkungen geführt (s. hierzu die Textanmerkungen in Kap. 6.12 sowie Kap. 7.9). Die Schulen fühlen sich bislang allein gelassen, was man durch die umfassendere Organisation in einem Landesverwaltungsnetz auffangen könnte.

---

<sup>141</sup> Diese Nutzung ginge über eine rein statistische, wie sie offenbar in Baden-Württemberg angestrebt wird, hinaus. In Heft 1/2 aus 2002 der VDI-Nachrichten, S. 4, findet sich folgende Notiz:

**Stuttgart: Schulen ans Netz der Verwaltung**

*Die rund 4000 Schulen Baden-Württembergs werden bis 2005 an das Computernetz der Verwaltung angeschlossen werden. Das neue Intranet soll der Erhebung von Statistiken dienen, was wiederum die Planung verbessern soll. „Im Bereich der statistischen Erhebungen verlassen wir heute sozusagen die Zeit des Mittelalters“, so Kultusministerin Annette Schavan (CDU) zu dem bundesweit einmaligen Projekt, in das das Land 15 Mio. Euro investieren wird.*

Konsequenz wäre dann, dass lediglich die eigenen Bedürfnisse innerhalb der Schule als dezentrale Zuständigkeit zu regeln sind<sup>142</sup>, wobei die Vorgaben der landesweiten Konzepte einzuhalten sind. Auf diese Weise kann erreicht werden, dass auch der derzeit noch bestehende „Wildwuchs“ an eingesetzter Software für schulische Verwaltungsaufgaben beseitigt und eine einheitliche Ausstattung erreicht wird. Daraus wiederum resultiert, dass sowohl Benutzerschulung als auch Wartungsaufwand zentralisiert und damit gering gehalten und so Kosten reduziert werden können.

Innerhalb der Schulen ist lediglich der Aufwand zu leisten, der erforderlich ist, das vom Gesamt-Verwaltungsnetz getrennt zu haltende Unterrichtsnetz zu pflegen, also z.B. diejenigen Rechner, die im Informatikraum, im Fremdsprachenraum oder ähnlich genutzt werden oder als eine Art Schulungsplattform dienen, um den Schülern den sicheren Umgang mit der Technik näher zu bringen. Darüber hinaus gibt es die Möglichkeit, mit bestimmten Berechtigungen das Verwaltungsintranet aufzurufen und Verwaltungssoftware zu nutzen. Sofern die schulinterne Technik gewartet werden muss, ist dies nach wie vor Kompetenzbereich der einzelnen Schule.

Das hat den Vorteil, dass die jeweilige Schule immer auf dem aktuellen Stand der Landestechnik bleibt, um Planungen, Konzepte und Vorhaben im Landesnetz weiß und entsprechende Vorarbeiten leisten kann, dass sie außerdem auf Erfahrungen anderer zurückgreifen kann und nicht für jedes auftretende Problem eine eigene Lösung erarbeiten muss, und – nicht zuletzt – dass Erfahrungen, Unterrichtsinhalte, Fachfragen, eventuell inhaltliche Darstellungen von besonderen Unterrichtsvorhaben oder Projekten ebenfalls zur Verfügung stehen und – wie in der freien Wirtschaft seit Jahren positiv umgesetzt – benchmarking und damit das „Lernen vom Besten“ möglich werden. Und es liegt hier der Vorteil, dass die bislang genutzte

---

<sup>142</sup> S. hierzu JONIETZ, D., in Computer und Unterricht 2001, der sowohl die schulspezifischen Anforderungen an Netzwerke als auch Vor- und Nachteile pädagogischer Netzwerke in die Betrachtungen einbezieht und konkrete Umsetzungsvorschläge formuliert, die jedoch wiederum mit den Anforderungen an Datenschutz und Datensicherheit abgeglichen werden müssen.

Vorgehensweise des Supports und der Wartung schulischer IuK-Technik durch einen Lehrer durch zentralen Support ersetzt wird. Egal also, ob Ferienzeit, ob der beauftragte Lehrer krank oder versetzt ist, die Technik wird weiterhin von zentraler Stelle betreut.<sup>143</sup>

Jede Schule betreibt so ihr eigenes internes Netz, das jedoch im Gesamtkontext lediglich ein Subnetz bildet. Dieses wird innerhalb des schulischen Intranets durch eigene Sicherheitsmaßnahmen zu anderen Schulen und zu anderen Verwaltungsbereichen abgesichert.

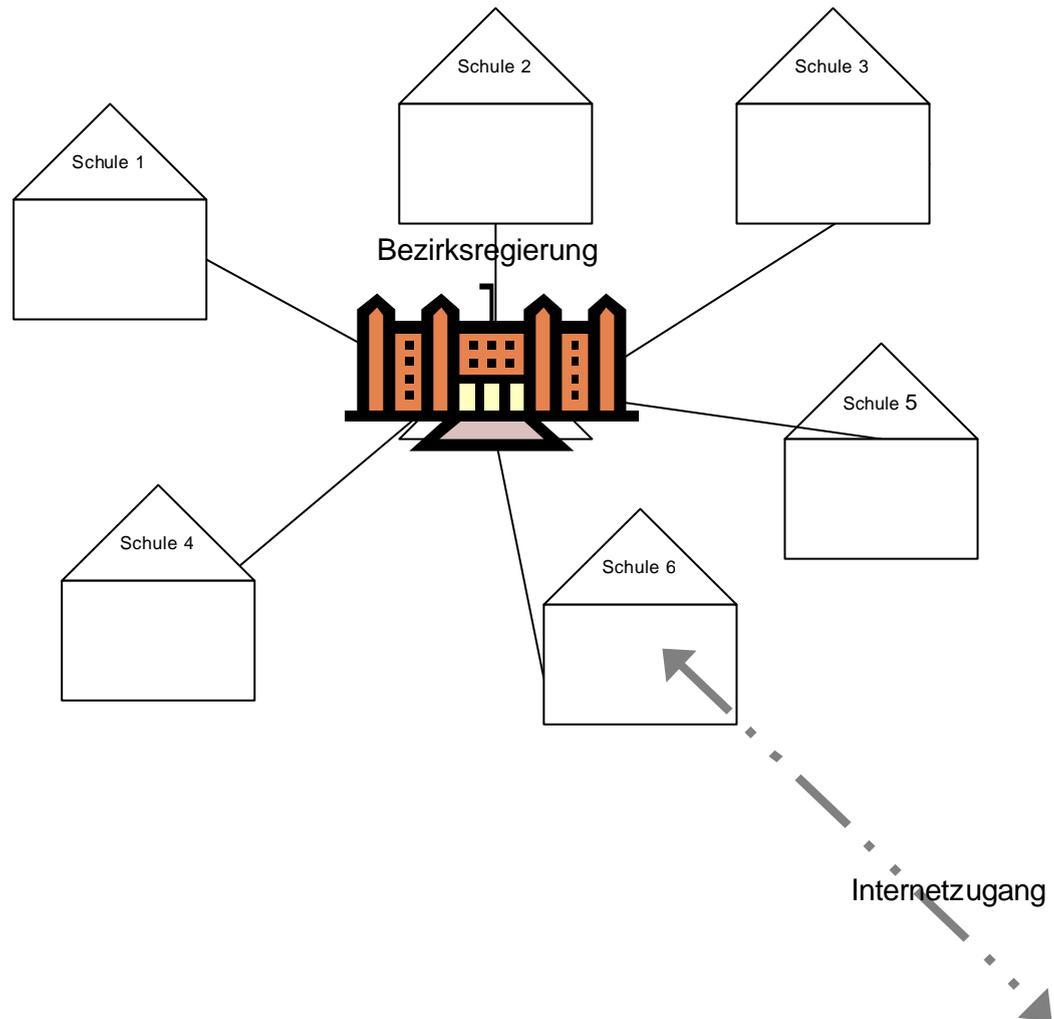
---

<sup>143</sup> Vgl. VDI Nachrichten vom 1. August 2003, S. 19:

*„... Denn je mehr Rechner und je ambitionierter die Konzepte und Systeme, desto weniger greift die bislang praktizierte innerschulische Lösung, einzelnen Lehrern oder engagierten Eltern die IT-Betreuung zu überantworten. So attraktiv, da kostengünstig, diese in der Vergangenheit auch sein mochte: Als langfristiges Konzept trägt sie nicht. Fehlt der Lehrer oder verlässt er die Schule, fließt das meist undokumentierte Wissen völlig ab, muss mühsam nach Ersatz gesucht werden...“*

### 11.3 Vernetzung der Schulen miteinander

Die so entstehenden vielen kleinen Subnetze werden zu einem Gesamt-Intranet aller Schulen zusammengeschlossen.



**Abbildung 13: Intranet der Schulen**

Die einzelnen wie in Abb. 12 intern vernetzten Schulen werden über die jeweiligen Bezirksregierungen miteinander verbunden, so dass eine Kommunikation zwischen den einzelnen Schulen möglich wird. Dabei handelt es sich noch immer um ein reines schulinternes Netz, das bislang nicht mit anderen Behörden verbunden ist. Zugang zum Internet kann über Server in einzelnen Schulen oder zentral über einen Server in der Bezirksregierung geregelt werden.  
(Abb. erstellt durch Verf.)

Über mehrere Zugangs-Server wird der online Datenverkehr innerhalb der Schulen und der Aufsichtsbehörden ermöglicht. Dies gestattet dann letztendlich auch, dass Schriftverkehr zwischen Schulen, Aufsichts-

behörden, Kommunen und so fort online abgewickelt werden. Es wird auf diese Weise so, wie es in der freien Wirtschaft und in anderen Behörden<sup>144</sup> bereits geraume Zeit realisiert wird, der Weg zur papierlosen Kommunikation beschritten. Natürlich kann dies alles nur unter der Diktion der Sicherheitsaspekte realisiert werden; die Planung einer solchen Kommunikationsstruktur muss also bereits zu Beginn der Planung mit in das Gesamtkonzept des Managements einbezogen werden.

Diese Vernetzung der Schulen miteinander eröffnet aber auch neue Horizonte bezüglich der Unterrichtsgestaltung und der Unterrichtsinhalte (s. S. 182). Eine umfassende Nutzung des Intranets, z.B. zum Einstellen von inhaltlichen Planungen, ermöglicht nach Zulassung durch die Berechtigten jeweils den Einblick anderer, das Lernen voneinander auch in den Lehrerkollegien, das Lernen vom Besten im Sinne eines guten Bench-Marking und damit ein gestaltbares, im Sinne der Schüler und der Allgemeinheit bereits seit langem anzustrebendes Qualitätsmanagement werden so ermöglicht. Die Schule der Zukunft kann sich nicht mehr mit der inhaltlichen und gestalterischen Lehrerarbeit im stillen Kämmerlein des heimischen Büros begnügen.

Zu vermeiden ist aber, dass diese Offenheit in jederlei Hinsicht zu einer vermehrten und eventuell übersteigerten Kontrolle der Fach- und Dienstaufsicht führen kann und so den Lehrerdatenschutz untergräbt. Die Chancen, die eine Vernetzung aller Schulen ohne Rücksicht auf Schulform oder Ausrichtung, Konzept oder Prägung zu einem einzigen umspannenden Schulnetz bietet, überwiegen diese Risiken aber bei weitem.

---

<sup>144</sup> So z.B. in manchen Landesbehörden und Ministerien

## 11.4 Einbettung der Schulnetze in das Internet

Keine Schule sollte sich mit dem begnügen müssen, was das schulische Intranet ihr bietet. Der Weg in die grenzenlose Kommunikation ist, wie die Beispiele in der Arbeit (s. Kap. 2.3) zeigen, ein Weg, den Schulen für ihr tägliches Geschehen werden nutzen müssen, um nicht die Entwicklungen an sich „vorbeirauschen“ zu sehen.

Die durch einige wenige engagierte Lehrer genutzten Möglichkeiten, die sich in Internet-Präsentationen und Veröffentlichungen finden, sind lediglich Highlights, an denen sich der untrainierte User orientieren kann. Sie müssen zum Alltag werden, es muss für Schüler und Lehrer normales Geschehen werden, dass der Rechner in den Unterricht integriert wird, ohne selbst Unterrichtsgegenstand (wie im Informatikunterricht) zu sein. Das geht nur dann, wenn Intranet-Nutzung und Subnet-Schule sich mit dem Weg ins Internet die Waage halten.

Eine entsprechend den Sicherheitsanforderungen gestaltete Struktur ist dabei wesentliche Grundvoraussetzung. Auch hier aber kann nicht jeder Schule einzeln die Entscheidung überlassen bleiben, wie, durch welche Zugangsart, mit welchem Provider und so fort sie dies gewährleisten will. Wenn der Netzaufbau in der Hand des Landes liegen muss, die Gestaltung des Intranets dort vorbereitet und umgesetzt wird, die Maßgaben für die schulischen Teilnetze dort vorformuliert werden, so kann auch nur dort entschieden werden, wie und mit welchen Mitteln die einzelnen Schulen ins Internet kommen können. Ob und wie dies gestaltet werden kann, ist Planungsaufgabe des vorbereitenden Ressorts. Ob dort letztlich entschieden wird, selbst als Provider aufzutreten, sich an kommerzielle Provider zu wenden oder an Landesdienststellen zu koppeln, kann nur abhängig sein von den übrigen zu erfolgenden Planungen. Auch hier gilt wieder: Ohne vernetzte Strukturen und ohne die Beachtung von Bedingungen, Konflikten u.ä. kann eine derartige Entscheidung nicht getroffen werden. Beispielhaft ist in Abb. 13 der Internetzugang den Bezirksregierungen zugeschlagen

worden, er kann ebenso gut zentral durch eine Landesbehörde (z.B. Landesamt für Datenverarbeitung und Statistik – LDS) realisiert werden, wie Abb. 11 es zeigt. Es muss aber wiederum auf die im BSI-Handbuch gemachten Aussagen verwiesen werden, die letztlich zu einer geeigneten Entscheidung werden führen können. Dort wird auch auf die Sicherheitsrisiken, die gerade mit dem Zugang zum Internet gegeben sein werden, verwiesen. Wie und wo letztendlich Sicherheit erzeugt wird, wie viele Firewalls wo installiert werden, wie deren Konfiguration auszusehen hat, ob es eine demilitarisierte Zone (in die mail- und www-server gesetzt werden können) geben wird oder nicht, all dies sind Detailfragen, die planerisch vorgedacht werden müssen, aber in aller Konsequenz lösbar sind und damit den Einsatz des Internets in Schulen ermöglichen werden.

Wesentlich allein erscheint, dass alle Schulen den Zugang zum landesweiten Verwaltungsnetz haben, innerhalb ihrer eigenen Zuständigkeiten die originären Aufgaben erfüllen können und das Internet für alle möglichen Erfordernisse nutzen können.

Naheliegend ist, dass die schulischen Rechner sämtlich auf das Internet zugreifen können sollten. Auf welchem Weg dies passiert, wie die Datenströme geleitet werden und an welchen Stellen es zu einer Identifizierung oder Protokollierung kommt, ist für den Einzelnen unerheblich. Wesentlich für ihn ist nur, dass seine Rechner inklusive aller Features ungehindert funktionieren (s. hierzu auch S. 156).

Es ist daher wie in Abb. 11 durchaus möglich, sämtliche Kommunikation auch über Landesserver abzuwickeln, also zentrale Proxy-Server, Mail-Server, Application-Server usw. vorzuhalten, über die jeder einzelne Rechner geleitet wird. Dies setzt Investitionen in diesem Bereich voraus, die wohl – angesichts der leeren Haushaltskassen – z.Zt. astronomisch anmuten, auf lange Sicht jedoch Ersparnisse bringen werden. Einmalinstallation, Einmalkonfiguration, Einmalbeschaffung sind sowohl kurzfristig als auch mittel- und langfristig lukrativer und wirtschaftlicher. Gleichzeitig entfaltet

eine derartige Lösung über die mögliche zentrale Protokollverwaltung besondere Wirkung im Bereich der Sicherheit.<sup>145</sup>

Analog zu diesen schulischen Vernetzungen gibt es ebenfalls Netze innerhalb aller anderen Verwaltungsbehörden. Letztendlich richten sie sich alle nach demselben landesübergreifenden Konzept. Das bedeutet, dass Abb. 12 ebenso übertragbar ist auf alle anderen Bereiche, sie stellt also nicht nur ein Schulnetz dar, sondern vielmehr auch das Netz einer Polizeibehörde, einer Kommunalverwaltung, einer Finanzverwaltung oder von Justizbehörden. So ließe sich Abb. 12 mehrfach kopieren, trüge dann jedoch unterschiedliche Titel und stellte das polizeiinterne Netz, das Justiznetz, das Netz der Kommunalverwaltungen usw. dar.

Natürlich sind in allen diesen Subnetzen wiederum Unterteilungen vorzunehmen. Keine Kommune wird in der Lage sein, alle ihre Zuständigkeitsbereiche (Feuerwehr, Katastrophenschutz, Einwohnermeldeamt, Straßenverkehrsamt, Steueramt, Stadtkasse und viele mehr) nach absolut einheitlichen Kriterien anzugliedern. Es werden Differenzierungen erforderlich sein, die sich aber wiederum nach den Regularien des Gesamtnetzes zu richten haben und die sich auch in der mittleren und oberen Netzebene wieder finden werden, da ja Bezirksregierungen und Ministerien über dieselben und noch mehr Zuständigkeiten verfügen.

In der Mehrheit haben die beteiligten Verwaltungszweige eine gemeinsame übergeordnete Aufsichtsbehörde als sog. Landesmittelbehörde: die Bezirksregierungen. So wie diese also für schulische Bereiche zuständig sind, überwachen sie auch die Verwaltungsarbeit auf den anderen Gebieten. Die Bezirksregierungen stellen also quasi die „Schnittmenge“ (fast) aller Bereiche dar.<sup>146</sup>

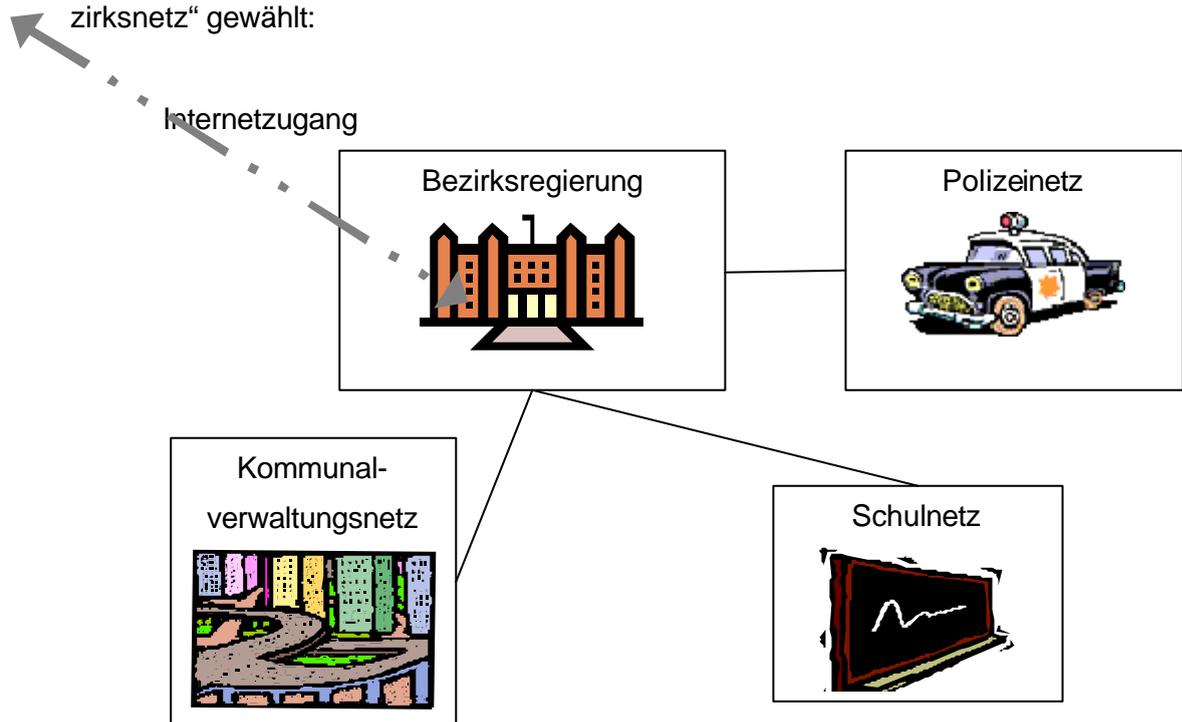
---

<sup>145</sup> z.B. über die zentrale Zuweisung von IP Adressen; s. hierzu RRNZ (2001), SCHÄFER (2003), RIGGERT (2002), KERSTEN (1995) u.a.

<sup>146</sup> Diejenigen, die auf dieser Ebene noch nicht mit erfasst sind, wie z.B. die Justizbehörden, werden aber in der nächst höheren Strukturebene einbezogen.

## 11.5 Bezirksregierungen bzw. Regionen

Diese vielen Einzelnetze werden daher zusammengefasst zu einem größeren Netzbereich (Mittlere Netzebene), dessen Gestaltung sich z.B. nach der Zuordnung zu den Bezirksregierungen oder nach regionalen Kriterien richten kann. Die Ausrichtung regionaler Art brächte den Vorteil mit sich, dass auch diejenigen Behörden / Schulen und die ihnen zuzuordnenden Kleinnetze mit in die nächst größere Organisationsstruktur einbezogen werden, die keiner Bezirksregierung organisatorisch zugerechnet werden können (z.B. Justizbehörden, private Grundschulen usw.). Da die Organisationshierarchie jedoch noch immer die Bezirksregierungen vorsieht, wird für die Skizzierung einer mittleren Netzebene auch die Bezeichnung „Bezirksnetz“ gewählt:



**Abbildung 14: Skizze Bezirksnetze – mittlere Netzebene**

Zusammenfassung der unter 11.1.2 beschriebenen Kleinnetze von Schulen und organisatorisch der Aufsicht der Bezirksregierungen zugeordneten Verwaltungsbehörden zum regionalen Netzwerk. In den Bezirksregierungen laufen Kommunikationswege zusammen, hier werden zentral Daten und Anwendungen zur Verfügung gestellt, ebenso zentral Administrationsleistungen erbracht usw.

(Abb. erstellt durch Verf.)

Die solchermaßen miteinander verbundenen Netze unterschiedlicher Verwaltungszweige haben durch die entstehenden „Überschneidungen“ innerhalb der Bezirksregierungen die Möglichkeiten lückenloser Kommunikation (z.B. durch eigenes Intranet-mailing), allerdings auch jeweils von anderen abgeschottete Bereiche mit sensiblen Daten, die lediglich dem berechtigten Personenkreis zugänglich sind.

Wesentlich erscheint, dass die Berechtigungen auch abhängig sind von Hierarchien und Funktionen und dem jeweils damit verbundenen Informationsbedarf (der Englischlehrer einer Schule hat einen weit geringeren Informationsbedarf über vorhandene Mittel zur Bestellung von Unterrichtsmaterial als der Haushälter der Bezirksregierung, der für weitreichendere Planungen für eine Vielzahl von Schulen zuständig ist). Die zu setzenden Berechtigungen müssen demzufolge auch in Abhängigkeit zum jeweiligen Informationsbedarf gesehen werden, was wiederum für die zentrale Entwicklung landesweiter Vorgaben spricht. Es ist bereits frühzeitig zu planen, welcher User in welchen Bereichen welchen Informationsbedarf hat und wer damit auch bereichsübergreifende Berechtigungen erhält. Dazu ein Beispiel:

Abschreibungskommissionen in den Verwaltungsbehörden entscheiden über die „Vernichtung“ von Geräten, u.a. PCs und IuK-Technik im Allgemeinen. Jede Behörde muss also ihren eigenen Bestand kennen, der jeweils zuständige Verwaltungsmitarbeiter Zugriff auf diese seine eigenen Daten haben.

Innerhalb der Bezirksregierungen wird koordiniert, ob und wo die für einen Verwaltungszweig nicht mehr nutzbaren Geräte eventuell doch noch einer adäquaten Nutzung zugeführt werden können. So werden für den hochtechnisierten Bereich einer polizeitechnischen Dienststelle unterdimensionierte PCs durchaus noch brauchbar für andere Verwaltungsbereiche sein und nach dort verlagert werden können. Der zuständige Sachbearbeiter der Bezirksregierung braucht also weiter gefächerte Informationen,

auf die er durch seine Berechtigungen im Gesamtnetz jederzeit Zugriff haben sollte. So werden Informationen dort erhoben, wo sie benötigt werden, Meldewege verkürzt, Kosten eingespart und Effizienz gefördert. Dies aber lässt sich nur dann realisieren, wenn es tatsächlich zu einer derartigen Vernetzung der Regionen kommt. Dabei ist es unerheblich, ob es sich um fünf mittlere Netzebenen handelt (derzeit fünf Bezirksregierungen in NRW), oder ob – den aus der Presse zu entnehmenden aktuellen politischen Diskussionen über eine eventuelle Neustrukturierung der Verwaltungen folgend – nur drei Bereiche gebildet werden. Die Anzahl der aufzubauenden Netzwerke hat letztlich keine Auswirkungen auf deren Struktur und Vorgaben.

## **11.6 Zusammenfassung zum Landesnetz NRW**

Die Bezirksregierungen verfügen somit jede über ihr eigenes umfassendes Netz. Damit ist die Kommunikation zwischen den beteiligten Behörden / Schulen, die der Mittleren Netzebene der Bezirksregierungen angehören, per Intranet möglich geworden. Diese Mittleren Netzebenen der regionalen Bereiche werden wiederum miteinander verbunden zur Oberen Netzebene, dem gesamten Landesverwaltungsnetz. So entsteht das in Abb. 11 eingangs dargestellte umfassende Netz unter Einbeziehung aller Ministerien und unter „Herrschaft“ des Landes NRW / der Landesregierung. Von diesem Netz aus sind die sichere Kommunikation und sicheres Surfen im Internet für alle Angehörigen der Verwaltung nach Maßgabe ihrer jeweiligen Berechtigung möglich.<sup>147</sup>

---

<sup>147</sup> In letzter Konsequenz kann eine solche Netzstruktur wegweisend sein. Losgelöst von dem Gedanken, dass in den meisten Verwaltungsbereichen die Kommunal- bzw. Länderhoheit besteht, kann dennoch ein solches Netz auch auf bundesdeutsche Ausdehnung, letztendlich sogar auf ein europäisches Netzwerk übertragen werden.

Außer den Bezirks-Regierungs-Netzen werden in das Landesverwaltungsnetz, wie in Abb. 11 skizziert, auch die in den justiz- und finanzministeriellen Bereichen einzurichtenden Netze integriert, so dass es ein allumfassendes Netzwerk mit entsprechenden Schnittstellen gibt, die landesweit miteinander arbeiten können.

Der Lehrer / der Polizist / der Sachbearbeiter für Hundesteuer, der sich an seinem PC in seiner Schule / Wache / Dienststelle einloggt, kann auf alle Daten zurückgreifen, für die er eine Berechtigung hat und die in der Struktur der Netze für ihn persönlich oder für alle Nutzer freigegeben sind. Das hat zur Konsequenz, dass Informationen eine Vielzahl von Berechtigten auf schnellstem Wege erreichen und vorhandene Daten mehrfach genutzt, aber nur einmal zentral vorgehalten werden können. (s. hierzu Kap. 11.4 und 11.5).

Dennoch ist – neben der Zentralisierung der technischen Wartung – auf möglichst dezentralisierte Verantwortlichkeit und Selbstverwaltung zu achten. Hier sind insbesondere haus- und buchhalterische Elemente, Personalsachen und interne Abläufe zu nennen und abzubilden.<sup>148</sup> Sowohl Beschaffungsfragen als auch Personalpolitik, sowohl Werbungsaspekte als auch Verwaltungsleistungen, sowohl Fach- als auch Dienstaufsicht gilt es mit technischer Unterstützung auf der jeweiligen Ebene, immer bezogen auf den erforderlichen Informationsbedarf, zu ermöglichen. Nur so kann es mit möglichst maximaler Zentralisierung zu einer gleichzeitig maximalen Selbstverantwortlichkeit jeder Ebene kommen.

Es ist aber auch darauf abzustellen, die Transparenz der Verwaltung zu optimieren, dem Bürger real die Chance zu geben, die Wege, Entschei-

---

<sup>148</sup> Keine Verwaltung kann ohne eine gut durchdachte „work flow“-Komponente innerhalb ihrer Softwarelösungen wirklich effizient arbeiten. Ebenso sind Abläufe abzubilden wie z.B. Mitzeichnungsverfahren und Entscheidungsfindungsprozesse, die teils auch die Bereiche einer einzelnen Behörde resp. Schule verlassen, aber für sie bedeutsam sind.

dungen und Konsequenzen verstehen und sie damit auch akzeptieren zu können. Dem steht nicht entgegen, wenn einzelne Schulen sich in einem Landes-Datenpool bedienen und die für sie notwendigen Verwaltungsangaben dort erfragen können.

Allerdings setzt ein solchermaßen verwaltungsumspannendes Netz voraus, dass gerade den Aspekten der Sicherheit und des Datenschutzes besondere Aufmerksamkeit gewidmet wird. Wenn innerhalb eines großen Netzes der öffentlichen Verwaltung alle Verwaltungszweige vereint sind, ist für manche Bereiche mehr, für andere weniger der Zugriff aus anderen Verwaltungsbereichen zu verhindern.<sup>149</sup>

---

<sup>149</sup> Wenn z.B. die Grundschule A aus Aachen die Schülerzahlen, Muttersprachen und Altersstatistiken der Grundschule B eines vergleichbaren Bezirkes in Minden einsehen kann, ist dem sicherlich weniger entgegen zuhalten, als wenn Mitarbeiter der Mülldeponie C die Daten der erfolgten Festnahmen und Verhaftungen des Polizeipräsidiums Köln einsehen können. Dies wäre wiederum nicht tolerabel.

## 12 Resümee

Die landes-, bundes- und europaweiten Initiativen zur Vernetzung der Schulen und damit zur Befähigung der Schüler und Schülerinnen, sich in der Welt der Information und Kommunikation sicher zu bewegen, zeigen Erfolge. Allerdings ist das Land NRW in diesem Zusammenhang trotz aller investierter Mittel und trotz allen Engagements immer noch eher ein Entwicklungsland (s. hierzu Kap. 2). Dies aber hängt nicht nur zusammen mit den fehlenden Mitteln, sondern auch mit den Erfordernissen, vorhandenes Lehrpersonal entsprechend fortzubilden und diese Fortbildungsmaßnahmen zu finanzieren, zielgerichtet aufzubauen und zu realisieren (s. hierzu Frage 7 sowie Ergebnisse der EU-Studie). Schulen fühlen sich mit den Aufgaben, die mit der Nutzung moderner Technologie verbunden sind, allein gelassen. So äußern sich manche Befragungsteilnehmer außerordentlich kritisch. Damit ist eine frühe Chance zur Begeisterung der Betroffenen in den Schulen vertan. Es gilt, dieses Manko im Nachhinein aufzufangen.

Dies aber kann nur durch Nutzung mehrfacher, parallel laufender Wege geschehen:

1. Es müssen finanzielle Unterstützungen unterschiedlichster Art geleistet werden, was angesichts der knappen Haushaltslage kaum mehr möglich sein wird. Das ginge nur, käme es zu einem Umdenkungsprozess, der den bisherigen Schwächen in der Umsetzung entgegentritt, die Weiterentwicklung ökonomischer und effizienter gestaltet. **Die Lösung kann nur ein auf höchster Ebene initiiertes Projekt eines Gesamt-Verwaltungsnetzes sein**, in dem sich letztendlich auch die Schulen wieder finden werden, und zwar so, dass sie sowohl im Rahmen von Projektbeteiligungen mitbestimmen können als auch so, dass sie Gestaltungsfreiräume für ihre ganz speziellen Aufgabenzuschnitte ha-

ben werden, ebenso wie alle anderen Verwaltungszweige dies auch haben müssen.

2. Das bisherige Problem der Schulen, sich nur ansatzweise mit den Anforderungen des Datenschutzes und der Datensicherheit auseinandergesetzt zu haben, kann auf diese Weise ebenso aufgefangen werden, da durch die **begleitenden Fachleute auf Landesebene** ein Gesamtkonzept zu entwickeln ist, in das die Schulen integriert werden müssen. Allerdings werden auch die Schulen sich als Teil einer Gesamtnetzes an vorgegebene Regularien halten müssen, die manch einem zunächst als Einschränkung vorkommen, die jedoch, wenn sie hingenommen werden, den Umgang mit den Möglichkeiten des Netzes erleichtern und zur Sicherheit beitragen. Und auch die Frage, welches Betriebssystem genutzt wird, welche firewalls wo installiert werden, ist dann nur noch auf höchster Ebene zu entscheiden, zu finanzieren, zu realisieren.
3. Durch ein Netz, das die gesamte Landesverwaltung umfasst, sind **wesentliche Teile der Administration auf eine landesweite Ebene verlagert**. Die verbleibenden Aufgaben innerhalb der schulischen Subnetze (vgl. Kap. 11) können durch Lehrer der einzelnen Schulen erfüllt werden. Das aber setzt wiederum voraus, dass es zu einer zentralen Aus- und Fortbildung kommt, die sich an den Erfordernissen orientiert: Lehrer mit Administrationaufgaben erhalten spezielle Schulungen, andere lernen das Netz zu nutzen und im Sinne ihrer Schüler und ihres Unterrichts dessen Chancen zu erkennen. **Zielgerichtete und zielgruppenorientierte Fortbildung kann nicht in der Organisationsmacht und Entscheidungskompetenz der Schulen selbst liegen, sie muss zentral als Planungsaufgabe verstanden und angenommen werden**. Damit können die Defizite, die die Befragung an Schulen ergeben haben, aufgearbeitet und ausgeräumt werden.

Der technische Fortschritt ist ebenso wenig aufzuhalten wie die gesellschaftliche Entwicklung, beide bedingen einander, beide wirken aufeinander. Damit ist es für alle Lebensbereiche, somit auch für alle zum Bereich der Bildung gehörenden Institutionen und Personen, wesentlich, sich in diese Entwicklungsschritte einzureihen, nicht etwa unkritisch mit dem Strom zu schwimmen, aber fördernd, nicht bremsend, und offen, nicht gehemmt an der Gesamtentwicklung Teil zu haben und mitzuwirken.

## 13 Anhang

### 13.1 Auszug aus Web.de Portal v. 30.04.2003:

WEB.DE Portale – Internet

Seite 1 von 1

Wissenswertes rund um's Internet: Neuigkeiten, Aktuelles, Hintergrundberichte und Dienste



Das WWW feiert seinen zehnten Geburtstag  
Karlsruhe (WEB-DE) - Am 30. April 1993 gab das Europäische Labor für Teilchenphysik in Genf den von Tim Berner-Lee entwickelten WWW-Standard zur Nutzung frei. Hyperlinks verknüpfen seitdem die Daten.

Die Erfindung des Briten hat wie kaum eine technische Entwicklung zuvor Kultur und Gesellschaft verändert. Die Buchstaben "WWW" sind mittlerweile zu einem Synonym für das Internet geworden.

Dass es sich dabei im Grunde genommen um eine Kommerzialisierung! einer Militärtechnologie handelt, ist vielen Anwendern hingegen nicht bekannt. Ebenfalls wird oft vergessen, dass das Verfahren für den Datenaustausch über das weltweite Netz, das TCP/IP-Protokoll, bereits seit über 20 Jahren als Standard besteht.

Lesen Sie dazu auch:

- Hintergrund: Das TCP/IP-Protokoll

## 13.2 München rüstet (fast) mit Linux aus

WEB.DE Portale - Computer – Betriebssysteme



### Betriebssysteme

#### München versetzt Microsoft mit Linux-Votum einen Stich [zurück] ins Herz

München (dpa) - Auf den 30-Millionen-Euro-Auftrag der Stadt München, die städtischen Personal Computer mit neuer Software auszustatten, war Microsoft nicht unbedingt angewiesen. Rund sieben Milliarden Euro Umsatz machte der Softwaregigant allein im vergangenen Geschäftsquartal, da fällt die Ausstattung von 14 000 PCs nicht so sehr ins Gewicht. Im Prestige-Wettkampf gegen die Open-Source-Bewegung hat die Niederlage für Microsoft in München trotz des vergleichsweise geringen Vertragsvolumens jedoch eine hohe symbolische Bedeutung: Die Münchner Ratsversammlung hat mit ihrem Votum für das freie Betriebssystem Linux und OpenOffice dem weltgrößten Softwarekonzern einen Stich mitten ins Herz versetzt.

Die Wettbewerber von Microsoft triumphierten nach der Entscheidung des Stadtrats: «Durch diesen Entschluss setzt München ein Zeichen für alle Kommunen sowie den Mittelstand, sich aus der Umklammerung eines Monopols zu befreien», sagte Martin Häring, Marketing-Direktor der Sun Microsystems GmbH. Der Markt habe verstanden, dass Offenheit der zentrale Schlüssel für zukünftige Innovation und fairen Wettbewerb sei. Richard Seibt, Vorstandsvorsitzender der SuSE Linux AG, sprach sogar von einer «historischen Entscheidung» der Ratsversammlung der bayerischen Landeshauptstadt. «Was in der großen Weltpolitik der Fall der Berliner Mauer war, das wird dieses Votum in unserer Branche sein.»

Selbst wenn man einen großen historischen Vergleich scheut, dann ist vielen Beobachtern dennoch klar, dass Microsoft künftig in Schwierigkeiten kommen kann. Insbesondere das Office-Programm, bislang die «Cash-Cow» von Microsoft, wird künftig nicht mehr zu den hohen Preisen vermarktet werden können wie bisher. Das hatte die Konzernzentrale in Redmond schon erkannt und wenige Stunden vor der Entscheidung in München die Office-Preise weltweit um 15 Prozent gesenkt.

Microsoft muss nun befürchten, dass das Beispiel München Schule macht. Nachdem die Stadt Schwäbisch Hall sich als erste Kommune Deutschlands für eine Microsoft-freie Computerlösung entschieden hatte, trafen bereits Anfragen aus aller Welt ein, wie man denn konkret ohne die Programme des Software-Marktführers auskommen kann. Dieser Effekt dürfte sich jetzt in einem wesentlich größeren Ausmaß wiederholen.

Microsoft-Sprecher Hans-Jürgen Croissant glaubt nicht an diesen Domino-Effekt: «Wir sind der Überzeugung, dass unser Angebot das wirtschaftlichste war.» Microsoft sehe in der Stadtverwaltung München weiterhin einen wichtigen Partner und Kunden, mit dem man etwa im Bildungsbereich gut zusammen arbeite.

Jürgen Gallmann, Geschäftsführer von Microsoft Deutschland, muss seinem obersten Chef in den USA, Steve Ballmer, jetzt aber erklären, warum ausgerechnet München, der Sitz der deutschen Microsoft-Niederlassung, auf Windows XP und Microsoft Office verzichten will. Schließlich hatte CEO Ballmer für ein Gespräch mit dem Münchner Oberbürgermeister Christian Ude (SPD) eigens seinen Urlaub in der Schweiz unterbrochen. Und Microsoft-Gründer Bill Gates hatte zum 20. Jahrestag der Gründung von Microsoft Deutschland noch nette Worte von Bayerns Ministerpräsident Edmund Stoiber gehört. Im Vorfeld der Entscheidung hatte Microsoft jedoch bereits von ideologisch geprägten Vorurteilen gesprochen und sich über einen unfairen Wettbewerb beklagt, da IBM und SuSE ihr Angebot in Kenntnis der Microsoft-Offerte noch einmal verändern durften.

Ob in München tatsächlich das Anbieter-Duo IBM und SuSE zum Zuge kommen wird, steht noch nicht fest. Theoretisch könnten auch andere Anbieter wie HP oder Fujitsu-Siemens berücksichtigt werden. «Jetzt beginnt die Arbeit, in einem Feindesign die Dinge festzuhalten, die der Stadt wichtig sind», sagt SuSE-Chef Seibt. Außerdem müsse das Vertrauen der Mitarbeiter gewonnen werden, die an den neuen Computern arbeiten werden.

© dpa - Meldung vom 28.05.2003 16:59 Uhr

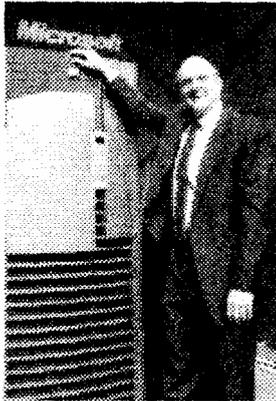
<http://portale.web.de/Computer/Betriebssystem/7msgid=3123578>

28.05.2003

Sie sind hier: WEB.DE > Computer > Software > Meldung

## Software

### Microsoft gibt Münchner Stadtverwaltung Rabatt



Hamburg/München (dpa) - Microsoft hat bei der Ausstattung der städtischen Verwaltungen in Deutschland nach einem Bericht der «Financial Times Deutschland» einen Punktsieg gegen den Konkurrenten Linux erzielt. Die Fraktionssprecherin der SPD im Münchner Stadtrat habe bestätigt, dass die Verwaltung jetzt überraschend das Microsoft- Angebot zur Ausrüstung der Münchner Stadtverwaltung empfiehlt, schreibt die Zeitung. Zuvor hatte die Stadtverwaltung unter anderem aus Kostengründen die Ausstattung mit Linux- Lösungen favorisiert.

Microsoft-Chef Steve Ballmer persönlich hatte im April seinen Urlaub in der Schweiz unterbrochen, um Oberbürgermeister Christian Ude von einer Entscheidung für Microsoft zu überzeugen. Der weltgrößte Softwarekonzern soll zuvor einen Rabatt von 15 Prozent eingeräumt haben, um seinen Konkurrenten Linux auszustechen. Nach Informationen der «FTD» bereitet jedoch auch der Linux-Dienstleister inzwischen ein neues Angebot vor. Die abschließende Entscheidung wolle der Stadtrat am 28. Mai treffen.

München wäre die erste deutsche Großstadt gewesen, die auf das konkurrierende Linux-Betriebssystem umsteigt. Der Entscheidung in München wird Symbolcharakter für die anstehende Ausrüstung von kommunalen Verwaltungen zugesprochen. Auch der Deutsche Bundestag will künftig auf das freie Betriebssystem Linux setzen.

© dpa - Meldung vom 21.05.2003 19:29 Uhr

### 13.3 Killing-my-software – Text des MP3-Files

(Melodie von "Killing me softly)

I tried to run my programs  
With windows ninety-five.  
It makes six recommended  
But I've got only five!  
So there it was my system  
Completely obsoleted  
Typing path-names with my fingers,  
Cursing out loud at my mouse.

Refr:  
Killing my software with windows,  
killing my software with windows  
needing more disk-space with windows  
needing new programs

with windows!

## 13.4 Lovesan

**tecChannel! : Druckversion der News**



tecChannel.de - News vom 15.04.2003

### Lovesan: Microsoft räumt Fehler ein

(tecChannel.de) Nach der rasanten Verbreitung des Computerwurms W32.Lovesan bzw. W32.Blaster hat Microsoft Fehler eingeräumt. Experten hatten dem Softwareproduzenten vorgehalten, nicht offensiv genug auf die Sicherheitslücken in ihren Programmen hingewiesen zu haben. Der Kontakt zu den privaten Nutzern soll nun verbessert werden. "Daran arbeiten wir. Da sind Fehler gemacht worden", sagte Thomas Baumgärtner, Pressesprecher von Microsoft Deutschland, laut "tagesschau, de". Die Kommunikation müsse intensiviert werden. "Die Gratwanderung besteht darin, dass man nicht mit erhobenem Zeigefinger und schulmeisterlich dasteht", so Baumgärtner. Nach vorsichtigen Schätzungen sollen von dem seit Montagnacht kursierenden Wurm inzwischen rund 120.000 bis 150.000 Computer vorwiegend von Privatanwendern attackiert worden sein. Andere Beobachter gehen sogar von weltweit mehr als 200.000 betroffenen Systemen aus.

Der Wurm verbreitet sich über das Internet und nutzt eine Schwachstelle in den Microsoft-Betriebssystemen Windows NT, 2000 und XP. Seit Juli bietet Microsoft einen entsprechenden Schutz zum Herunterladen an. Details zur Verbreitung des Wurmes finden Sie in diesem Beitrag.

Die wichtigsten Aspekte zum Thema Sicherheit finden Sie auf über 230 Seiten in unserem tecCHANNEL-Compact "IT-Security", das Sie online zum Vorzugspreis von 8,90 Euro bestellen oder für 4,90 Euro als PDF downloaden können. In unserem Premium-Bereich gibt es diese und weitere tecCHANNEL-Compact-Ausgaben kostenlos zum Download.

(dpa/fkh)

Im Internet finden Sie diese Meldung auf [www.tecchannel.de](http://www.tecchannel.de) unter der URL:

<http://www.tecchannel.de/news/20030815/thema20030815-11544.html>

©1999-2000 idg interactive

<http://www.tecchannel.de/cgi-bin/printnews/printnews.pl?id=11544>

28.08.2003

## 13.5 Sobig F

WEB.DE Portale > Internet

Meldung vom 20.08.2003 17:20 Uhr

### BSI warnt vor neuem Computer-Wurm «Sobig.F»

Hamburg (dpa) - Das Bundesamt für Sicherheit in der Informationstechnik hat am Dienstag erneut vor einem neuen gefährlichen Computer-Wurm gewarnt. Kaum hat sich die Aufregung um den vergangene Woche kursierenden Wurm «Lovesan» etwas gelegt, wurde bereits ein neuer Schädling in Umlauf gebracht.

Eine Variante des bereits bekannten «Sobig»- Wurms habe innerhalb von nur wenigen Stunden bereits Tausende Rechner infiziert, teilte das BSI mit, «Sobig.F» verbreitet sich seit Dienstag per E-Mail mit großer Geschwindigkeit und wird nach einem Doppelklick auf den Dateianhang aktiviert. Erstmals war ein Sobig-Wurm vor etwas mehr als einem halben Jahr im Internet in Umlauf gebracht worden.

Eine entsprechende «Sobig.F»-E-Mail lasse sich nur schwer erkennen, da die Namen der Anhänge sowie auch die des Absenders variieren können, sagte Frank Felzmann vom BSI. Sie sind unter Umständen auch als Antwort von einem Bekannten getarnt und enthalten im Textteil die Aufforderung «see attached file for details». Nach einem Doppelklick auf den Dateianhang installiert der Schädling jedoch ein so genanntes Trojanisches Pferd auf dem Rechner. Darunter versteht man eine manipulierte Software, die den Zugriff von Außen auf die Daten des Rechners ermöglicht. Das BSI warnt dringend davor, entsprechende Datei-Anhänge von eingehenden E-Mails ungeprüft zu öffnen.

Seit Montag ist auch eine neue Variante des Computer-Wurms «Lovesan» im Internet unterwegs. Anders als bei Computer-Würmern sonst üblich macht die «Lovesan»-Variante «D» jedoch ihren Vorgänger unschädlich und versucht, das nötige Microsoft-Sicherheits-Patch zu installieren. Die Installationsroutine laufe jedoch in vielen Fällen fehlerhaft ab. IT-Sicherheitsexperten raten deshalb den betroffenen Nutzern von Windows XP und 2000, sich vor dem «Anti-Wurm», auch «Welchia» oder «Nachi» genannt, mit aktueller Sicherheitssoftware zu schützen. Die von «Lovesan» am vergangenen Wochenende geplante Attacke auf die Server von Microsoft hatte der weltgrößte Softwarekonzern noch rechtzeitig erfolgreich abwenden können.

Alle Rechte vorbehalten. Vervielfältigung nur mit Genehmigung des Urhebers und der WEB.DE AG

<http://portale.web.de/Internet/>

## Computer-Wurm «Sobig.F» schlägt alle Rekorde

Hamburg (dpa) - Der erstmals am Dienstag in Umlauf gebrachte neue E-Mail-Wurm «Sobig.F» hat am Donnerstag bereits einen Geschwindigkeitsrekord aufgestellt. Das Moskauer IT-Sicherheitsunternehmen Kaspersky Lab sprach sogar von der «größten Epidemie» in den vergangenen eineinhalb Jahren. In seiner rasanten Verbreitung übertrifft er nach Einschätzung von Experten bislang bekannte Schädlinge um das Zehnfache. «Sobig.F» soll bereits Hunderttausende Windows-Rechner befallen haben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte erstmals am vergangenen Dienstag vor dem gefährlichen Computer-Wurm gewarnt.

«Hunderttausende Sobig-F-Kopien geistern nun durch das Internet, so dass bei einigen Unternehmen das E-Mail-System bereits kollabiert ist», sagte Gernot Hacker, Technik-Experte bei dem Münchner Anti-Virensoftware-Hersteller Sophos. Wegen der hohen Verbreitungsgeschwindigkeit vermutet das Unternehmen, dass der Wurm so genannte Spam-Technologie zum Massenversand eingesetzt hat.

«Sobig.F» ist eine Variante des Sobig-Wurms, der vor rund einem halben Jahr im Internet in Umlauf gebracht worden war. Anders als «Lovesan», der vor einer Woche weltweit für Aufregung gesorgt hatte, verbreitet sich «Sobig.F» über E-Mail und wird erst durch einen Doppelklick des Empfängers auf den Dateianhang aktiviert. Die E-Mails ließen sich jedoch nur schwer erkennen, da die Namen des Absenders gefälscht sind, warnt das BSI. Die Mail enthält im Textteil die Aufforderung «see attached file for details». Während «Lovesan» auf den befallenen Computern in der Regel keine nachhaltigen Schäden hinterlässt, öffnet «Sobig.F» sie für einen ungehinderten Angriff von außen. Betroffen sind alle gängigen Windows-Betriebssysteme. Bei Öffnen des Anhangs installiert der Schädling ein so genanntes Trojanisches Pferd auf dem Rechner. Trojanische Pferde sind manipulierte Programme, die den Zugriff von außen auf die Daten des Rechners ermöglichen. Alle führenden Sicherheitsunternehmen warnen dringend davor, Anhänge von eingehenden E-Mails ungeprüft zu öffnen.

Alle Rechte vorbehalten. Vervielfältigung nur mit Genehmigung des Urhebers und der WEB.DE AG © dpa  
<http://portale.web.de/Internet/>

[http://portale.web.de/popup/news/drucken/7msg\\_id=3537022&cat=Internet&pfad=I...](http://portale.web.de/popup/news/drucken/7msg_id=3537022&cat=Internet&pfad=I...)  
25.08.2003

## 13.6 Datenschutzerläuterungen der Firma Intersport

[Persönliche Daten](#)    INTERSPORT freut sich über Ihren Besuch  
[Nutzungsdaten](#)    auf unserer Internet-Seite sowie über Ihr  
[Zugriffsdaten](#)    Interesse an unserem Unternehmen.

Wir nehmen den Schutz Ihrer privaten Daten ernst und möchten, dass Sie sich beim Besuch unserer Internet-Seiten wohl fühlen.

Für die Beachtung der Datenschutz-Grundsätze sorgt der betriebliche [Datenschutzbeauftragte](#).

Sie können sich auf allen INTERSPORT-Internet-Seiten anonym bewegen. Falls wir persönliche Daten aus Ihrem Besuch der Internet-Seiten erheben, verarbeiten oder nutzen wollen, legen wir es offen.

Aus dem allgemeinen Persönlichkeitsrecht wird das Recht des Einzelnen auf informationelle Selbstbestimmung abgeleitet. Sein Schutz wird durch Rechtsvorschriften - z.B. durch das Bundesdatenschutzgesetz und Teledienstschutzgesetz begründet.

Unser Internet-Auftritt ist im Einklang mit den gesetzlichen Datenschutzbestimmungen gestaltet.

Die Verwendung folgender Bereiche unserer Internet-Seiten ist Benutzern nur mit der Anerkennung dieser Datenschutzbestimmungen

gestattet:

- [Kontaktformular](#)
- Gewinnspiele

Wir respektieren Ihre Datenschutzrechte, insbesondere Ihr Auskunftsrecht über gespeicherte Daten.

Unsere Mitarbeiterinnen und Mitarbeiter haben Verschwiegenheitspflichten zu wahren.

Unsere Webseiten können Links zu anderen Anbietern enthalten, auf die sich unsere Datenschutz-Grundsätze nicht erstrecken.

[top](#)

## **Persönliche Daten**

**Definition:** Einzelangaben (Daten), die sich unmittelbar auf eine natürliche Person beziehen, die eine Person bestimmbar machen oder die sich auf eine Person zurückführen lassen.

**Verwendung:** Wenn wir persönliche Daten aus Ihrem Besuch erheben, verarbeiten oder nutzen wollen, informieren wir Sie.

Sie entscheiden, welche persönlichen Daten wir erhalten und wozu wir sie verarbeiten und nutzen dürfen. Meist werden solche Angaben der Erstellung eines von Ihnen gewünschten Produkt- oder Serviceangebotes dienen.

Die unternehmensinterne Nutzung zu Werbezwecken kann erfolgen, sofern Sie ihr nicht widersprochen haben.

Dann werden die Angaben entweder an den von Ihnen gewählten Mitarbeiter weitergereicht oder nach spätestens drei Monaten gelöscht.

**Gewährleistung:** Wir verkaufen oder vermieten keinerlei personenbezogene Daten an Personen oder Stellen außerhalb der INTERSPORT eG - auch nicht aus Benutzergruppen oder E-Mail-Listen.

Sie haben jederzeit die Möglichkeit, über unseren [Datenschutzbeauftragten](#) eine Änderung oder Löschung Ihrer personenbezogenen Daten durchzuführen.

Wir beachten die durch Datenschutz- und Wettbewerbsrecht gezogenen Grenzen.

[top](#)

## **Nutzungsdaten**

**Definition:** Personenbezogene Daten, die anfallen können, um die Inanspruchnahme von Telediensten, d. h. den Besuch von INTERSPORT Webseiten zu ermöglichen.

**Verwendung:** Wenn wir - zur Verbesserung des individuellen Produktangebotes und unseres Service - Nutzungsdaten aus Ihrem Besuch von INTERSPORT Webseiten verwenden und mit

Ihren Kundendaten zusammenführen wollen, holen wir im Zuge des Internet-Dialogs hierzu Ihre ausdrückliche Einwilligung ein. Wollen Sie kein Einverständnis geben, so können Sie jeden Dialog unbeobachtet fortsetzen, abbrechen oder beenden.

**Gewährleistung:** Wir verkaufen oder vermieten keinerlei personenbezogene Daten an Personen oder Stellen außerhalb der INTERSPORT eG - auch nicht aus Benutzergruppen oder E-Mail-Listen.

Sie haben jederzeit die Möglichkeit, über unseren [Datenschutzbeauftragten](#) eine Änderung oder Löschung Ihrer personenbezogenen Daten durchzuführen.

Wir beachten die durch Datenschutz- und Wettbewerbsrecht gezogenen Grenzen.

[top](#)

### **Zugriffsdaten**

**Definition:** Nicht personenbezogene Daten über das Anfordern (Download) einer Datei.

**Erklärung:** Bei jeder Anforderung einer Datei aus unserem Download-Angebot werden Zugriffsdaten gespeichert.

Jeder Datensatz besteht aus:

- der Seite, von der aus die Datei angefordert wurde

- dem Namen der Datei
- einer Beschreibung des Typs des verwendeten Webbrowsers
- Datum und Uhrzeit der Anforderung
- der übertragenen Datenmenge
- dem Zugriffsstatus (Datei übertragen, Datei nicht gefunden etc.)
- auf die Speicherung Ihrer Rechneradresse (IP-Nummer) wird verzichtet

**Verwendung:**

Die gespeicherten Daten werden ausschließlich zu statistischen Zwecken ausgewertet.

**Gewährleistung:**

Eine Weitergabe an Dritte, auch in Auszügen, findet nicht statt. Wir berichtigen und vervollständigen gespeicherte Daten jeweils, sobald uns eine Veränderung bekannt wird. Bei Bedarf verständigen wir auch Datenempfänger davon.

Gespeicherte Daten löschen wir, wenn die gesetzliche oder vertragliche Aufbewahrungsfrist abgelaufen ist oder falls die Daten nicht mehr benötigt werden.

[top](#)

### 13.7 Auszug aus EU-Richtlinie RL 95/46, Erwägungsgründe:

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 100 a,

auf Vorschlag der Kommission [1], nach Stellungnahme des Wirtschafts- und Sozialausschusses [2], gemäß dem Verfahren des Artikels 189 b des Vertrags [3], in Erwägung nachstehender Gründe:

(1) Die Ziele der Gemeinschaft, wie sie in dem durch den Vertrag über die Europäische Union geänderten Vertrag festgelegt sind, bestehen darin, einen immer engeren Zusammenschluß der europäischen Völker zu schaffen, engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossenen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.

(3) Für die Errichtung und das Funktionieren des Binnenmarktes, der gemäß Artikel 7 a des Vertrags den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleisten soll, ist es nicht nur erforderlich, daß personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können, sondern auch, daß die Grundrechte der Personen gewahrt werden.

(4) Immer häufiger werden personenbezogene Daten in der Gemeinschaft in den verschiedenen Bereichen wirtschaftlicher und sozialer Tätigkeiten verarbeitet. Die Fortschritte der Informationstechnik erleichtern die Verarbeitung und den Austausch dieser Daten beträchtlich.

(5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Artikel 7 a des Vertrags ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschaftsrechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt

wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaats durchführen zu können.

(6) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Telekommunikationsnetze in der Gemeinschaft erfordern und erleichtern den grenzüberschreitenden Verkehr personenbezogener Daten.

(7) Das unterschiedliche Niveau des Schutzes der Rechte und Freiheiten von Personen, insbesondere der Privatsphäre, bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaats in das Gebiet eines anderen Mitgliedstaats verhindern. Dieses unterschiedliche Schutzniveau kann somit ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und die Erfüllung des Auftrags der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden verhindern. Dieses unterschiedliche Schutzniveau ergibt sich aus der Verschiedenartigkeit der einzelstaatlichen Rechts- und Verwaltungsvorschriften.

(8) Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerlässlich. Insbesondere unter Berücksichtigung der großen Unterschiede, die gegenwärtig zwischen den einschlägigen einzelstaatlichen Rechtsvorschriften bestehen, und der Notwendigkeit, die Rechtsvorschriften der Mitgliedstaaten zu koordinieren, damit der grenzüberschreitende Fluß personenbezogener Daten kohärent und in Übereinstimmung mit dem Ziel des Binnenmarktes im Sinne des Artikels 7 a des Vertrags geregelt wird, läßt sich dieses für den Binnenmarkt grundlegende Ziel nicht allein durch das Vorgehen der Mitgliedstaaten verwirklichen. Deshalb ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich.

(9) Die Mitgliedstaaten dürfen aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen. Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an. Innerhalb dieses Spielraums können unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann.

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern

muß im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

(11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

## **13.8 Auszug aus BSI-Grundschutzhandbuch, hier: Kap. 1.4**

### **1.4 Kurzdarstellung vorhandener Bausteine**

In der nachfolgenden Übersicht werden die im IT-Grundschutzhandbuch vorhandenen Bausteine kurz skizziert. Sie bietet einen kompakten Überblick über den Umfang der erarbeiteten Maßnahmenempfehlungen des IT-Grundschutzhandbuchs.

#### **3.0 IT-Sicherheitsmanagement**

Das Kapitel zeigt einen systematischen Weg auf, wie ein funktionierendes IT-Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann.

#### **3.1 Organisation**

In diesem Baustein werden die für die IT-Sicherheit grundlegend notwendigen organisatorischen Regelungen angeführt. Beispiele sind Festlegung der Verantwortlichkeiten, Datenträgerverwaltung und Regelungen zum Passwortgebrauch. Sie sind für jedes IT-System umzusetzen.

#### **3.2 Personal**

Der Baustein "Personal" beschreibt die Maßnahmen im Personalbereich, die zum Erreichen von IT-Sicherheit zu beachten sind. Beispiele sind Vertretungsregelungen, Schulungsmaßnahmen und geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern. Sie sind unabhängig von der Art der eingesetzten IT-Systems zu beachten.

#### **3.3 Notfallvorsorge-Konzept**

Hier wird eine Vorgehensweise dargestellt, wie ein Notfallvorsorge-Konzept erstellt werden kann. Dieser Baustein sollte insbesondere für größere IT-Systeme berücksichtigt werden.

#### **3.4 Datensicherungskonzept**

Dieser Baustein stellt dar, wie ein fundiertes Datensicherungskonzept systematisch erarbeitet werden kann. Dieser Baustein ist insbesondere für größere IT-Systeme oder IT-Systeme mit großem Datenbestand gedacht.

#### **3.5 Datenschutz**

Die Rahmenbedingungen für einen praxisgerechten Datenschutz und die Verbindung zur IT-Sicherheit über den IT-Grundschutz werden in diesem Baustein dargestellt. Das Kapitel Datenschutz wurde federführend vom Bundesbeauftragten für den Datenschutz (BfD) gemeinsam mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder erstellt und kann beim BfD abgerufen werden.

### **3.6 Computer-Virenschutzkonzept**

Ziel eines Computer-Virenschutzkonzeptes ist es, ein geeignetes Maßnahmenbündel zusammenzustellen, bei dessen Einsatz das Auftreten von Computer-Viren auf den in einer Organisation eingesetzten IT-Systemen verhindert bzw. möglichst früh erkannt wird, um Gegenmaßnahmen vornehmen zu können und mögliche Schäden zu minimieren.

### **3.7 Kryptokonzept**

Dieser Baustein beschreibt eine Vorgehensweise, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenen Daten wirkungsvoll durch kryptographische Verfahren und Techniken geschützt werden können.

### **3.8 Behandlung von Sicherheitsvorfällen**

Um die IT-Sicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen (Incident Handling) konzipiert und eingeübt zu haben. Als Sicherheitsvorfall wird dabei ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden anrichten können. Um Schäden zu verhüten bzw. zu begrenzen, sollte die Behandlung der Sicherheitsvorfälle zügig und effizient ablaufen.

#### **4.1 Gebäude**

Hier werden die Maßnahmen genannt, die in jedem Gebäude, in dem Datenverarbeitung stattfindet, zu beachten sind. Es sind Maßnahmen zur Stromversorgung, zum Brand- und Gebäudeschutz sowie organisatorische Maßnahmen wie die Schlüsselverwaltung.

#### **4.2 Verkabelung**

Im Baustein "Verkabelung" werden Maßnahmen empfohlen, die für die Verkabelung eines Gebäudes mit Versorgungs- und Kommunikationsleitungen relevant sind. Beispiele sind Brandabschottung von Trassen, Auswahl geeigneter Kabeltypen und Dokumentation der Verkabelung.

##### **4.3.1 Büroraum**

Im Kapitel "Büroraum" sind alle Maßnahmen zusammengefasst, die im Zusammenhang mit dem IT-Einsatz in einem Büro zu beachten sind. Beispiele sind: Geschlossene Fenster und Türen und die Beaufsichtigung von Fremdpersonen.

##### **4.3.2 Serverraum**

Hier werden die Maßnahmen genannt, die bei Nutzung eines Raumes, in dem ein Server (für IT-Systeme oder TK-Anlagen) aufgestellt ist, beachtet werden müssen. Beispiele sind: Vermeidung von Wasserleitungen, Klimatisierung, lokale unterbrechungsfreie Stromversorgung und Rauchverbot.

##### **4.3.3 Datenträgerarchiv**

Wird ein Raum als Datenträgerarchiv genutzt, so sind bestimmte Randbedingungen für die IT-Sicherheit einzuhalten. Diese werden als Maßnahmen für den IT-Grundschutz formuliert. Beispiele sind: Handfeuerlöscher, Verwendung von Sicherheitstüren und Rauchverbot.

#### **4.3.4 Raum für technische Infrastruktur**

Auch für Räume, in denen technische Infrastruktur installiert wird, wie im Eingangsraum für externe Kommunikationsleitungen, Verteilerraum, Niederspannungsverteilterraum, müssen im Sinne der IT-Sicherheit bestimmte Maßnahmen ergriffen werden, die in diesem Kapitel genannt werden.

#### **4.4 Schutzschränke**

Für die sichere Aufbewahrung von Datenträgern oder Hardware können Schutzschränke die Schutzwirkung von Räumen (Serverraum, Datenträgerarchiv) zusätzlich erhöhen. Ggf. kann ein spezieller Serverschrank auch als Alternative zu einem Serverraum eingesetzt werden. Die für die Beschaffung, die Aufstellung und die Nutzung eines Schutzschrankes erforderlichen Maßnahmen werden in diesem Baustein beschrieben.

#### **4.5 Häuslicher Arbeitsplatz**

In diesem Baustein werden die Maßnahmen beschrieben, die erforderlich sind, um einen häuslichen Arbeitsplatz mit einem adäquaten Sicherheitsstandard einzurichten, so dass dieser für dienstliche Aufgaben genutzt werden kann.

#### **5.1 DOS-PC (ein Benutzer)**

In diesem Baustein werden die Maßnahmen genannt, die beim Einsatz eines handelsüblichen PCs beachtet werden müssen, der standardmäßig nur von einem Benutzer betrieben wird. Beispiele sind: Passwortschutz, Einsatz eines Viren-Suchprogramms, regelmäßige Datensicherung.

#### **5.2 Unix-System**

Betrachtet wird ein IT-System unter dem Betriebssystem Unix oder Linux, das entweder ohne Verbindung zu anderen Rechnern oder als Client in einem Netz betrieben wird. Terminals oder PCs, die als Terminal betrieben werden, können angeschlossen sein. Hierzu werden sowohl organisatorische wie auch Unix-spezifische Maßnahmen genannt.

#### **5.3 Tragbarer PC**

Ein tragbarer PC (Laptop) erfordert gegenüber dem normalen PC zusätzliche IT-Sicherheitsmaßnahmen, da er aufgrund der mobilen Nutzung anderen Gefährdungen ausgesetzt ist. Beispiele für zusätzliche Maßnahmen sind: geeignete Aufbewahrung im mobilen Einsatz und der Einsatz eines Verschlüsselungsproduktes.

#### **5.4 PCs mit wechselnden Benutzern**

In diesem Baustein werden die Maßnahmen genannt, die beim Einsatz eines handelsüblichen PCs beachtet werden müssen, der standardmäßig von mehreren Benutzern betrieben wird. Beispiele sind: PC-Sicherheitsprodukt, Passwortschutz, Einsatz eines Viren-Suchprogramms, regelmäßige Datensicherung.

#### **5.5 PC unter Windows NT**

In diesem Baustein werden Maßnahmen genannt, die für nicht vernetzte PCs mit dem Betriebssystem Windows NT (Version 3.51 oder 4.0) erforderlich sind. Auf sicherheitsspezifische Aspekte einzelner Windows NT-Anwendungen wird nur am Rande eingegangen.

## **5.6 PC mit Windows 95**

Nicht vernetzte PCs mit dem Betriebssystem Windows 95 können als Stand-alone-Systeme bzw. als Clients in einem Netz für einen oder für mehrere Benutzer eingerichtet werden. Für beide Betriebsvarianten werden die erforderlichen Maßnahmen in diesem Baustein genannt.

## **5.99 Allgemeines nicht vernetztes IT-System**

Für die noch nicht im IT-Grundschutzhandbuch betrachteten IT-Systeme wie z. B. OS/2 kann der generische Baustein 5.99 angewendet werden.

## **6.1 Servergestütztes Netz**

In diesem Baustein werden die notwendigen Maßnahmen erläutert, die beim Betrieb eines servergestützten Netzes beachtet werden müssen. Diese Betrachtungen sind unabhängig von den Server- und Client-Betriebssystemen. Die bezüglich der Betriebssysteme zu ergreifenden Maßnahmen befinden sich in den spezifischen Bausteinen der Kapitel 5 und 6.

## **6.2 Unix-Server**

Es werden IT-Systeme betrachtet, die als Server in einem Netz Dienste anbieten und unter dem Betriebssystem Unix oder Linux betrieben werden. Für diese IT-Umgebung werden Maßnahmen genannt, die IT-Sicherheit ermöglichen. Diese Maßnahmen sind Unix-spezifisch und müssen durch Kapitel 6.1 ergänzt werden.

## **6.3 Peer-to-Peer-Netz**

Beschrieben wird, wie ein Peer-to-Peer-Netz für den IT-Grundschutz ausreichend sicher betrieben werden kann. Themen sind die Konzeption eines solchen Netzes unter Sicherheitsgesichtspunkten, Administrationsmöglichkeiten und funktionelle Einschränkungen. Grundlagen bilden die Betriebssysteme Windows für Workgroups 3.11, Windows 95 und Windows NT.

## **6.4 Windows NT Netz**

In diesem Baustein wird die Konzeption und der Betrieb eines sicheren Windows NT Netzes beschrieben. Hierbei handelt es sich überwiegend um Windows NT-spezifische Maßnahmen, die um die allgemeinen Maßnahmen aus Kapitel 6.1 ergänzt werden müssen.

## **6.5 Novell Netware 3.x**

Gegenstand dieses Kapitels ist ein Novell 3.x Netz in einer Client-Server-Funktionalität. Damit ist dieses Kapitel die betriebssystemspezifische Ergänzung des Kapitels 6.1 "Servergestütztes Netz". Behandelt werden die Installation, die Einrichtung, der Betrieb und die Revision von Novell Netware Servern.

## **6.6 Novell Netware 4.x**

Gegenstand dieses Kapitels ist ein Novell 4.x Netz in einer Client-Server-Funktionalität. Damit ist dieses Kapitel die betriebssystemspezifische Ergänzung des Kapitels 6.1 "Servergestütztes Netz". Die erforderlichen Maßnahmen für die Bereiche Installation, Einrichtung und Betrieb eines Novell 4.x Netzes werden beschrieben. Hierbei wird insbesondere auch auf den Verzeichnisdienst NDS (Novell Directory Services) eingegangen.

## **6.7 Heterogene Netze**

Mit Hilfe des Bausteins wird die Analyse und Weiterentwicklung eines bestehenden bzw. die Planung eines neuen heterogenen Netzes ermöglicht. Für einen sicheren Betrieb des heterogenen Netzes wird u. a. aufgezeigt, wie eine geeignete Segmentierung des Netzes vorgenommen wird, wie ein Netzmanagement-System geplant und umgesetzt wird und wie ein Audit und die Revision des Netzes erfolgen kann. Daneben werden Aspekte wie die redundante Auslegung von Netzkomponenten und Sicherung von Konfigurationsdaten im Rahmen der Notfallplanung behandelt.

## **6.8 Netz- und Systemmanagement**

Mittels eines Managementsystems kann eine zentrale Verwaltung aller in einem lokalen Netz angesiedelten Hard- und Softwarekomponenten durchgeführt werden. Für den erfolgreichen Aufbau eines Netz- und Systemmanagementsystems werden in diesem Baustein die erforderlichen Schritte beschrieben, beginnend mit der Konzeption über die Beschaffung bis hin zum Betrieb.

### **7.1 Datenträgeraustausch**

Beschrieben werden die Maßnahmen, die bei einem Datenträgeraustausch beachtet werden sollten. Technische Maßnahmen wie Verschlüsselung werden ebenso betrachtet wie die richtige Auswahl der Versandart. Die Maßnahmen zielen insbesondere auf den Fall, dass der Datenträgeraustausch regelmäßig stattfindet.

### **7.2 Modem**

Dargestellt werden in diesem Baustein Maßnahmen, die im Zusammenhang mit dem Einsatz eines Modems zu beachten sind. Dies sind insbesondere Callback-Mechanismen und Verschlüsselung. Auch Hinweise zur Absicherung der Fernwartung über Modem werden gegeben.

### **7.3 Firewall**

Die Vernetzung vorhandener Teilnetze mit globalen Netzen wie dem Internet erfordert einen effektiven Schutz des eigenen Netzes. Um dies mit Hilfe einer Firewall zu gewährleisten, bedarf es der Formulierung von Sicherheitszielen, die schließlich durch eine korrekte Installation und Administration der Firewall umgesetzt werden.

### **7.4 E-Mail**

Für eine sichere E-Mail-Kommunikation werden hier die erforderlichen Maßnahmen sowohl auf Seiten des Mailservers als auch auf Seiten des Mailclients aufgeführt. Außerdem werden die von den Benutzern einzuhaltenden Sicherheitsbestimmungen vorgestellt.

### **7.5 WWW-Server**

Ein WWW-Server ist ein IT-System, das über eine Informationsdatenbank WWW-Clients Dateien zur Verfügung stellt. Ein WWW-Client, auch Browser genannt, zeigt die Informationen eines WWW-Servers auf dem Benutzerrechner an. Die Sicherheit der WWW-Nutzung beruht auf der Sicherheit des WWW-Servers, des WWW-Clients und der Kommunikationsverbindung zwischen beiden. Die für eine sichere WWW-Nutzung erforderlichen Maßnahmen werden im Baustein WWW-Server beschrieben.

## **7.6 Remote-Access**

Um einem Benutzer entfernte Zugriffe (Remote Access) mit seinem lokalen Rechner auf ein entferntes Rechnernetz zu ermöglichen, müssen hierfür entsprechende Dienste (RAS, Remote Access Service) eingerichtet werden. Wie die einzelnen RAS-Systemkomponenten abgesichert werden können und wie hierzu ein entsprechendes RAS-Sicherheitskonzept erstellt werden kann, wird in diesem Baustein vorgestellt.

### **8.1 TK-Anlage**

In diesem Baustein wird eine auf ISDN basierende Telekommunikationsanlage betrachtet. Eine TK-Anlage in der heutigen Ausprägung ist ein komplexes IT-System, bei dessen Administration eine Reihe von Maßnahmen beachtet werden müssen, um den sicheren Betrieb der TK-Anlage zu gewährleisten.

### **8.2 Faxgerät**

Die Informationsübermittlung per stand-alone Faxgerät eröffnet ein neues Feld von Gefährdungen. Dargestellt werden daher die notwendigen Maßnahmen, mit denen für die Faxnutzung ein IT-Grundschutz realisiert werden kann. Dies sind zum Beispiel die Entsorgung von Fax-Verbrauchsgütern, die geeignete Aufstellung des Faxgerätes und die ggf. notwendigen Absprachen von Absender und Empfänger.

### **8.3 Anrufbeantworter**

Moderne Anrufbeantworter mit Fernabfragemöglichkeiten können als IT-Systeme aufgefasst werden, in denen Sprachinformationen gespeichert werden. Sie sind der Gefährdung ausgesetzt, dass die Fernabfrage missbraucht wird. Dargestellt werden IT-Grundschutz-Maßnahmen für Anrufbeantworter, auch speziell zu dieser Gefährdung.

### **8.4 LAN-Anbindung eines IT-Systems über ISDN**

Die Anbindung eines IT-Systems über eine ISDN-Adapterkarte mit S0-Schnittstelle an ein entfernt stehendes lokales Netz (LAN) wird in diesem Baustein betrachtet. Vorausgesetzt wird, dass innerhalb dieses LAN ein Router vorhanden ist, der über eine S2M-Schnittstelle mit dem öffentlichen Netz verbunden ist.

### **8.5 Faxserver**

In diesem Baustein werden für die Informationsübertragung per Fax als technische Basis ausschließlich Faxserver betrachtet. Ein Faxserver in diesem Sinne ist eine Applikation, die auf einem IT-System installiert ist und in einem Netz für andere IT-Systeme die Dienste Faxversand und/oder Faxempfang zur Verfügung stellt.

### **8.6 Mobiltelefon**

Um für digitale Mobilfunksysteme nach dem GSM-Standard (D- und E-Netze) einen sicheren Einsatz zu gewährleisten, werden in diesem Kapitel für die Komponenten Mobiltelefon, Basisstation und Festnetz und deren Zusammenspiel untereinander geeignete Sicherheitsmaßnahmen vorgeschlagen.

### **9.1 Standardsoftware**

Es wird eine Vorgehensweise beschrieben, wie der Lebenszyklus von Standardsoftware, d. h. Anforderungskatalog, Auswahl, Testen, Freigabe, Installation und Deinstallation, gestaltet werden kann. Insbesondere werden Aspekte wie Tests der Funktionalität und Sicherheitseigenschaften, Installationsanweisungen und Freigabeerklärung erläutert.

### **9.2 Datenbanken**

Die für die Auswahl einer Datenbank, deren Installation und Konfiguration sowie für den laufenden Betrieb erforderlichen Maßnahmen wie z. B. Erstellung eines Datenbankkonzeptes, Regelung zur Einrichtung von Datenbankbenutzern/-benutzergruppen oder Richtlinien für Datenbank-Anfragen werden in diesem Kapitel beschrieben.

### **9.3 Telearbeit**

Die aus organisatorischer und personeller Sicht erforderlichen Regelungen für die Einrichtung von Telearbeitsplätzen werden in diesem Baustein beschrieben. Weiterhin werden die sicherheitstechnischen Anforderungen an die Telearbeit formuliert, die durch den Einsatz geeigneter IT-Komponenten realisiert werden müssen.

## 14 Abbildungsverzeichnis

Abbildung 1: Stand-alone-Rechner .....	16
Abbildung 2: „Minimal-Netz“ .....	18
Abbildung 3: Peer-to-Peer-Vernetzung .....	26
Abbildung 4: Beispiel einer möglichen Struktur eines Client-Server-Netztes mit mehreren Servern.....	28
Abbildung 5: Stern-Topologie.....	30
Abbildung 6: Bus-Topologie .....	32
Abbildung 7: Ring-Topologie .....	33
Abbildung 8: Nutzung mikroelektronischer Steuerungselemente .....	36
Abbildung 9: Entwicklung der Anzahl von Hosts 1991 bis 2003 .....	104
Abbildung 10: Struktur potentieller Schadensereignisse.....	144
Abbildung 11: Skizze eines umfassenden Landesverwaltungsnetzes.....	155
Abbildung 12: Skizze eines schulinternen Netztes .....	157
Abbildung 13: Intranet der Schulen.....	161
Abbildung 14: Skizze Bezirksnetze – mittlere Netzebene .....	166

## 15 Literatur- und Quellenverzeichnis

(abgeschlossen Juli 2003)

- |  |   |
|--|---|
| A Campo, M.:   | PC-Sicherheit.<br>Bonn 2001-2002  |
| Auernhammer, H.:                                       | Bundesdatenschutzgesetz - Kommentar.<br>München 1993  |
| Baron, S./ Becker, K. / Schreiner,<br>H.P.:            | Die Informationsgesellschaft im Neuen<br>Jahrtausend.<br>Bergisch Gladbach 1997   |
| Benninghaus, H. :                                      | Einführung in die sozialwissenschaftliche<br>Datenanalyse. 2. Aufl.<br>München 1991   |
| Bernstein, H.:   | PC-Sicherheit.<br>Berlin/Offenbach 2001   |
| Bertelsmann Stiftung, Heinz Nixdorf<br>Stiftung (Hr.): | Bildungsinnovation durch Medien; Bil-<br>dungswege in der Informations-<br>Gesellschaft.<br>Gütersloh 1997  |
| Bildungskommission NRW (Hr.):                          | Zukunft der Bildung, Schule der Zukunft.<br>Neuwied 1994  |
| Binstadt, P.:  | Informations- und kommunikationstech-<br>nologische Grundbildung: Konzeptionen -<br>Konkretionen – Gestaltungsvorschläge.<br>Alsbach 1992                                 |
| Blankert, H.:  | Eine europäische Informationsgesell-<br>schaft für alle: Abschlussbericht der<br>Gruppe Hochrangiger Experten.<br>Luxemburg 1997  |
| Bliemeister, J. (Hr.):                                 | Informationsstelle Schule und Computer:<br>Ein Modell zur Optimierung des Informa-<br>tionsaustausches im Bereich der informa-<br>tionstechnischen Bildung.<br>Mainz 1991 |

- Böge, A. (Hr.): Elektrotechnik, Elektronik, Digitaltechnik, Steuerungstechnik. 5. Aufl. Braunschweig 2001
- Borowka, P.: Netzwerk-Technologien. 4. Aufl. Bonn 2002
- Botte, A. (Hr.): Implikationen der Informationsgesellschaft für die Bildung. Berlin 1997
- Brebeck, J./ Winkler, P.: PCs vernetzen. München 2000
- Brenner, A. / Gunzenhäuser, P.: Computer und Informatik in der Schule. Stuttgart 1987
- Brügmann, U.: Netzwerke von Anfang an. Düsseldorf 2001
- Buba, E-M.: Computernetze. Datenübertragung, Datenkommunikation, Datendienste. Reinbek 1992
- Büllesbach, A./ Heymann, T. (Hr.): Informationsrecht 2000, Perspektiven für das nächste Jahrzehnt; Informationstechnik und Recht. Bd. 9. Köln 2000
- Buttler, G. / Stroh, R.: Einführung in die Statistik. 7. Aufl. Reinbek 2000
- Büttner, C.: Computer in der Grundschule. Geräte, didaktische Konzepte, Unterrichtssoftware. 2. Aufl. Weinheim 1999
- Cebrián, J.L.: Im Netz – die hypnotisierte Gesellschaft. Der neue Bericht an den Club of Rome. Deutsche Verlagsanstalt, Stuttgart 1999
- Chapman, B./ Zwicky, E.: Building Internet Firewalls. O'Reilly & Associates 1995
- Zwicky, E. / Cooper, S. / Chapman, B.: Einrichten von Internet Firewalls. O'Reilly & Associates 2001

Ceruzzi, P.E.	Geschichte der ED. Bonn 2003
CHIP-Bibliothek	Drahtlos glücklich. Praxistest: W-LAN, Home-RF, Bluetooth, DECT Haar 2002
CHIP-Bibliothek	PC-Grundwissen – Schulung. Haar 2000
Chomsky, N. / Dietrich, H.:	Globalisierung im Cyberspace. Globale Gesellschaft. Märkte, Demokratie und Erziehung. Bad Honnef 1996
Comer, D.:	Computernetzwerke und Internets. Mün- chen 1998
Cyranek, G. (Hr.):	Computerkultur im Umbruch? Neue Technologien und die Zukunft für Schule und berufliche Bildung. Frankfurt/M 1991
Derfler, F.:	So funktionieren Netzwerke. München 2001
Determann, L.:	Kommunikationsfreiheit im Internet; Frei- heitsrechte und gesetzliche Beschrän- kungen. Baden-Baden 1999
Deutsche Telekom:	Abschlussbericht und Protokolle zum 1. TeleLearning Symposium der Deutschen Telekom, 18. Dezember 1995
Dickschus, A.:	PC-Wissen. 4. Aufl. Haar 2000
Die Landesbeauftragte für den Da- tenschutz Nordrhein-Westfalen	20 Jahre Datenschutz – Individualismus oder Gemeinschaftssinn? Düsseldorf 1998
Die Landesbeauftragte für den Da- tenschutz Nordrhein-Westfalen	Datenschutzbericht 1999. Düsseldorf 1999
Dieckmann, H. / Schachtsiek, B. (Hr.):	Lernkonzepte im Wandel. Die Zukunft der Bildung. Stuttgart 1998

- Dierkes, M.: Die Technisierung und ihre Folgen: zur Biographie eines Forschungsfeldes. Berlin 1993
- Drabe, M., Garbe, D. (Hr.): Schulen ans Netz. Berichte aus der Praxis. 2. Aufl. Bonn 2000
- Dreesen, A. Schwimmen lernen im Info-Meer. In: Computer+Unterricht, H.46 (2002), S.11-15
- Drs.: Computer – eine Herausforderung für die Grundschule. In: Die Grundschule, H. 114 (1998), S. 6 – 13
- Eckert, C.: IT-Sicherheit; Konzept – Verfahren - Protokolle. München 2001
- Ehlert, W. (Hr.): Sozialverträgliche Technikgestaltung und / oder Technisierung von Sachzwang? Opladen 1992
- Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft (Hr.): Deutschlands Weg in die Informationsgesellschaft. Bd. 9 Bonn 1998
- Ertl, A. Das globale Dorf. München 1996
- Europäische Kommission (Hr.): Lehren und Lernen. Auf dem Wege zur kognitiven Gesellschaft. Weißbuch zur allgemeinen und beruflichen Bildung. Brüssel 1995
- Falk, R. / Weiß, R. (Hr.): Mikro-Computer. Herausforderung für das Bildungswesen. Köln 1987
- Fleissner, P.: Der Mensch lebt nicht vom Bit alleine ...: Information in Technik und Gesellschaft. 3. Aufl. Frankfurt/M, 1998

- Frank, G.: Grundlagenwissen über Netzwerke. Braunschweig 1996
- Friedewald, M. Der Computer als Werkzeug und als Medium.. Die geistigen und technischen Wurzeln des Personal Computers. Berlin 1999
- Friedrichs, G. / Schaff, A. (Hr.): Auf Gedeih und Verderb. Mikroelektronik und Gesellschaft. Bericht an den Club of Rome. Reinbek 1984
- Gabriel, W.: Personale Pädagogik in der Informationsgesellschaft: berufliche Bildung, Selbstbildung und Selbstorganisation in der Pädagogik Rudolf Steiners. Frankfurt/Main 1996
- Geiger, G. (Hr.): Sicherheit in der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen. Baden-Baden 2000
- Geist, H.-J.: Telekommunikation mit Computer, Fax und Telefon. Aachen 2001
- Gerling, R.W.: Nachholbedarf: EG-Richtlinien zum Datenschutz. In: C't, H. 6 (1999), S. 316 f
- Gesellschaft für Informatik e.V. (GI): Empfehlungen zur Planung und Betreuung von Rechnersystemen an Schulen; Beilage zu LOG IN 21 Heft 1(2001)
- Gibbs, M. Durchblick im Netz. Bonn 1995
- Gössner, R.: „Big Brother“ & Co: der moderne Überwachungsstaat in der Informationsgesellschaft. Hamburg 2000
- Graf, L. u.a.: Keine Angst vor dem Mikrocomputer. Düsseldorf 1984

- Granzer, D.: Der Computer als Bildungsmittel. Grundschule, H. 9 (2002), S. 53 – 56
- Grønboek Windows 98 für Einsteiger. KnowWare Nr. 151
- Handbuch Praxis: Schul-EDV; Systembetreuung – Schulnetze. Stadtbergen 2000
- Handke, J.-C. Rund um den PC (für Anfänger). KnowWare Nr. 143
- Hanke, J.-C. Word für Studenten. KnowWare Nr. 138
- Hansen, H.R. / Neumann, G.: Wirtschaftsinformatik I; Grundlagen betrieblicher Informationsverarbeitung. 7. Aufl. Stuttgart 2001
- Hardy, P. Word 97 für Anfänger. KnowWare Nr. 147
- Hartmann, F. (Hr.): Informationsgesellschaft. Sozialwissenschaftliche Aspekte. Wien 1998
- Hauf, O.: Die Informationsgesellschaft: Anatomie einer Lebenslüge. Frankfurt/Main 1996
- Hennen, L.: Technisierung des Alltags. Opladen 1992
- Henrichwark, C. / Vaupel, W.: Auf dem Wege zum Medienkonzept. e-nitiative.nrw. Düsseldorf 2002
- Hering, E.: Elektronik für Ingenieure. Berlin 2001
- Heyden, K.-H. / Lorenz, W.: Lernen mit dem Computer in der Grundschule. Lernen mit Neuen Medien. Einrichten von Medienecken. Berlin 1999

- Hoeren, T. (Hr.):  
Rechtsfragen der Informationsgesellschaft.  
Berlin 1999
- Horster, P.: (Hr.):  
Kommunikationssicherheit im Zeichen des Internet. Grundlagen, Strategien, Realisierungen, Anwendungen. Braunschweig/Wiesbaden 2001
- Horx, M:  
Die acht Sphären der Zukunft. Ein Wegweiser in die Kultur des 21. Jahrhunderts.  
Wien 1999
- Hunziker, P.:  
Medien, Kommunikation und Gesellschaft. Einführung in die Soziologie der Massenkommunikation. 2. Aufl.  
Darmstadt 1996
- Imhof, K. / Rees, W. / Rüfner, W. (Hr.):  
Steuerungs- und Regelungsprobleme in der Informationsgesellschaft.  
Opladen 1999
- Isensee, J. (Hr.):  
Dem Staate, was des Staates – der Kirche, was der Kirche ist.  
Berlin 1999
- Issing, L./ Schaumberg, H.:  
Lernen mit Laptops. Ergebnisse einer Evaluationsstudie.  
Gütersloh 2002
- Janowicz, K.:  
Sicherheit im Internet. O'Reillys Internet-Bibliothek, Köln 2002
- Joerges, B. (Hr.):  
Technik im Alltag.  
Frankfurt/M 1988
- Jonietz, D.:  
Schulische Rechnernetze.  
In: Log In Bd. 20, H. 3 bis 6 (2000) sowie Log In Bd. 21, H. 1 bis 4 (2001)
- Kamlah  
Right to Privacy; Das Allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen.  
Köln 1969
- Kammerl, R. (Hr.):  
Computergestütztes Lernen.  
München 2000

- Kauffels, F.: Netzwerk- und System-Management; Probleme, Standards, Strategien. Bergheim 1995
- Keller, C.: Globale Informationsgesellschaft: wissenschaftliche Theorie, politisches Programm, globalisierte Geschäftssphäre. Tübingen 1998
- Kelling, G.L. / Coles, C.M.: Fixing Broken Windows; Restoring Order and Reducing Crime in our Communities. Touchstone 1998
- Kerner M. (Hr.): Der vernetzte Mensch: Sprache, Arbeit und Kultur in der Informationsgesellschaft. Aachen 1999
- Kersten, H.: Sicherheit in der Informationstechnik; Einführung in die Probleme, Konzepte und Lösungen. 2. Aufl. München 1995
- Klingen, L. / Otto, A.: Computereinsatz im Unterricht. Stuttgart 1986
- Kloepfer, M.: Datenschutz als Grundrecht. Königstein / Taunus 1980
- Kommission der Europäischen Gemeinschaft: Arbeitsdokument der Kommissionsdienststellen; eEurope, Benchmarking, Europas Jugend ins Digitalzeitalter. Brüssel 2001
- Kultusminister Nordrhein-Westfalen (Hr.): Neue Informations- und Kommunikationstechnologien in der Schule. Düsseldorf 1985
- Kuri, J.: Wellenlänge; Drahtlose Netzwerke erobern den Massenmarkt. In: C't, H. 6 (1999), S. 216 ff
- Kuri, J.: Wellenbrecher; Von Funk bis Telefon - Alternativen für die Heimvernetzung. In: C't, H. 6 (1999), S. 218 ff

- Kuri, J.: Wellensalat; 11 Lösungen für drahtlose Netze im Test.  
In: C't, H. 6 (1999), S. 240 ff
- Lackner, K./ Kühl, K.: Strafgesetzbuch. 24.Aufl.  
München 2001
- Landesinstitut für Erziehung und Unterricht LEU (Hr.): Computer in der Grundschule. Ein neues Medium. Materialien Grundschule.  
Stuttgart 1999
- Landesinstitut für Schule und Weiterbildung in Nordrhein-Westfalen (Hr.): Lernen mit neuen Medien in der Grundschule. 2. Aufl.  
Soest 1999
- Larisch D.: Das Einsteigerseminar Netzwerktechnik.  
Kaarst 2000
- Latzer, M. u.a. (Hr.): Die Zukunft der Kommunikation. Phänomene und Trends in der Informationsgesellschaft.  
Innsbruck 1999
- Lienemann, G. / Dördelmann, F.: Intranets. Konzeption, Sicherheit und Realisierung.  
Heidelberg 2002
- Lipinski, K.: Lexikon Netzwerktechnik.  
Bonn 1998
- Loschelder, W.: Grenzen staatlicher Wertevermittlung in der Schule.  
In: Zeitschrift für Beamtenrecht, H. 1-2 (2001), S. 6 ff
- Mader, G. / Stöckl, W.: Virtuelles Lernen. Begriffsbestimmung und aktuelle empirische Befunde.  
Innsbruck 1999
- Mahle, W. (Hr.): Orientierung in der Informationsgesellschaft.  
Konstanz 2000
- Matejovski, D. (Hr.): Neue, schöne Welt?: Lebensformen der Informationsgesellschaft.  
Frankfurt/M 2000

- Matis, H.: Die Wundermaschine. Eine unendliche Geschichte der Datenverarbeitung. Bonn 2002
- Melzig-Thiel, B.: Arbeit in der Informationsgesellschaft: Gefährdung und Risiken neuer Informations- und Kommunikationstechnologien für die Beschäftigung. Frankfurt/M 2000
- Meyer-Larsen, W. (Hr.): Der Orwell-Staat 1984. Reinbeck 1984
- Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes Nordrhein-Westfalen (Hr.): Orientierungshilfen zur Ausstattung der Grundschulen für das Lernen mit Neuen Medien. Frechen 1999
- Ministerium für Wirtschaft und Mittelstand, Technologie und Verkehr des Landes NRW / Ministerium für Schule und Weiterbildung des Landes NRW: NRW-Schulen ans Netz; Verständigung weltweit. Düsseldorf 1996
- Mitzlaff, H. / Speck-Hamdan, A. (Hr.): Grundschule und neue Medien. Beiträge zur Reform der Grundschule. Frankfurt/M. 1998
- Mitzlaff, H.: Handbuch Grundschule und Computer. Vom Tabu zur Alltagspraxis. Weinheim 1996
- Mitzlaff, H.: Lernen mit Mausclick. Computer in der Grundschule. Frankfurt/M. 1997
- Mörike, M.: Die Trends der Informationstechnologie: Hintergründe – Praxis – Visionen. München 1997
- Molinari, M.: Drahtlose lokale Netze. Bergheim 1994
- Müller, A.-C. / Freyn, A.: Schulix, das wartungsarme Schulnetzwerk dank Linux; 1. Preis des Wettbewerbs „Pffiffige EDV-Lösungen“. In: Computer und Unterricht, H. 43 (2001), S. 14

- Mutius, B. v.: Die Verwandlung der Welt. Ein Dialog mit der Zukunft. Stuttgart 2000
- Niemann, H.-W.: Vom Faustkeil zum Computer. Stuttgart 1985
- Oberliesen, R.: Information, Daten und Signale: Geschichte technischer Informationsverarbeitung. Reinbek 1982
- Nam Kha Pham: Wireless LAN: Zu viel versprochen, In: PC Praxis, H. 9 (2001), S. 162 ff
- Plöger, S.: Ein Schulnetz für alle. In: Computer und Unterricht, H. 43 (2001), S. 34f
- Postman, N.: Keine Götter mehr. Das Ende der Erziehung. 2. Aufl. Berlin 1995
- Presse und Informationsamt der Bundesregierung: Medienkompetenz, Qualifikation für die Zukunft. Wiesbaden 1997
- Quinn-Andry, T.: Netzwerk-Design. München 1998
- Rammert, W. (Hr.): Computerwelten – Alltagswelten. Wie verändert der Computer die soziale Wirklichkeit. Opladen 1990
- Reeb, H.-J.: Kommunikation im Wandel. In: Wochenschau Nr. 3 / 4, Ausgabe Sek. II: Multimedia-Informationsgesellschaft. Frankfurt 1996, S. 93 ff
- Reinke / Schmidt / Suck: Drahtlos glücklich. Praxistest: W-LAN, Home RF, Bluetooth, DECT. In: CHIP (2002), S. 235 ff
- Rifkin, J.: Leben im Zeitraffer. Essay. New World 1 (2002)

- Riggert, W.: Rechnernetze; Grundlagen – Ehternet – Internet. 2. Aufl. Leipzig 2002
- Rittershofer, A.: Computer und Netzwerke an Schulen. In: Computer und Unterricht, H. 41 (2001), S. 64 f
- RRZN – Regionales Rechenzentrum für Niedersachsen / Universität Hannover: Netzwerke, Grundlagen. 4. Aufl. Hannover 2001
- RRZN – Regionales Rechenzentrum für Niedersachsen / Universität Hannover: Computersicherheit im Internet für Anwender. Juni 2001
- Rüsse, W.: Informationspädagogik für Lehramtsstudierende in Darmstadt. In: Computer und Unterricht, H. 45 (2002), S.54 f
- Sackmann, R. / Weymann, A.: Die Technisierung des Alltags: Generationen und technische Innovationen. Frankfurt 1994
- Sarnow K.: Linux in der Schule, SuSE GmbH. Nürnberg 2000
- Schäfer, G.: Netzsicherheit. Algorithmische Grundlagen und Protokolle. Heidelberg 2003
- Schaumberg, H.: Neues lernen mit Laptops? Ein Überblick über Forschungsergebnisse zur Nutzung mobiler Computer in der schule. In: Zeitschrift für Medienpsychologie 13 (2001), S. 11 – 21
- Schell, F. / Stolzenburg, E. / Theunert, H. (Hr.): Medien-Kompetenz. Grundlagen und pädagogisches Handeln. München 1999
- Schiffmann, W/ Schmitz, R.: Technische Informatik 2; Grundlagen der Computertechnik. 4. Aufl. Berlin 2002

- Schönke, A. / Schröder, H.: Strafgesetzbuch. 25. Aufl.  
München 1997
- Schulte, G.: Wellenreiter; Technik und Standardisierung von drahtlosen Netzen.  
In: C't H. 6 (1999), S. 222 ff
- Schreiber, O.R.: Der PC im Netzwerk; Bestandteile – Standards – Kriterien.  
Würzburg 1989
- Schürmann, B.: Rechnerverbindungsstrukturen; Bussysteme und Netzwerke.  
Wiesbaden 1997
- Schwabe, J.: Entscheidungen des Bundesverfassungsgerichts; Studienauswahl.  
Hamburg 1994
- Siemens AG (Hr.): Chancen mit Chips; Zwischenbilanz einer Basistechnologie. Eine Sonderveröffentlichung der Siemens AG zur Ausstellung im Deutschen Museum.  
Berlin / München 1985
- Siemens AG: Halbleiterbauelemente für die Elektronik. O.O., o.J.
- Simitis, S.: Die Informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung.  
NJW 1984
- Steinbicker, J.: Zur Theorie der Informationsgesellschaft: ein Vergleich der Ansätze von Peter Drucker, Daniel Bell und Manuel Castells.  
Opladen 2001
- Stockinger, G.: Wege in die Informationsgesellschaft: eine soziologische Vision.  
Frankfurt/M 1999
- Storbeck, J.: EUROPOL – Sachstand und Ausblick.  
In: Die Polizei (1993), S. 229 ff

- Struck, P.: Netzwerk Schule. Wie Kinder mit dem Computer das Lernen lernen. München 1998
- Struck, P.: Die Schule der Zukunft. Von der Beherrungsanstalt zur Lernwerkstatt. Darmstadt 1996
- Sturm, J.: Das Schengener Durchführungsübereinkommen – SDÜ. Kriminalistik 1995, S. 162 ff
- Teitscheid, P.: Nachhaltige Produkt- und Dienstleistungsstrategien in der Informationsgesellschaft; Berlin 2002
- Tetsch, J. / Temme, M.: Eingriffsrecht. Band I: Grundlagen und Datenverarbeitung. Hilden 1998
- Thiedecke, Udo: Medien , Kommunikation und Komplexität: Vorstudien zur Informationsgesellschaft. Opladen 1997
- Traeger, D.H. / Volk, A.: LAN – Praxis lokaler Netze. 3. Aufl. Stuttgart, Leipzig, Wiesbaden 2001
- Treumann, K.P. u.a.: Medienkompetenz im digitalen Zeitalter. Wie die neuen Medien das Leben und Lernen Erwachsener verändern. Opladen 2002
- Tröndle, H. / Fischer, T.: Strafgesetzbuch und Nebengesetze. 51. Aufl. München 2003
- Tulodziecki, G. (Hr.): Neue Medien – neue Aufgaben für die Lehrerbildung: Initiative BIG – Bildung in der Informations-Gesellschaft. Gütersloh 1997
- Tulodziecki, G.: Neue Medien in den Schulen: Projekte, Konzepte, Kompetenzen; eine Bestandsaufnahme. Gütersloh 1996

- Tulodziecki, G.: Computer & Internet im Unterricht: medienpädagogische Grundlagen und Beispiele. Berlin 2002
- Turkle, S.: Leben im Netz. Identitäten im Zeitalter des Internet. Rowohlt, Hamburg 1998
- Tyrchan, G.: Programmieren: die vierte Kulturtechnik? Computer und Allgemeinbildung. In: VDI (Hrsg.): Mikroelektronik – Technik, Gesellschaft, Perspektiven – Düsseldorf 1985, S. 54 ff
- Tyrchan, G.: Computer in allgemeinbildenden Schulen. Curriculare Besonderheiten und Abgrenzungen, schulspezifische Konsequenzen bei Hard- und Software. In: Kath, F.M. u.a. (Hrsg.): Diskussionsfeld technische Bildung Alsbach 1985, S. 127 ff
- Tyrchan, G.: Microcomputers for School Technology in the Federal Republic of Germany. Proceedings of "50<sup>th</sup> ITEA International Conference". Norfolk 1988
- Urban, K.: Statistik, Einführung in die statistische Methodenlehre für Wirtschafts- und Sozialwissenschaftler. München 1989
- Vaupel, W. / Hoffmann, B.: Ausstattung für das Lernen mit neuen Medien. Ein Leitfaden für Schulen und Schulträger. e-nitiative.nrw, Düsseldorf 2001
- Von Stitzky, R.: Informationstechnische Grundbildung in der Schule. Münster 1995
- Vondran, E.P.: Entwicklungsgeschichte des Computers. Berlin 1982

- Wagner, R.: Die Informationsgesellschaft: Chancen für eine neue Lebensqualität am Beginn des dritten Jahrtausends. Münster 1996
- Weigel, E.: Dialogorientierte Datenverarbeitung. Ludwigshafen 1986
- Weltner, T.: Windows 98 SE. Data Becker, Düsseldorf 1999
- Wilson, J.Q. / Herrnstein, R.J.: Crime & Human Nature, The Definitive Study of the causes of Crime. London 1998
- Zimmermann, O.: Kulturpolitik für das 21. Jahrhundert – Anforderungen an die Informationsgesellschaft. Bonn 1999
- [www.bmbf.de/pub/it-ausstattung\\_der\\_schulen2002.pdf](http://www.bmbf.de/pub/it-ausstattung_der_schulen2002.pdf) IT-Ausstattung der allgemeinbildenden und berufsbildenden Schulen in Deutschland. Eine Bestandsaufnahme
- [www.en.eun.org](http://www.en.eun.org) Startseite des Europ. Schulnetzes (European schoolnet)
- [www.e-nitiative.nrw.de](http://www.e-nitiative.nrw.de)
- [www.learn-line.nrw.de/angebote/berichtsarchiv/info](http://www.learn-line.nrw.de/angebote/berichtsarchiv/info)
- www.lehrer-online.de: Die Schulhomepage; Fragen – Antworten – Mustertexte
- www.san-ev.de/itworks/land/natvgl-06-2002.pdf Bestehende Ansätze zu Systemlösungen für den IT-Einsatz in Deutschlands Schulen. Stand Juni 2002
- [www.primolo.de](http://www.primolo.de) Grundschulprojekte online präsentieren
- [www.schulen-ans-netz.de/itworks](http://www.schulen-ans-netz.de/itworks) Bestehende Ansätze zu Systemlösungen für den IT-Einsatz in Deutschlands Schulen; o.O., April 2003