Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg

Wahlpflichtfach:
„Personalmanagement“

Die private Nutzung des Internets am Arbeitsplatz

Diplomarbeit

vorgelegt von

Andreas Mayer

Studienjahr 2008/2009

Erstgutachter: Herr Professor Peter Raviol
Zweitgutachter: Herr Regierungsdirektor Frank Bauer

Inhaltsverzeichnis

1 Einführung 7
1.1 Internet, das neue Medium am Arbeitsplatz 8
1.2 Statistiken zur Internetnutzung am Arbeitsplatz 9
2 Regelungsmöglichkeiten im Arbeits- oder Dienstverhältnis 11
2.1 Tarifvertragliche Regelungen 12
2.2 Beschränkung auf die dienstliche Nutzung von Internet und E-Mail 13
2.3 Ausnahmen der Beschränkung auf die dienstliche Nutzung 16
2.4 Gestattung der privaten Nutzung von Internet und E-Mail 19
2.4.1 Betriebliche Übung 20
2.4.2 Bestimmung des Nutzungsumfangs 22
2.5 Regelung durch Dienstvereinbarung 25
2.6 Rücknahme der Gestattung 26
2.7 Keine Regelung wird getroffen 27
3 Maßnahmen bei Verstößen 27
3.1 Rechte der Personalvertretungen 28
3.1.1 Mitbestimmungsrechte 29
3.1.2 Mitbestimmungsfrei 33
3.2 Verwertbarkeit von Beweisen und Kontrolle der Beschäftigten aufgrund der gesetzlichen Grundlagen 34
3.2.1 Bundesdatenschutzgesetz 36
3.2.2 Landesdatenschutzgesetz Baden-Württemberg 38
3.2.3 Telekommunikationsgesetz 39
3.2.4 Telemediengesetz 42
3.2.5 Telekommunikations-Überwachungsverordnung 45
3.3 Schadensersatzanspruch des Arbeitsgebers 46
3.4 Abmahnung 48
3.5 Ordentliche Kündigung 49
3.6 Außerordentliche Kündigung 50
Exkurs: Onlinesucht 51
3.7 Krankheitsbedingte Kündigung 53
3.8 Disziplinarverfahren 55
4 Private Nutzung des Internets als Motivationsfaktor 55
5 Fazit und Ausblick 56

6 Literaturverzeichnis LIX
7 Internet-Literaturverzeichnis LXI
8 Anlagen LXIV
9 Erklärung LXXVIII

Abkürzungsverzeichnis

a.F.	alte Fassung
Abs.	Absatz
AP	Arbeitsrechtliche Praxis, Nachschlagewerk des Bundesarbeitsgerichts
ArbG	Arbeitsgericht
Art.	Artikel
AWG	Außenwirtschaftsgesetz i. d. F. vom 28.04.2008
BAG	Bundesarbeitsgericht
BBG	Bundesbeamtengesetz i. d. F. vom 17.06.2008
BDSG	Bundesdatenschutzgesetz i. d. F. vom 22.08.2006
BetrVG	Betriebsverfassungsgesetz i. d. F. vom 12.08.2008
BGB	Bürgerliches Gesetzbuch i. d. F. vom 12.08.2008
BPersVG	Bundespersonalvertretungsgesetz i. d. F. vom 14.08.2006
BVerfG	Bundesverfassungsgericht
Dt.	Deutsch
DV	Dienstvereinbarung
EDV	Elektronische Datenverarbeitung
EStG	Einkommensteuergesetz i. d. F. vom 16.12.2008
FTP	File Transfer Protocol (Dt.: Dateiübertragungsverfahren)
G-10-G	Artikel 10-Gesetz i. d. F. vom 21.12.2007
GG	Grundgesetz i. d. F. vom 08.10.2008

Hrsg.	Herausgeber
HSO	Hilfe zur Selbsthilfe bei Onlinesucht 2007 e.V.
i. d. F.	in der Fassung
i.d.R.	in der Regel
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IKT	Informations- und Kommunikationstechnologie
IRC	Internet Relay Chat
IT	Informationstechnologie
KSchG	Kündigungsschutzgesetz i. d. F. vom 26.03.2008
LAG	Landesarbeitsgericht
LBG	Landesbeamtengesetz Baden-Württemberg i. d. F. vom 03.12.2008
LDSG	Landesdatenschutzgesetz Baden-Württemberg i. d. F. vom 14.02.2007
LPersVG	Landespersonalvertretungsgesetz Baden-Württemberg i. d. F. vom 03.12.2008
m.w.N.	mit weiteren Nachweisen
MdStV	Mediendienste-Staatsvertrag
NZA	Neue Zeitschrift für Arbeitsrecht
O.A.	Ohne Autor
o.ä.	oder ähnliches
o.J.	ohne Jahr

o.O.	ohne Ort
Rn.	Randnummer
S.	Seite oder Satz
StGB	Strafgesetzbuch i. d. F. vom 31.10.2008
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TDSV	Telekommunikations-Datenschutzverordnung
TKG	Telekommunikationsgesetz i. d. F. vom 25.12.2008
TKÜV	Telekommunikations-Überwachungsverordnung i. d. F. vom 25.12.2008
TMG	Telemediengesetz i. d. F. vom 01.03.2007
u.a.	unter anderem oder und andere
UWG	Gesetz gegen den unlauteren Wettbewerb i. d. F. vom 22.12.2008
Vgl.	Vergleiche
WHO	World Health Organization (Dt.: Weltgesundheitsorganisation)

1 Einführung

Die Entwicklung von Computern und des Internets zählen wohl mit zu den wichtigsten Erfindungen des 20. Jahrhunderts und vielleicht von ihrer Grundidee sogar mit zu den wichtigsten Erfindungen, welche die Menschheit je gemacht hat. In der modernen Welt gehört ein Internetanschluss mittlerweile schon fast zum ganz normalen Standard, wie das Telefon oder Auto. Ein Ende der Weiterentwicklung des Computers und Internets und dessen Einsatzmöglichkeit ist nicht abzusehen. Zwar gibt es Teile dieser Entwicklung, die bereits am stagnieren, oder gar rückläufig sind, jedoch sind die Möglichkeiten noch lange nicht ausgeschöpft. Dies zeigt sich an neuesten Entwicklungen wie z.B. dem Web 2.0, dem sogenannten „Mitmachinternet“ in dem der User[1] dazu ermuntert wird, Webinhalte selbst zu gestalten. Selbst wer meint, dass er nichts mit dem Internet zu tun hat, wird mit der fortschreitenden Integration von Internetfunktionen in immer mehr Elektrogeräten (außer dem Computer) wie Handys, Navigationsgeräten, Fernsehern, Spielkonsolen, etc. doch aktiv oder passiv in Teilen davon berührt.

Es ist daher nicht verwunderlich, dass in erster Linie das Internet (noch) ein Medium darstellt, das hauptsächlich für den privaten Gebrauch interessant ist. Dies mag zum einen daran liegen, dass es, wie in oben genannter Aufzählung, viele Nutzungsmöglichkeiten des Internets gibt die man eher im privaten Bereich nutzt. Jedoch liegt dies zum anderen auch daran, dass viele Unternehmen und Behörden noch nicht erkannt haben, welches Potential ihnen das Internet, neben einer schlichten Homepage, bietet oder sie haben dieses Potential noch nicht ausgeschöpft. Der Hauptgrund weshalb überhaupt in den meisten Unternehmen und Behörden ein Internetanschluss besteht ist neben dem, dass man es in der modernen Geschäftswelt halt haben muss, der, dass damit Informationen schnell und einfach durch die Internetnutzer abgerufen werden können. Denn das Internet stellt von seinen Informationen her für ein Unternehmen oder eine Behörde eine unendlich große, sich ständig erweiternde und mittlerweile sogar sehr günstige Wissensplattform mit schnellem Zugriff dar, die man durch nichts anderes erset-

[1] Dt.: Nutzer (bzw. hier: der Internetnutzer).

zen könnte. Zwar ist Fachliteratur sicher auch wichtig, doch ein Buch hat eben die Nachteile der begrenzten Kapazität und der Aktualität.

Diese Diplomarbeit wird jedoch nicht erörtern welchen Sinn oder Unsinn die Nutzung des Internets für einen selbst, für ein Unternehmen oder eine Behörde darstellt. Das wird jeder für sich selbst entscheiden müssen. Sondern erfasst wird das Thema der privaten Internetnutzung am Arbeitsplatz, ein Thema bei dem es zwar in Teilen einige ähnliche Ansichten und „Grundsätze" gibt, jedoch scheiden sich die Geister oftmals noch. Im Folgenden werden daher auch an den passenden Stellen die unterschiedlichen Ansichten kurz erläutert und kommentiert. Entgegen der meisten Literaturquellen wird bei den anzusprechenden Punkten jedoch nicht umfassend auf alle arbeitsrechtlichen Punkte eingegangen. Es werden gewisse arbeitsrechtlichen Grundkenntnisse vorausgesetzt und daher Unterpunkte wie z.B. Fristen bei der ordentlichen Kündigung ausgelassen um dafür konzentrierter auf die Punkte einzugehen, welche beachtet werden müssen. Es wird dabei grundsätzlich auf den unternehmerischen Bereich eingegangen, jedoch wird in Teilbereichen auch auf spezielle Punkte für Behörden eingegangen. Daher wird auch der Begriff des Beschäftigten (wobei natürlich Frau wie Mann gleichermaßen gemeint ist) allgemein zur besseren Lesbarkeit verwendet und nur in den speziellen Punkten differenziert.

1.1 Internet, das neue Medium am Arbeitsplatz

Das Internet zählt heute zu den neuesten Medien in der Geschäftswelt. Es sorgt dafür, dass man sich schnell Informationen besorgt, sich als Unternehmen oder Behörde präsentieren kann, den Kontakt zu Kunden und Partnern herstellt oder diesen verbessert.[2] Eine der neuesten Entwicklungen hiervon ist das sogenannte e-Government. Es erleichtert den Kontakt der Bürger zur Behörde, zum Erhalt von Unterlagen oder zur gesamten Abwicklung von Verfahren, sowie den Kontakt von Behörden und Unternehmen um Bürokratie abzubauen.

[2] Vgl. Denzel, B./Alfes, K./Heide, S./Müller, T./Seifer, F., Private Nutzung des Internet am Arbeitsplatz – personalpolitische und rechtliche Überlegungen, Norderstedt 2003, S. 12 (im Folgenden zitiert als „Denzel/Alfes/u.a.").

Im Hinblick auf die individuelle Nutzung des neuen Mediums durch Beschäftigte wird durchgehend von Bedeutung sein, dass genau unterschieden wird ob eine private oder eine dienstliche Nutzung vorliegt, wobei es durchaus nicht ausgeschlossen ist, dass eine vermeintlich private Nutzung trotzdem dienstlich ist und es zu gewissen Überschneidungen kommen kann.[3, 4] Grundsätzlich liegt eine dienstliche Nutzung vor, wenn die Nutzung abstrakt-objektiv dazu geeignet ist die Erledigung der dienstlichen Aufgaben zu erreichen. Es genügt also wenn die Nutzung des Internets im Entferntesten geeignet sein könnte die Arbeit voran zu bringen.

1.2 Statistiken zur Internetnutzung am Arbeitsplatz

Um eine grobe Vorstellung vom Umfang der Internetnutzung in Unternehmen zu bekommen, sind im Folgenden einige statistische Kennzahlen sowie eine Studie erfasst und dargestellt.

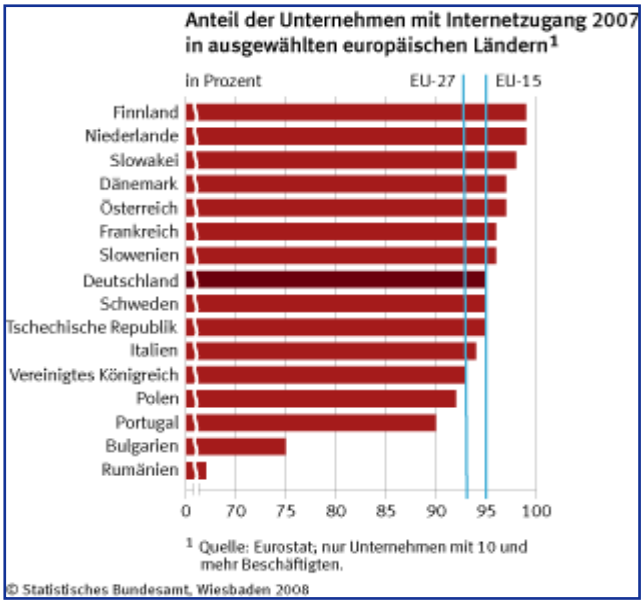


ABBILDUNG: NUTZUNG VON IKT IN UNTERNEHMEN

Im Januar 2008 lag der Anteil der Beschäftigten, die bei der Arbeit einen Computer mit Internetanschluss haben, bei 53%.

Zum Vergleich: im Jahr 2003 betrug dieser Wert noch 31%.[5] Wie hoch jedoch der Anteil der Unternehmen ist, die einen Internetzugang besitzen, zeigt die Statistik des Statistischen Amtes der

[3] Vgl. Hanau, P./Hoeren, T., Individualrechtliche Probleme der privaten Internetnutzung, in: Hoeren, T./Spindler, G./Holznagel, B./Gounalakis, G./Burkert, H./Dreier, T. (Hrsg.): Private Internetnutzung durch Arbeitnehmer, Schriftenreihe Informationen und Recht, Band 34, München 2003, S. 19-20.

[4] Vgl. Besgen, N./Prinz, T., Dienstliche und private Nutzung von Internet, Intranet und E-Mail – Individualarbeitsrecht, in: Besgen, N./Prinz, T. (Hrsg.): Neue Medien und Arbeitsrecht, Bonn/Berlin 2006, § 1 Rn. 4.

[5] Vgl. Statistisches Bundesamt, PC und Internet prägen zunehmend Berufs- und Privatleben, Bonn 2008, [Abruf: 15.01.2009], (Fortsetzung auf nächster Seite)

Europäischen Union, welche vom Statistischen Bundesamt graphisch aufgearbeitet wurde.[6] Der Anteil liegt hier bei den deutschen Unternehmen bei ca. 95%, wobei erwähnt werden muss, dass nur Unternehmen berücksichtigt wurden mit mehr als 10 Beschäftigten. Nimmt man nun auch die deutschen Unternehmen mit weniger als 10 Beschäftigten hinzu, so liegt der Anteil nur noch bei 77%.[7] lich seien die Zahlen des Jahres 2007 über den Kontakt von Unternehmen zu Behörden via Internet erwähnt. So nahmen 49% der Unternehmen die bote der öffentlichen Verwaltungen wahr. Von diesen 49% nutzten 81% die Angebote um Formulare herunterzuladen und 73% um Informationen einzuholen.[8]

Das IT-Sicherheitsunternehmen Websense führte zuletzt im Jahr 2001 eine Studie zur privaten Internetnutzung am Arbeitsplatz in Deutschland und drei weiteren Ländern durch. Ergebnisse der Studie haben gezeigt, dass in Deutschland durchschnittlich 41% der Befragten auf Seiten surfen, die keinen Bezug zu ihrer beruflichen Tätigkeit haben. Dies sind im Schnitt ca. 3 Stunden pro Woche.[9]

Die Gründe für diese private Nutzung können vielfältiger Art sein. Zum einen die reine Neugier aktuelle Geschehnisse über Nachrichtenportale mitzuverfolgen. Zudem um sich Informationen über bestimmte Themen zu verschaffen um bei

---

http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Presse/pm/2008/11/PD08__452__52911.psml.

[6] Vgl. Statistisches Bundesamt, Anteil der Unternehmen mit Internetzugang 2007 in ausgewählten europäischen Ländern, Wiesbaden 2008, [Abruf: 15.01.2009], http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Statistiken/Informationsgesellschaft/Unternehmen/Unternehmen.psml

[7] Vgl. Bauer, O./Tenz, B., Acht von Zehn Unternehmen in Deutschland haben Zugang zum Internet, in: Statistisches Bundesamt (Hrsg.): Informations- und Kommunikationstechnologie in Unternehmen, Wiesbaden 2008, S. 1201, [Abruf: 15.01.2009], http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Querschnittsveroeffentlichungen/WirtschaftStatistik/Informationsgesellschaft/IKTUnternehmen1207,property=file.pdf.

[8] Vgl. Statistisches Bundesamt, Nutzung von Informations- und Kommunikationstechnologie (IKT) in Unternehmen, Wiesbaden 2008, [Abruf: 15.01.2009], http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Informationsgesellschaft/Unternehmen/Aktuell,templateId=renderPrint.psml.

[9] Vgl. Websense Internation Ltd., Web@Work Study 2001, San Diego 2001, [Stand: 16.07.2003], http://www.websense.com/company/news/research/webatwork2001-germany.pdf zitiert bei Denzel/Alfes/u.a., S. 18-19.

aktuellen Geschehnissen im Kollegenkreis mitreden zu können. Oder schlichtweg um Zeit für Dinge zu sparen die man sonst von zu Hause aus erledigen müsste. Als Beispiele kann man die Nutzung von Onlinebanking, die Teilnahme an Onlineauktionen oder bei Diskussionsplattformen, der Produkteinkauf via Internet, sowie das Einholen von Informationen von Behörden für private Belange nennen. In der Literatur wird zudem noch der Faktor der Kostenersparnis genannt, sofern keine Abrechnung für die private Nutzung erfolgt. Jedoch dürfte dies bei den heutzutage günstigen Angeboten von Flatrates und Internetcafés eine eher untergeordnete Rolle spielen.[10]

2 Regelungsmöglichkeiten im Arbeits- oder Dienstverhältnis

Um eine private Nutzung des Internets festzustellen, zu verbieten oder eventuell arbeitsrechtliche Maßnahmen durchzuführen, muss zuerst festgestellt werden in welcher Form, oder überhaupt Regelungen zur privaten Internetnutzung vorhanden sind. Hierbei wäre es denkbar, dass es Regelungen gibt die von außen in den Vertrag hinein wirken z.B. per Tarifvertrag.

Da diese Regelungen gemäß der Normenhierarchie ranghöher stehen als Regelungen per Betriebsvereinbarung oder einzelnen Arbeitsverträgen, wird diese Möglichkeit im Folgenden zuerst und extra geprüft. Extra daher, da während der Anfertigung dieser Diplomarbeit kein Tarifvertrag bekannt war, der explizit auf die Regelung einer privaten oder dienstlichen Internetnutzung eingegangen ist.

Anschließend wird nicht mehr nach Art der Regelung unterschieden, sondern die Möglichkeiten der Beschränkung oder Gestattung werden genauer erläutert, wobei natürlich auch darauf eingegangen wird, wie dies nun in einer Betriebs- oder Dienstvereinbarung oder in einem Arbeitsvertrag geregelt werden könnte und worauf jeweils geachtet werden muss.

[10] Vgl. Denzel/Alfes/u.a., S. 18.

Im Anschluss daran wird die Rücknahme einer möglichen Beschränkung oder auch Gestattung erklärt, sowie darauf eingegangen was zu beachten ist, wenn gar keine Regelung zwischen den Parteien getroffen wird.

2.1 Tarifvertragliche Regelungen

Theoretisch ist eine kollektivarbeitsrechtliche Regelung per Tarifvertrag über eine erlaubte private Internetnutzung kein Problem. Der Knackpunkt liegt hingegen in der Praxis. Bei vielen Unternehmen die als eine Tarifvertragspartei auftreten, besteht eine sehr unterschiedliche Ausstattung im Hinblick auf Technik und Software (dieses Problem besteht in der Regel natürlich nicht bei Firmentarifverträgen, sofern in der Firma einheitliche technische Standards herrschen), welche erst angeglichen werden müssten, bevor man tiefer gehende Regelungen treffen könnte. Denkbar wäre hierbei eine Einigung der am Tarifvertrag beteiligten Arbeitgeber auf einen gewissen Mindeststandard an Software, (z.B. Einführung von Windows XP als Betriebssystem bei allen Arbeitgebern) worauf wiederum eine tarifvertragliche Regelung zum Einsatz einer bestimmten Software zur Datenerhebung aufgebaut werden könnte. Daher bleibt für die Praxis meist nur die Möglichkeit der Rahmenregelung übrig, welche ohne Beachtung von technischer Ausstattung für alle Unternehmen eines Tarifvertrags gelten können. Inhalte dieser Rahmenregelungen können Begriffsbestimmungen der undefinierten Begriffe des § 87 I Nr.6 BetrVG wie z.B. „technische Einrichtungen“, „Verhalten oder Leistung“, sowie „überwachen“, sein[11], aber auch eine genaue Definition des Nutzungsumfangs sollte im Hinblick auf Dauer, Herunterladen von Dateien, Einsatz von bestimmten (evtl. vorinstallierten) Browsern und Verbot bestimmter Webanwendungen (Chatsoftware, Flashplayern, etc.), Verbot des Besuchs von Webseiten mit pornographischem oder rechtswidrigem Inhalt, Kontroll- und Filterbefugnisse des Arbeitgebers, Übernahme der Verantwortung des Beschäftigten für seinen Internetzugang (durch z.B. Eingabe eines Passworts), oder einer eventuellen Kostenübernahme durch Beschäftigte erfolgen.[12]

[11] Vgl. Hanau/Hoeren, S. 77-88.

[12] Vgl. Besgen/Prinz, S. 41-42.

Zu beachten hierbei ist jedoch, dass sich aus § 88 III S.3 TKG ergibt, dass keine Einschränkung des in Art. 10 I GG genannten Fernmeldegeheimnisses vorliegen darf, denn dieses ist nur aufgrund eines Gesetzes oder einer anderen gesetzlichen Vorschrift einschränkbar, worunter eine tarifvertragliche Regelung nicht fällt.

Als Lösung hierzu ergibt sich jedoch die Möglichkeit, die Einwilligung jedes einzelnen Beschäftigten einzuholen. Eine solche Möglichkeit ist nicht im Telekommunikationsgesetz genannt, jedoch auch nicht untersagt. Eine konkrete Regelung zu treffen wurde vom Gesetzgeber bei der letzten Neufassung des Telekommunikationsgesetzes versäumt.[13] Daher muss man wie bisher die Regelungen der §§ 4 I und 4a BDSG als Grundlage nehmen, wonach der Beschäftigte auf sein ihm zustehendes Fernmeldegeheimnis (oder in diesem Fall auch Telekommunikationsgeheimnis) verzichten kann.[14] Da hierbei einiges zu beachten ist, wird dieser Punkt später unter 3.2.1 noch genauer erläutert.

2.2 Beschränkung auf die dienstliche Nutzung von Internet und E-Mail

Die einfachste Möglichkeit für den Arbeitgeber eine Regelung zu treffen ist es die Nutzung von Internet und E-Mail auf den dienstlichen Gebrauch zu beschränken. Um dies jedoch zu tun, muss vorher definiert sein, wann denn überhaupt eine dienstliche Nutzung vorliegt. Hierbei ist es unerheblich ob die Nutzung auch tatsächlich die Arbeit voran bringt, denn die Nutzung muss lediglich „abstrakt-objektiv dazu geeignet sein, die dienstlichen Aufgaben zu fördern“.[15] Aufgrund dieser weiten Umschreibung gibt es eine Reihe möglicher Überschneidungsmöglichkeiten zwischen privater und dienstlicher Nutzung welche gleich noch unter 2.3 genauer beschrieben werden.

---

[13] Vgl. Bundesgesetzblatt Teil I 2004, 26.06.2004, S. 1190 ff.

[14] Hanau/Hoeren, S. 56.

[15] Vgl. Besgen/Prinz, § 1 Rn. 4; Däubler, W., Internet und Arbeitsrecht, Frankfurt am Main 2004, Rn. 177.

Davor seien aber noch die verschiedenen Regelungsmöglichkeiten genannt. Als erstes kommt in Frage, dass der Arbeitgeber als Eigentümer des Internetanschlusses im Wege des Direktionsrechts per Weisung die Nutzung von Internet und E-Mail auf dienstliche Zwecke beschränkt. Der Vorteil ist hier, dass auf schnelle und einfache Art klare Verhältnisse geschaffen werden können, zudem ist eine solche Weisung mitbestimmungsfrei.[16]

Die zweite Möglichkeit bestünde per Betriebs- oder Dienstvereinbarung, also unter Beteiligung der Personalvertretung. Diese Lösung ist mehr als freiwilliger Akt des Arbeitgebers anzusehen, denn durch sein Weisungsrecht könnte er nach der ersten Möglichkeit den Betriebs-/Personalrat auch schlichtweg umgehen. Da jedoch die jeweiligen Vertretungen wie wir unter 6.1 noch sehen werden Mitbestimmungsrechte im Hinblick auf die Einrichtung von Internetarbeitsplätzen oder z.B. bei der technischen Überwachung von Beschäftigten haben, kann es sinnvoll sein sich mit den Vertretungen frühzeitig zusammenzusetzen und unter dem Punkt der Beschränkung auf die dienstliche Nutzung, auch Einigungen bei Themen wie Prüfkriterien, Instrumenten zur Überwachung, oder z.B. der Abfolge der Personalmaßnahmen zu treffen. Zu beachten ist wie unter 2.1, dass das Fernmeldegeheimnis nicht durch Betriebs- oder Dienstvereinbarung abbedungen werden kann.[17]

Die dritte Möglichkeit ist eine Regelung direkt im Arbeitsvertrag, eine entsprechende Klausel oder Information könnte direkt dem Arbeitsvertrag beigefügt werden. Sollte jedoch keine Regelung im Arbeitsvertrag oder als dessen Anhang vorhanden sein, kann der Umkehrschluss, dass eine private Nutzung erlaubt ist, nicht angenommen werden. Es gilt der Grundsatz, dass alle vom Arbeitgeber bereitgestellten Mittel zunächst nur für die dienstliche Nutzung eingesetzt werden dürfen.[18]

---

[16] Vgl. Denzel/Alfes/u.a., S. 79.

[17] Vgl. Hanau/Hoeren, S. 57; Denzel/Alfes/u.a., S. 57.

[18] Vgl. Jouran, Karim R., Internet am Arbeitsplatz – Irrtümer, Feil, T. (Hrsg.), Hannover 2005, S.1, [Abruf: 12.02.2009], http://www.recht-freundlich.de/download/Internet_am_Arbeitsplatz_Irrtuemer_2005-07-29.pdf (im Folgenden zitiert als "Karim, Internet am Arbeitsplatz – Irrtümer".

Eine Beschränkung auf die rein dienstliche Nutzung, egal in welcher Form führt dazu, dass der Arbeitgeber einfachere Kontrollrechte bekommen, als wenn eine private Nutzung gestattet ist. Denn bei einer lediglich dienstlichen Nutzung ist die sogenannte Eigensphäre des Beschäftigten wesentlich weniger berührt als bei einer privaten Nutzung.[19] Der Arbeitgeber hat zudem das Recht die ordnungsgemäße Erbringung der Arbeitsleistung zu kontrollieren, wozu auch die Kontrolle des Inhalts einer E-Mail zählt. Eine E-Mail ist hierbei nicht in dem Umfang schutzbedürftig wie ein Telefonat, da sie aufgrund ihrer Art diesem kaum ähnelt, bis auf die Übertragung per Datenkabel. Im Gegenteil: eine E-Mail wird erst geschrieben, womöglich nochmal korrekturgelesen und dann versandt, was man auch als Erfüllung des Textformerfordernisses des § 126b BGB ansehen kann.[20] Zudem muss man dem Arbeitgeber eine gewisse Kontrolle seines Geschäftsbetriebs zubilligen, denn wenn der Arbeitgeber die Inhalte der dienstlichen E-Mails nicht kontrollieren könnte, würde er die Möglichkeit verlieren einen Einblick zu erhalten was die Firma nach außen verschickt, oder was die Firma an Dokumenten erhält.[21] Die Einrichtung einer E-Mailadresse mit Namen oder Namensbestandteilen des Beschäftigten ist hierbei ebenfalls kein Argument für eine Einschränkung des Kontrollrechts. Zwar wird dies teilweise in der Literatur so dargestellt[22], jedoch entspricht es der Praxis, dass E-Mailadressen mit Namen oder Namensbestandteilen in Firmen verwendet werden und die Kunden an diese E-Mailadressen ihre Sendungen richten. Hinzu kommt zudem, dass ein Absender, der die E-Mail nicht als privat kennzeichnet, damit rechnen muss, dass seine Nachricht bei einem Unternehmen irgendwo zentral erfasst (wie bei einer Poststelle) und vielleicht sogar von Fremden (z.B. der Urlaubs- oder Krankheitsvertretung) gelesen wird. [23]

[19] Vgl. Hanau/Hoeren, S. 60.

[20] Vgl. Besgen/Prinz, § 1 Rn. 41.

[21] Vgl. Besgen/Prinz, § 1 Rn. 44.

[22] So Ernst, in: NZA 2002, S. 585, 589 zitiert bei Besgen/Prinz, § 1 Rn. 42.

[23] Vgl. Besgen/Prinz, § 1 Rn. 43, 44.

Unproblematisch erscheinen hingegen Kontrollen bei denen die Daten gem. § 3 VI BDSG in anonymisierter Form geprüft werden. Hierbei dürfen auch Inhalte von E-Mails geprüft werden, ohne dass man vorher zwischen dienstlich und privat unterscheidet. Mittels moderner Filterprogramme kann man heutzutage automatisch bestimmte Wörter, Wortkombinationen, etc. herausfinden lassen. Falls sich durch diese Filterung ein Verdacht der privaten Nutzung ergibt, kann gezielt weiter geprüft werden, wobei das „berechtigte Interesse des Arbeitgebers gegenüber dem Persönlichkeitsrecht des Arbeitnehmers“[24] überwiegt. Ebenfalls überwiegt dieses, wenn mittels einer Überwachungssoftware die Internetnutzung kontrolliert wird. Bei der Nutzung von solcher Software, ob für E-Mails oder Internet, ist zu beachten, dass der Betriebs- oder Personalrat zu beteiligen ist.[25, 26]

2.3 Ausnahmen der Beschränkung auf die dienstliche Nutzung

Da es zu Überschneidungen zwischen dienstlicher und privater Nutzung kommen kann und diese private Nutzung sogar gerechtfertigt sein kann, sind im Folgenden einige Ausnahmen von der Beschränkung auf die dienstliche Nutzung genannt.

Eine erste Ausnahme könnte während den Pausen bestehen. Es handelt sich hierbei nicht um Arbeitszeit, sondern um Zeit in der sich ein Beschäftigter von der normalen Arbeit kurz erholen, etwas in Ruhe essen, oder sonstiges tun kann. Ob in dieser Zeit das Internet privat genutzt werden darf, ist jedoch bei einer Beschränkung auf die dienstliche Nutzung höchst fraglich. Der Arbeitgeber hat durch seine Beschränkung die private Nutzung klar untersagt, sofern er für die Pausen keine Ausnahmeregelung getroffen hat. Im Zweifel gilt der Grundsatz, dass alle vom Arbeitgeber zur Verfügung gestellten Arbeitsmittel zunächst nur für die Arbeit genutzt werden dürfen.[27] Insbesondere ist hierbei zu beachten, ob der

[24] Besgen/Prinz, § 1 Rn. 40.

[25] Siehe auch 2.1 und 3.1.

[26] Vgl. Besgen/Prinz, § 1 Rn. 40, 53.

[27] Vgl. Karim, Internet am Arbeitsplatz – Irrtümer, S. 1.

Arbeitgeber eine Flatrate zur Internetnutzung besitzt. Besitzt er keine Flatrate, würden ihm weitere Kosten entstehen und er wäre dadurch geschädigt.[28]

Die zweite Ausnahme wären Nutzungen, die man unter dem Ziel einer guten Arbeitsatmosphäre zusammenfassen könnte (halb dienstlich/halb privat). Hierunter zählen private Anmerkungen zu eigentlich dienstlichen Angelegenheiten, z.B. wenn ein Mitarbeiter seinem Vorgesetzten in einer dienstlichen E-Mail gleich noch seine Urlaubswünsche anträgt[29], oder wenn es, wie bei der Arbeit meist üblich, auch einen kurzen Austausch zwischen Mitarbeitern über private Inhalte gibt,[30] wobei natürlich gemeint ist, dass eine dienstliche E-Mail private Anmerkungen enthält und diese E-Mail nicht rein privater Art ist. Ein Beispiel könnte sein, dass ein Kollege dem anderen in einer dienstlichen E-Mail mitteilt, dass er erst zehn Minuten später in die Mittagspause gehen kann, dass er ihn fragt wie sein Urlaub war, wie es ihm geht, oder wie das Wetter bei ihm (in einer Außen- oder anderen Dienststelle) ist.

Drittens wäre es eine Ausnahme wenn die Nutzung aufgrund eines dienstlichen Anlasses erfolgt. Hierunter fallen z.B. eine E-Mail an die Ehefrau, dass man aufgrund einer dienstlichen Besprechung oder angeordneter Überstunden erst später nach Hause kommt[31], oder bei Verschiebung einer Dienstreise eine E-Mail an die Ehefrau oder Freunde, die man am Zielort der Dienstreise treffen wollte.[32]

Als vierte Ausnahme gilt die Nutzung nach der Installation eines Internetanschlusses. Demnach darf der Beschäftigte in einer ersten Anlernphase auch private Seiten besuchen um sich mit der Nutzung des Internets vertraut zu machen.[33] Heutzutage mag dies jedoch höchstens auf Beschäftigte zutreffen, die sich außer-

[28] Vgl. Besgen/Prinz, § 1 Rn. 20.

[29] Vgl. Hanau/Hoeren, S. 20.

[30] Vgl. Däubler, Rn. 179.

[31] Vgl. Karim, Internet am Arbeitsplatz – Irrtümer, S. 1; Däubler, Rn. 178.

[32] Vgl. Däubler, Rn. 178.

[33] Vgl. Hanau/Hoeren, S. 20.

halb der Arbeit nicht mit dem Internet beschäftigt haben und sich keinerlei Vorkenntnisse verschaffen konnten. Dies dürfte bei jüngeren Beschäftigten kaum noch der Fall sein, denn die Nutzung des Internets gehört heute fast zum Alltagsgebrauch in jüngeren Generationen und ist z.B. in Baden-Württemberg auch Bestandteil des Bildungsplans.[34]

Als fünftes ist es auch fraglich, ob man beim Besuch von Gewerkschaftshomepages von einer privaten Nutzung sprechen kann. Ist der Beschäftigte z.B. in der Personalvertretung, dann wäre der Besuch einer Gewerkschaftshomepage nur schwer als privat klassifizierbar. Bei anderen Beschäftigen ist dies jedoch unklar. Zwar darf man niemanden wegen einer Gewerkschaftszugehörigkeit benachteiligen, aber der Arbeitgeber wird wohl kaum seine Arbeitsmittel und die Arbeitszeit für einen normalen Beschäftigten zur Verfügung stellen müssen, damit dieser sich auf Gewerkschaftshomepages informieren kann. Diese Informationen können nämlich auch ohne Probleme in der Freizeit abgerufen werden.

Als nächstes kommen Ausnahmen in Betracht, bei denen ein überwiegendes privates Interesse des Beschäftigten vorliegt, dies jedoch als Notfall verstanden werden kann. Hierunter zählen „dringende Behördenangelegenheiten und [die] kurzzeitige Kontaktaufnahme mit einem erkrankten nahen Angehörigen“[35] wobei es wiederum Auslegungssache ist, wann eine Behördenangelegenheit z.B. dringend ist. Dies könnte z.B. sein, wenn ein Kontakt zur Behörde nur während der Arbeitszeit hergestellt werden kann. Um sich nach einem erkrankten nahen Angehörigen zu erkundigen dürfte es nicht ausreichend sein, wenn dieser lediglich mit einer Erkältung zu Hause ist, sondern es müsste schon eine ernsthaftere Erkrankung vorliegen.

Zuletzt kommt noch die Ausnahme in Betracht, dass ein Beschäftigter während der dienstlichen Recherche z.B. mittels Suchmaschinen auf Seiten kommt die

---

[34] Vgl. von Hentig, H., Einführung in den Bildungsplan 2004, Bildungsrat Baden-Württemberg (Hrsg.), 2004, S. 7, [Abruf: 12.02.2009], http://www.bildung-staerkt-menschen.de/service/downloads/Sonstiges/Einfuehrung_BP.pdf.

[35] Denzel/Alfes/u.a., S. 4.

nicht mehr dienstlichen Inhalts sind, dies aber ggf. durch die Vorschau bei der Suchmaschine nicht erkenntlich war. Hier kann man dem Beschäftigten jedoch keinen Vorwurf machen, unter der Voraussetzung natürlich, dass er solche Seiten umgehend wieder verlässt. Dies lässt sich auch nachvollziehen sofern ein Überwachungsprogramm installiert ist, welches u.a. die Internetnutzung protokolliert. Welche Daten hierfür genau erhoben werden dürfen, wird noch unter 3.2 genauer erläutert.

2.4 Gestattung der privaten Nutzung von Internet und E-Mail

Der Arbeitgeber kann natürlich in seinem Betrieb die private Nutzung von Internet und E-Mail auch gestatten. Hierbei ist der Aufwand den der Arbeitgeber machen muss, um jedoch geregelte Verhältnisse zu schaffen, recht groß. In diesem Abschnitt wird zum einen darauf eingegangen, welche Regelungs- und Gestaltungsmöglichkeiten es gibt und worauf der Arbeitgeber achten muss, um den Nutzungsumfang zu beschränken um somit eine ausufernde Privatnutzung trotz Gestattung zu unterbinden.

Die Möglichkeiten eine private Nutzung zu gestatten sind schnell aufgezählt. Zum einen kann dies natürlich direkt im Arbeitsvertrag geregelt werden, wobei zu prüfen ist ob eine solche Regelung nicht womöglich als allgemeine Geschäftsbedingungen anzusehen sind.[36] Zum anderen besteht die Möglichkeit durch Betriebsvereinbarung[37], per Aushang, Hinweis im Intranet, Rundmail[38], oder Erklärung im Betrieb.[39] Als Erlaubnis zur privaten E-Mail-Nutzung wird auch die Zuweisung einer zweiten E-Mailadresse für private Kommunikation angesehen.[40]

---

[36] Vgl. Besgen/Prinz, § 1 Rn. 8.

[37] Wobei wieder auf die nicht erlaubte Einschränkung des Fernmeldegeheimnisses unter 2.1 hinzuweisen ist.

[38] Vgl. Besgen/Prinz, § 1 Rn. 6.

[39] Vgl. Denzel/Alfes/u.a., S. 5.

[40] Vgl. Hanau/Hoeren, S. 21.

Die letzte Möglichkeit wäre eine Gestattung durch betriebliche Übung, also durch ein regelmäßiges Verhalten des Arbeitgebers, welches dem Beschäftigten suggeriert sein Verhalten wäre in Ordnung. Als Beispiel zählt hierzu, die Kenntnis des Arbeitgebers von der privaten Nutzung, die er aber nicht verbietet, sondern duldet.[41]

Egal wie die private Nutzung gestattet wird, ist auf jeden Fall gem. § 87 I Nr.1 BetrVG der Betriebsrat im Wege der Mitbestimmung zu beteiligen, da es sich um eine Regelung handelt, die das Verhalten der Beschäftigten regelt.[42]

2.4.1 Betriebliche Übung

Während alle anderen Formen recht eindeutig hergeben, ob eine private Nutzung gestattet ist, so herrscht jedoch Unsicherheit wenn es darum geht zu bestimmen, ob die private Nutzung durch eine betriebliche Übung gestattet wurde. Ob eine betriebliche Übung vorliegt ist regelmäßig vom Beschäftigten zu beweisen.[43] Als möglichen Beweis könnte man die erlaubte private Nutzung des Telefons heranführen. Dies ist in der Literatur strittig.

Ein Teil der Literatur sieht eine E-Mail als „eine Fixierung des Gedankeninhalts (...) [welcher] eher mit einer Postkarte zu vergleichen ist“[44] und sieht durch den Austausch von E-Mails weitere Gefahrenquellen für das System des Arbeitgebers, wodurch eine konkludente Erlaubnis aufgrund erlaubten privaten Telefonierens abzulehnen ist.[45]

Der andere Teil meint, dass so lange die Kosten des Telefonats und der E-Mail in etwa gleichem Rahmen sind, eine private Nutzung von E-Mails durchaus gestattet

[41] Vgl. Hanau/Hoeren, S. 22; Besgen/Prinz, § 1 Rn. 9.

[42] Vgl. Denzel/Alfes/u.a., S. 79.

[43] Vgl. Besgen/Prinz, § 1 Rn. 9.

[44] Denzel/Alfes/u.a., S. 6.

[45] Vgl. Denzel/Alfes/u.a. S. 6-7.

ist.[46] Eine höhere Virusgefahr wird verneint, da die Virus-Gefahr bereits durch den Empfang von dienstlichen E-Mails ausreichend gegeben sei.[47]

Hinsichtlich der Virusgefahr kann der zweiten Auffassung gefolgt werden, da durch jeglichen E-Mail-Verkehr die Virusgefahr erheblich gesteigert wird. Ein entsprechend programmierter Virus kann sich selbst weiter verbreiten und an jeder E-Mail angehängt sein, auch an E-Mails die von einem bekannten dienstlichen Absender kommt. In Bezug auf die Erlaubnis der privaten E-Mail-Nutzung bei erlaubten privaten Telefonaten ist die erste Auffassung nicht tiefreichend genug und der zweiten Auffassung nicht zu folgen. Ihr ist nicht zu folgen, weil sie einen wichtigen Punkt nicht beachtet. Eine Erlaubnis der privaten Nutzung von E-Mails wirkt sich wesentlich weiter aus als bei privaten Telefonaten. Bei Telefonaten ist lediglich das gesprochene Wort als Informationsaustausch vorhanden, welches von einem Arbeitgeber normalerweise nicht nachträglich kontrolliert werden kann. Bei einem schriftlich vorliegenden Informationsaustausch als E-Mail hat der Arbeitgeber jedoch eine weit höhere Sensibilität zu bewahren im Hinblick auf den Datenschutz, sowie größere Einbußen in seinen Kontrollbefugnissen als Arbeitgeber. Eine private Nutzung kann sich aufgrund dieser Argumente nicht konkludent aus der erlaubten privaten Nutzung des Telefons ergeben.[48]

Eine betriebliche Übung kann sich jedoch ergeben, wenn der Arbeitgeber im Browser bereits spezielle Lesezeichen bereitstellt, die nicht für den dienstlichen Gebrauch geeignet sind. [49] Allerdings muss hierbei noch unterschieden werden, ob diese Lesezeichen auch wirklich vom Arbeitgeber angebracht wurden, oder ob es sich um Lesezeichen handelt, die bei der Installation des Internetbrowser automatisch mit installiert wurden. Es kommt dann darauf an, in wie weit gewollt war, dass die Lesezeichen mit installiert werden und ob der Arbeitgeber sie mit angemessenem Aufwand hätte entfernen können.

---

[46] Vgl. Däubler, Rn. 184a; Hanau/Hoeren, S. 21.

[47] Vgl. Hanau/Hoeren, S. 21-22.

[48] Vgl. Besgen/Prinz, § 1 Rn. 23.

[49] Vgl. Däubler, Rn. 184.

Des Weiteren kann sich eine Erlaubnis zur privaten Nutzung auch ergeben, wenn der Arbeitgeber spezielle Internetzugänge bereitstellt, z.B. entsprechende Terminals in der Kantine.[50] Eine Erlaubnis der privaten Nutzung besteht dann jedoch nur an diesen Terminals und nicht auch am Arbeitsplatz, da der Arbeitgeber eine konkrete Abgrenzung getroffen hat.

Zuletzt sei noch erwähnt, dass sich eine Erlaubnis konkludent ergeben kann, wenn die private Nutzung gegenüber dem Beschäftigten abgerechnet wird.[51] Denn durch die Abrechnung wird der Anschein erweckt die private Nutzung wäre gestattet.

2.4.2 Bestimmung des Nutzungsumfangs

Eine Bestimmung des Nutzungsumfangs bei der Gestattung der privaten Nutzung ist der wichtigste Teil. Ohne eine möglichst konkrete Nutzungsbeschreibung kann später nicht bestimmt werden, ob ein Verstoß des Beschäftigten vorlag oder nicht. Dies könnte im Zweifelsfall dem Arbeitgeber zum Nachteil ausgelegt werden. Vor allem deswegen, da der Arbeitgeber den Umfang der privaten Nutzung alleine und frei bestimmen kann.[52]

Um eine konkrete Regelung auszuarbeiten, sollte unter anderem (falls vorhanden) ein Mitarbeiter der EDV-Abteilung anwesend sein, der die Leistungsfähigkeit des Firmennetzwerks kennt und aus technischer Seite beurteilen kann, was möglich ist und was nicht.[53] Danach sollte zuerst der Ort der privaten Nutzung festgelegt werden. Dies kann zum einen der Arbeitsplatz sein, jedoch können auch spezielle Terminals z.B. in der Kantine bereitgestellt werden. Dies kann vorteilhaft sein um private und dienstliche Nutzung konkret abzugrenzen und somit leichter kontrollieren zu können, sowie eine höhere Systemsicherheit zu erreichen, da im Zweifel

[50] Vgl. Denzel/Alfes/u.a., S. 6; Däubler, Rn. 184.

[51] Vgl. Ebenda, S. 6; Ebenda, Rn. 184.

[52] Vgl. Besgen/Prinz, § 1 Rn. 15, 19.

[53] Vgl. Hanau/Hoeren, S. 23.

nur die Computer mit Viren infiziert werden, die lediglich privat genutzt werden.[54]

Der nächste Schritt wäre eine Konkretisierung der Nutzung in Bezug auf:

- ➔ Die maximale Nutzungsdauer pro Tag/Woche/Monat/Jahr.
- ➔ Ob Internet oder E-Mail oder beides privat genutzt werden darf.
- ➔ Verbot des Besuchs bestimmter Internetseiten (z.B. Seiten mit pornographischen, rechtswidrigen Inhalten, Internetcommunities, Chatrooms, Onlinecasinos, Video-Communitys, etc.)
- ➔ Verhaltensweise des Beschäftigten mit privaten E-Mails, z.B. Markierung dieser als privat, damit dem Arbeitgeber die Kontrolle der dienstlichen E-Mails leichter gemacht wird. Oder die Beschränkung privater E-Mails auf den Textbereich, so dass keine privaten Dateianhänge angehängt werden dürfen.
- ➔ Das Herunterladen von Dateien, z.B. eine Begrenzung der Dateien auf eine maximale Größe um eine Belastung des Netzwerks durch zu große Downloads zu verhindern. Und des Weiteren sollte hierbei auch bestimmt werden wo ggf. heruntergeladene Dateien abgespeichert werden dürfen.
- ➔ Verbot und Erlaubnis zum Herunterladen/Nutzen bestimmter Dateiformate. Eine konkrete Erlaubnis von bestimmten Dateiformaten (z.B. pdf, doc, xls) verbietet dem Beschäftigten eine Datei mit nicht genannten Dateiformaten herunterzuladen. Dies kann mitunter die sicherere Lösung sein um einer Virengefahr durch neue Dateiformate vorzubeugen, diese Liste muss allerdings ggf. öfters überarbeitet werden.
- ➔ Verbot bestimmter Internetdienste, z.B. FTP-Anwendungen, Java, Flash, IRC, etc.

[54] Vgl. Besgen/Prinz, § 1 Rn. 24.

- ➔ Die Überwachungsrechte des Arbeitgebers (zur Kontrolle, sowie Löschung und Filterrung bestimmter z.B. rassistischer oder pornographischer Inhalte) sollte ebenfalls konkretisiert werden.

- ➔ Instrumente welche zur Überwachung des Beschäftigten eingesetzt werden dürfen, z.B. Scan-Funktionen, spezielle Software.

- ➔ Eine eventuelle Kostenbeteiligung des Beschäftigten bei privater Nutzung, sowie deren Abrechnung. Hierbei ist insbesondere zu berücksichtigen, ob beim Arbeitgeber eine Flatrate oder eine andere Abrechnungsmethode für das Internet besteht.[55]

Dies sind natürlich nur ein paar Beispiele der wichtigsten Punkte die eine solche Regelung enthalten sollte. Diese Liste kann beliebig gekürzt, erweitert oder detailliert werden.

Eine andere Alternative wäre durch technische Einschränkung des Zugangs dem Mitarbeiter nur bestimmte Internetseiten freizuschalten. Der Zugriff auf diese Seiten kann dann z.B. mittels eines Mitarbeiterportals erfolgen.

Wird die Nutzung nicht konkret geregelt, kann keine grundsätzliche Aussage darüber gemacht werden, was gestattet ist und was nicht. Nur insoweit kann man sich festlegen, dass alles erlaubt ist, was die dienstlichen Belange nicht stört und dem Arbeitgeber keine zusätzlichen Kosten bereitet.[56] Der Aufruf von Seiten mit strafrechtlich verbotenen Inhalten ist selbstverständlich nie gestattet.[57] Bei Seiten mit pornographischen Inhalten ist dies ähnlich, auch wenn diese individuell und heimlich genutzt werden. Das LAG Baden-Württemberg hatte in seinem Beschluss vom 19.10.1993[58] entschieden, dass der individuelle Konsum von Haschisch bei der Arbeit, das Arbeitsverhältnis nicht berührt. Dies sieht Däubler als Vergleich

[55] Vgl. Besgen/Prinz, § 1 Rn. 18.

[56] Vgl. Hanau/Hoeren, S. 24.

[57] Vgl. Besgen/Prinz, § 1 Rn. 21.

[58] Vgl. LAG Baden-Württemberg, NZA 4/1994, S. 175-178.

zum Konsum pornographischer Internetseiten bei der Arbeit. Die restliche Literatur sieht dies jedoch anders, da der Besuch von Seiten im Internet immer Spuren hinterlässt, mit denen Rückschlüsse auf den Seitenbesucher und somit auf den Arbeitgeber gezogen werden können. Der private Haschischkonsum kann dahingegen vollkommen unentdeckt bleiben.[59]

2.5 Regelung durch Dienstvereinbarung [60]

Im Bereich von Behörden, öffentlichen Körperschaften, etc. in denen Personalvertretungen vorhanden sind, ist es gem. § 73 BPersVG, § 73 LPersVG möglich die Einführung und Anwendung von Telekommunikationsdiensten per Dienstvereinbarung zu regeln. Bei einer Dienstvereinbarung können ähnliche Inhalte wie unter 2.3.2 die Nutzung des Internets genauer definieren, sofern die private Nutzung durch die Dienstvereinbarung gestattet werden soll. Eine besonders gute Idee zur Dienstvereinbarung hat die Stadt Oldenburg mit ihrem Gesamtpersonalrat gehabt.[61] Geregelt wurde in dieser Dienstvereinbarung der grundsätzliche Einsatz von Telekommunikations- und Telediensten und zwar umfassend vom Handy, über Voice-Mail bis hin zu Intranet und Fax. Ebenso wie Beweisverwertungsverbote, Löschungsfristen, etc. für alle diese Medien. Zwar ist die Dienstvereinbarung an manchen Stellen sicher verbesserungswürdig wie z.B. fehlen Regelungen zur Krankheitsvertretungen oder der Archivierung der Daten, aber der Grundgedanke eine Dienstvereinbarung abzuschließen, die auf alle Arten von Telekommunikationsdiensten anwendbar ist, war sicherlich eine gute Sache. In der sich heute immer schneller entwickelnden Technologie können somit bis jetzt noch nicht eingesetzte Technologien bereits erfasst werden und es ist letztendlich vielleicht gar nicht oder nur teilweise noch Regelungsbedarf übrig. Des Weiteren kann durch eine Allgemeinhaltung der Regelung ein weites Feld, von Telefon, über Fax, bis hin zum Internet abdeckend geregelt werden, was auch vorteilhaft

[59] Vgl. Besgen/Prinz, § 1 Rn. 21; Hanau/Hoeren, S. 25; Däubler, Rn. 192.

[60] Für diesen Punkt lagen zur Anregung u.a. verschiedene Dienstvereinbarungen vor, deren Veröffentlichung aus verständlichen Gründen nicht gewünscht wurde.

[61] Vgl. Kiper, M., Dienstvereinbarungen zu Telekommunikations- und Telediensten, Der Personalrat 3/2002, S. 104-109.

im Hinblick auf die Transparenz einer Dienstvereinbarung für die Beschäftigten ist. Als Grundlage für eine allgemein gehaltende Begrifflichkeit kann man sich dem Telekommunikationsgesetz bedienen. Dort sind bereits in § 3 TKG zahlreiche Begrifflichkeiten zur Telekommunikation geregelt. Einer weiteren Definition von Begriffen wie Telekommunikation oder Telekommunikationsdienste steht nichts entgegen.

2.6 Rücknahme der Gestattung

Die Rücknahme der Gestattung der privaten Internetnutzung richtet sich danach, wie diese gestattet wurde. Zuerst sei auf jeden Fall erwähnt, dass eine Rücknahme der Gestattung nicht dem Mitbestimmungsrecht des Betriebsrats unterliegt, denn die Gestattung der privaten Nutzung stellt eine freiwillige Leistung des Arbeitgebers dar.[62]

Grundsätzlich sollte schon bei der Gestattung an die Rücknahme gedacht werden. In der Regelung der Gestattung sollte daher entweder ein Freiwilligkeits- oder Widerrufsvorbehalt integriert sein. Der Unterschied bei diesen beiden Möglichkeiten besteht darin, dass bei einem Freiwilligkeitsvorbehalt keine betriebliche Übung entsteht, wodurch die Gestattung jederzeit zurückgenommen werden kann, selbst wenn die private Nutzung über einen längeren Zeitraum gestattet war.[63] Beim Widerrufsvorbehalt muss der Arbeitgeber jedoch nach billigem Ermessen entscheiden und für den Widerruf einen sachlichen Grund vorlegen. Dieser könnte beispielsweise eine durch die private Nutzung hervorgerufene Kostenbelastung oder Störung des Netzwerks sein.[64]

In anderen Fällen kommt lediglich eine Kündigung in Frage. Eine Änderungskündigung kommt in Betracht, wenn die private Nutzung sich durch eine betriebliche Übung ergeben hat und mit den begünstigten Beschäftigten keine Vereinbarung ausgehandelt werden kann. Zu berücksichtigen ist hierbei, dass der Arbeitgeber

[62] Vgl. Denzel/Alfes/u.a., S. 7; Hanau/Hoeren, S. 22; Däubler, Rn. 186.

[63] Vgl. Denzel/Alfes/u.a., S. 8.

[64] Vgl. Däubler, Rn. 188.

gegenüber dem Beschäftigten einen Vertrauenstatbestand geschaffen hat.[65] Eine Änderungskündigung wird jedoch nicht für möglich gehalten, da für diese die dringenden betrieblichen Erfordernisse fehlen, wie sie laut §§ 2 S.1 i.V.m. 1 II S.1 KSchG erforderlich wären. Zudem sind Änderungskündigungen nicht gegenüber allen Beschäftigten möglich und können zu späteren Auseinandersetzungen führen.[66]

Gegebenenfalls ist es auch möglich eine betriebliche Übung durch eine entsprechend lange Gegenübung zurückzunehmen. Die letzte Möglichkeit wäre ansonsten ein Änderungsvertrag.[67]

2.7 Keine Regelung wird getroffen

Wird gar keine Regelung getroffen, so gilt grundsätzlich, dass die Arbeitsmittel nur für die Arbeit zu verwenden sind.[68] Es ist hierbei nicht verlangt, dass der Arbeitgeber ausdrückliche Regelungen ausarbeitet, jedoch kann eine Nichtregelung zu späteren Streitigkeiten führen und es könnte z.B. eine betriebliche Übung entstehen obwohl dies vielleicht gar nicht vorgesehen war.

Falls nun keine Regelung getroffen wurde und somit grundsätzlich nur die dienstliche Nutzung gestattet ist, sind wiederum die Ausnahmen, welche bereits unter 2.3 erläutert wurden, zu berücksichtigen.

3 Maßnahmen bei Verstößen

Verstößt ein Beschäftigter gegen eine zuvor festgelegte Regelung, oder bei einer Nichtregelung gegen den Grundsatz der lediglich dienstlichen Nutzung der Arbeitsmittel, so stehen dem Arbeitgeber eine Reihe arbeitsrechtlicher Maßnahmen zur Verfügung um gegen einen Verstoß vorzugehen. Dies kann wie bei anderen

[65] Vgl. Hanau/Hoeren, S. 22.

[66] Vgl. Däubler, Rn. 188.

[67] Vgl. Denzel/Alfes/u.a., S. 8.

[68] Vgl. Karim, Internet am Arbeitsplatz – Irrtümer, S. 1.

Verstößen gegen arbeitsrechtlichte Pflichten von einer mündlichen Ermahnung, über die Abmahnung bis zur ordentlichen oder außerordentlichen Kündigung reichen bzw. bei Beamten zu Disziplinarmaßnahmen. Im Bezug auf die private Nutzung von Internet und E-Mail hat der Arbeitgeber neben der Beteiligung der Personalvertretungen (und dies nicht nur bei Verstößen, sondern bereits vorher siehe 3.1) außerdem zu beachten, wie er den Beschäftigten kontrollieren darf und ob er seine Beweise überhaupt verwenden kann. Hinzu kommt eine Prüfung auf mögliche Schadensersatzansprüche des Arbeitgebers. Ergänzend wird hierbei auch noch auf die krankheitsbedingte Kündigung eingegangen, die aufgrund der bisher fehlenden eindeutigen Grundlage (der Krankheit oder Sucht), zwar keine wirkliche Rolle bei den Kündigungen spielt, jedoch einmal eine Rolle spielen könnte und daher auch erwähnt wird.

3.1 Rechte der Personalvertretungen

Als Personalvertretungen kommen der Betriebsrat, sowie der Personalrat mit dem jeweils geltenden Betriebsverfassungs-, Bundespersonalvertretungs- oder Landespersonalvertretungsgesetz in Betracht. Im Folgenden ist, sofern nicht ausdrücklich bestimmte Vorschriften genannt werden, immer von allen dreien die Rede. Des Weiteren wird hier nur auf das Personalvertretungsgesetz für das Land Baden-Württemberg eingegangen, wobei in anderen Bundesländern ähnliche Vorschriften zu finden sein dürften.

Wie bereits zuvor angesprochen ist die Personalvertretung nicht nur bei Verstößen zu beteiligen, sondern bereits bei Entscheidungen im Vorfeld. So ist bereits bei der Planung von Arbeitsplätzen an denen Zugänge zu Internet, Intranet, oder E-Mail eingerichtet werden sollen, der Betriebsrat gem. § 90 I Nr.2 und 4 BetrVG, sowie der Personalrat gem. § 68 II BPersVG, bzw. § 68 LPersVG zu unterrichten und dies gem. § 90 II BetrVG mit dem Betriebsrat zu beraten.[69] „Diese Beratung

[69] Vgl. Denzel/Alfes/u.a., S. 78.

muss alle erkennbaren sozialen, personellen, wirtschaftlichen, gesundheitlichen und arbeitstechnische Auswirkungen umfassen.“[70]

3.1.1 Mitbestimmungsrechte

Die Mitbestimmungsrechte greifen ein, so bald der Arbeitgeber eine technische Einrichtung zur Überwachung der Mitarbeiter anbringt (es bestehen also keine Mitbestimmungsrechte bei der Planung[71]), oder wenn die private Nutzung gestattet wird und durch eine Regelung der Nutzungsumfang geregelt wird.

Zuerst wird die Mitbestimmung bei der Einführung und Anwendung von Überwachungseinrichtungen erläutert. Hierbei sind die maßgeblichen Grundlagen § 87 I Nr.6 BetrVG, § 75 III Nr. 17 BPersVG und § 79 III Nr. 12 LPersVG, welche alle von ihrem Wortlaut her ähnlich sind und folgende Begriffe zur Definition offen lassen: „technische Einrichtung“, „Verhalten und Leistung“ und „überwachen“. Des Weiteren enthalten die Normen auch einen Bestimmtheitsbegriff. Dieser ist laut Literatur so auszulegen, dass bereits die objektive Möglichkeit[72] zur Überwachung genügt, um ein Mitbestimmungsrecht auszulösen „(objektiv-finale Theorie)“[73]. Eine solche Möglichkeit kann bereits darin liegen, dass der Arbeitgeber sich den Cache oder den Verlauf des Browser anschaut.[74]

Als erstes wird nun der Begriff der „technischen Einrichtung“ definiert. Unter diesen Begriff fallen „optische, mechanische, akustische, elektronische und sonstige Geräte, sobald ein gewisses Maß an Vergegenständlichung gegeben ist“.[75] Bei Hardwarekomponenten dürfte der Begriff der Vergegenständlichung keine Diskussionsgrundlage darstellen, allerdings ist es fraglich, ob eine Software zur Überwachung der Beschäftigten diesem Begriff noch entspricht. Dies kann bejaht

---

[70] Denzel/Alfes/u.a., S. 78.

[71] Vgl. Hanau/Hoeren, S. 86.

[72] Vgl. Däubler, Rn. 288.

[73] Hanau/Hoeren, S. 85.

[74] Vgl. Hanau/Hoeren, S. 85 m.w.N.

[75] Hanau/Hoeren, S. 78 m.w.N.

werden, da eine Software rein für sich gesehen nutzlos ist. Erst wenn sie in Verbindung mit dem Computer gebracht (installiert) wird, ist sie einsatzbereit. Bei der Beurteilung des Begriffs ist daher auf das gesamte System abzustellen.[76]

Zweitens ist zu definieren, ab wann es der Fall ist, dass das Verhalten und die Leistung der Beschäftigten ermittelt werden. Verhaltensdaten sind nach dem systematischen Zusammenhang des § 87 I BetrVG (dies gilt auch für die anderen Vorschriften der Personalvertretungsgesetze) weit auszulegen. Zu ihnen gehören alle Daten die ein „individuell steuerbares Tun oder Unterlassen (Verhalten) eines Arbeitnehmers enthalten".[77] In der Literatur gibt es auch andere Ansichten, nach denen der Verhaltensbegriff auf Verhaltensweisen bezogen wird, die im Bezug zur Erbringung der Arbeitsleistung stehen. Es wird dabei auf den Schutzzweck der Norm verwiesen unter Hinzuziehung des § 1 II KSchG. Dieser Auffassung kann jedoch nicht gefolgt werden, da die Norm des Kündigungsschutzgesetzes dem Bestandsschutz des Arbeitsverhältnisses dient, wohingegen die Norm des Betriebsverfassungsgesetzes dem Schutz des Persönlichkeitsrechts des Beschäftigten dient und somit viel umfassender ist.[78]

Des Weiteren ist für die Definition des Verhaltens und der Leistung maßgebend, ob die Daten des Überwachungsvorgangs einem einzelnen Beschäftigten zugeordnet werden können. Hierbei ist nicht die Qualität der durch die Überwachung erlangten Daten, sondern das Ergebnis des Vorgangs entscheidend. Es ist auch nicht entscheidend, wie sachgerecht oder vollständig die erlangten Daten sind. Hierzu gibt es Gegenmeinungen, nach denen ein Mitbestimmungsrecht nur greift, wenn das Schwergewicht der Überwachung auf den Daten der technischen Einrichtung ruht. Diese sind jedoch abzulehnen, da die Norm das Persönlichkeitsrecht des Beschäftigten schützen soll und ein Eingriff in dieses bereits vorliegt, wenn die technische Einrichtung nicht hauptsächlich der Überwachung dient. Dies ist beispielsweise der Fall wenn eine Software hauptsächlich der Verarbeitung von

[76] Vgl. Hanau/Hoeren, S. 78.

[77] Hanau/Hoeren, S. 81-82 m.w.N.

[78] Vgl. Hanau/Hoeren, S. 82.

Daten dient, jedoch über diese Verarbeitung und Eingaben am PC nebenbei ein Protokoll anfertigt.

Für die Zuordnung der Daten zu einem Beschäftigten ist es ebenso unerheblich, ob die Zuordnung durch die technische Einrichtung erfolgt, oder dies unter der Hinzuziehung weiterer Daten möglich wird, z.B. durch Hinzuziehung von Schichtplänen.

Bei Arbeitsplätzen, an denen ein oder mehrere Computer durch verschiedene Beschäftigte genutzt werden, ist eine eindeutige Zuordnung nur gegeben wenn die Beschäftigten sich mit einer Kennung anmelden oder wie eben beschrieben dies per Schichtplänen oder ähnlichem zuordenbar ist. Gleichfalls ist eine Überwachung des Verhaltens und der Leistung auch gegeben, wenn die Computer zwar mit einem Standardpasswort von jedem Beschäftigten genutzt werden können, die Nutzung sich jedoch auf eine bestimmte Arbeitsgruppe zuordnen lässt. Da dann über diese Arbeitsgruppe Aussagen über ihr Verhalten und ihre Leistung gemacht werden können.[79]

Drittens muss noch der Überwachungsbegriff festgelegt werden. Hierzu hat das BAG in seiner „Bildschirmarbeitsplatz-Entscheidung“[80] diesen Begriff so definiert, dass eine Überwachung im Sinne der jeweiligen Normen „jeden Vorgang, durch den Informationen über das Verhalten oder die Leistung von Arbeitnehmern erhoben und in aller Regel irgendwie aufgezeichnet werden, um sie der menschlichen Wahrnehmung zugänglich zu machen“[81] darstellt. Demnach ist ein Mitbestimmungsrecht der Personalvertretung bereits bei der Installation eines ganz normalen Browsers unter Beibehaltung der Standardfunktionen (wozu auch die Protokollierung zählt) zu bejahen.[82]

---

[79] Vgl. Hanau/Hoeren, S. 81-85.

[80] BAG, AP Nr.7 zu § 87 BetrVG 1972 Überwachung.

[81] Hanau/Hoeren, S. 79.

[82] Vgl. Hanau/Hoeren, S. 79.

Weiters ist jedoch zu hinterfragen ob ein Mitbestimmungsrecht der Personalvertretung auch besteht wenn ermittelte Daten durch eine andere Einrichtung weiter verarbeitet werden. Werden Daten der Beschäftigten auf einer weiteren technischen Einrichtung gespeichert, z.B. einem extra hierfür bereitgestellten Server, so stellt dies auch eine Einrichtung dar, bei deren Einführung und Anwendung ein Mitbestimmungsrecht besteht.[83] Ein Mitbestimmungsrecht besteht ebenfalls wenn die Daten durch eine weitere technische Einrichtung in irgendeiner Form ausgelesen, also sichtbar oder aufbereitet werden. Werden jedoch Daten nicht technisch weiterverarbeitet, so dass sie für arbeitsrechtliche Maßnahmen, z.B. Abmahnung aufgelistet werden o.ä., dann ist zumindest im Hinblick auf die Überwachung kein Mitbestimmungsrecht mehr gegeben.[84]

Ein paar Sonderfälle sind noch abzuhandeln. Zum einen die Frage wie sich das Mitbestimmungsrecht auswirkt, wenn eine neue Softwareversion der Überwachungseinrichtung aufgespielt wird. Unter der Anwendung versteht sich nämlich auch jede Veränderung oder Erweiterung der Einrichtung. Wird mit der neuen Softwareversion die technische Einrichtung z.B. bei der Aufbereitung der Daten verbessert, so ist ein Mitbestimmungsrecht bereits gegeben. Zum anderen besteht noch die Frage, wie es denn mit der Mitbestimmung aussieht, wenn die technische Einrichtung vor der Wahl einer Personalvertretung bereits installiert wurde. Der Personalvertretung steht hierbei ebenfalls ein Mitbestimmungsrecht zu, jedoch mit einer Übergangszeit von ca. einem Jahr. In dieser Zeit ist die Nutzung der Einrichtung mitbestimmungsfrei, wird jedoch rechtswidrig, wenn innerhalb dieses Zeitraums keine Einigung mit dem Arbeitgeber darüber erzielt werden kann.[85]

Abschließend ist noch zu erwähnen, dass das Mitbestimmungsrecht der Personalvertretung nicht dadurch umgangen werden kann, indem man einen Dritten mit der Überwachung beauftragt. Der Arbeitgeber hat in einem solchen Fall die Verträge mit dem Dritten so zu gestalten, dass das Mitbestimmungsrecht der Perso-

[83] Vgl. Hanau/Hoeren, S. 79-80.

[84] Vgl. Hanau/Hoeren, S. 79.

[85] Vgl. Hanau/Hoeren, S. 87.

nalvertretung gewahrt bleibt und dass die Regelung des § 11 BDSG beachtet wurde.[86]

Um das Mitbestimmungsrecht auszuschließen wäre es nun noch denkbar die Daten der Beschäftigten entsprechend zu anonymisieren. Dies erscheint grundsätzlich möglich, sofern eine echte Anonymisierung der Daten der Beschäftigten vorliegt. Eine echte Anonymisierung bedeutet, dass gem. § 3 VI BDSG die personenbezogenen Daten so verändert werden, dass eine Aussage über persönliche oder sachliche Verhältnisse nicht mehr möglich ist. Eine unechte Anonymisierung besteht, wenn eine Aussage über die Daten der Beschäftigten nur noch mit unverhältnismäßig großem Aufwand getroffen werden können. Um eine echte Anonymisierung durchzuführen, müssten die Daten bereits anonymisiert sein, bevor sie von einem Programm wie z.B. Outlook genutzt werden. Dies ist technisch ohne Probleme möglich, jedoch verringert sich die Qualität der Daten nach dem aktuellen technischen Stand derart, dass diese unbrauchbar werden. Eine echte Anonymisierung ist also nach bisherigen Kenntnissen nicht möglich. Das Mitbestimmungsrecht der Personalvertretungen kann somit bis heute nicht durch das Anonymisieren der Daten ausgeschlossen werden.[87]

Nun ist noch die Mitbestimmung gem. § 87 I Nr.1 BetrVG, § 75 III Nr. 15 BPVG und § 79 I Nr. 12 LPVG zu erwähnen. Demnach haben die Personalvertretungen ein Mitbestimmungsrecht wenn es um Fragen der Ordnung und des Verhaltens der Beschäftigten geht. Hierunter fallen entsprechende Vereinbarungen, die den Nutzungsumfang von Internet und E-Mail regeln (siehe Punkt 2.3.2).[88]

3.1.2 Mitbestimmungsfrei

Mitbestimmungsfreie Entscheidungen des Arbeitgebers sind unter anderem Weisungen, worunter z.B. die Anweisung fällt, das Internet lediglich dienstlich zu nutzen.

---

[86] Vgl. Hanau/Hoeren, S. 88.

[87] Vgl. Hanau/Hoeren, S. 90-95.

[88] Vgl. Denzel/Alfes/u.a., S. 79.

Ebenso mitbestimmungsfrei ist die Entscheidung des Arbeitgebers, wie die E-Mail-Adresse gestaltet werden soll (z.B. mit Vor- und Nachname), oder in welchem Umfang sich die Beschäftigten bei einer gestatteten privaten Nutzung an den entstehenden Kosten beteiligen müssen.[89]

3.2 Verwertbarkeit von Beweisen und Kontrolle der Beschäftigten aufgrund der gesetzlichen Grundlagen

Ein weiterer Punkt der bereits im Vorfeld vom Arbeitgeber beachtet werden sollte ist, wie er überhaupt seine Beschäftigten überwachen darf und was getan werden muss um erlangte Beweise überhaupt später verwenden zu können. Es besteht ein ausdrückliches Beweisverwertungsverbot, wenn entweder das gerade unter 3.1.1 beschrieben Mitbestimmungsrecht verletzt wurde, oder wenn der Rahmen der zulässigen Kontrolle verletzt wurde.[90]

Mitbestimmungsrechte bzw. deren Normen in den jeweiligen Gesetzen dienen dem Schutz der Beschäftigten. Nicht nach diesen Normen erlangte Beweise dürfen bei einem Prozess nicht verwertet werden, außer der Beschäftigte würde diese selbst in den Prozess mit einbringen. Eine Gegenansicht meint, dass auch Beweise verwertet werden dürfen, die nicht nach den Regeln der Mitbestimmung erlangt wurden. Diese müssten unter Abwägung des „Recht auf Beweis auf Arbeitgeberseite und der Menschenwürde und des allgemeinen Persönlichkeitsrechts des Arbeitnehmers“[91] evtl. mit einbezogen werden um der Wahrheitsfindung zu dienen. Dem ist jedoch nicht zu folgen, da in unserem Rechtssystem die absolute Wahrheitsfindung nicht um jeden Preis erlangt werden soll und es nicht sein kann, dass Arbeitgeber, die sich rechtmäßig verhalten und die Personalvertretungen mitbestimmen lassen, womöglich in einem Prozess später schlechter gestellt sind, als Arbeitgeber, die diese Schutzregelungen übergehen.[92]

---

[89] Vgl. Denzel/Alfes/u.a., S. 79.

[90] Vgl. Denzel/Alfes/u.a., S. 85.

[91] Denzel/Alfes/u.a., S. 86.

[92] Vgl. Denzel/Alfes/u.a., S. 86-87.

Bei der Überwachung oder Kontrolle der Beschäftigten ist zu beachten, dass diese Kontrollen nur stichprobenweise erfolgen dürfen und nicht auf Dauer die Beschäftigten überwachen. Hier anzusprechen ist die sog. „Mikrozensus-Entscheidung" des BVerfG welches besagt, dass eine detaillierte Aufzeichnung der Daten verboten ist.[93] In Fortsetzung dessen ist zu unterscheiden, ob im Unternehmen die private Nutzung oder nur die dienstliche Nutzung gestattet ist. Ist nur die dienstliche Nutzung gestattet, so kann der Arbeitgeber jegliche Daten die auf dem Computer des Beschäftigten gespeichert sind kontrollieren. Hier besteht kein Schutz der Persönlichkeitssphäre des Beschäftigten. Anders ist dies, wenn die private Nutzung gestattet ist. Hierbei darf die Kontrolle nur soweit gehen, dass die arbeitsvertraglichen Pflichten eingehalten werden.[94]

Einen besonderen Schutz genießen zudem angestellte Berufsgeheimnisträger wie Ärzte, Rechtsanwälte oder Betriebs- bzw. Personalräte. Ihre Tätigkeit beinhaltet u.a. die Möglichkeit von Dingen Kenntnis zu erlangen, die sie nicht an Ihren Arbeitgeber weiter geben dürfen und über die sie schweigen müssen. Zu nennen wären hier beispielsweise die Vorschriften des § 203 StGB, § 78 BetrVG, § 8 BPersVG, § 10 LPersVG. Die Überwachung oder Kontrolle der Computer oder des Nutzungsverhaltens dieser besonderen Personengruppen ist daher grundsätzlich unzulässig.[95]

Bis jetzt wurde generell dargestellt was im Bezug auf Überwachung und Kontrolle erlaubt ist und was nicht und in wie weit Personalvertretungen zu beteiligen sind. Nun folgend werden die für Überwachungsvorgänge, Kontrolle und Speicherung von Daten relevanten, gesetzlichen Vorschriften näher erläutert. Dabei wurden die Rechtsgrundlagen des neu gefassten Telekommunikationsgesetzes und des neuen Telemediengesetzes und der damit außer Kraft getretenen Gesetzes und Verordnungen berücksichtigt. Zu erwähnen ist noch, dass über all diesen Gesetzen

[93] Vgl. Denzel/Alfes/u.a., S. 77.

[94] Vgl. Besgen/Prinz, S. 94-95.

[95] Vgl. Denzel/Alfes/u.a., S.77-78.

das allgemeine Persönlichkeitsrecht, welches sich aus Art. 2 I GG ergibt, thront und jeder Zeit bei Abwägungsvorgängen zu beachten ist.

3.2.1 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz dient dem Schutz der Daten und somit des Persönlichkeitsrechts der betroffenen Personen gem. § 1 I S.1 BDSG. Es gilt gem. § 1 II BDSG bei allen öffentlichen und nicht-öffentlichen Stellen die Daten erheben, verarbeiten und nutzen und sofern es keine spezielleren Regelungen z.B. bei Landesstellen die Landesdatenschutzgesetze gibt. Nicht öffentliche Stellen sind gem. § 2 IV BDSG natürliche und juristische Personen, Gesellschaften und andere Personengesellschaften unter weiteren Voraussetzungen. Sofern das Telekommunikations- und Telemediengesetz im Folgenden keine spezielleren Regelungen enthalten, gilt das Bundesdatenschutzgesetz als lex generalis.[96]

Das Bundesdatenschutzgesetz findet Anwendung, wenn in die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten (siehe hierzu § 3 I BDSG) entweder gem. § 4 I BDSG i.V.m. § 4a BDSG eingewilligt wurde, dies per Rechtsvorschrift gem. § 4 BDSG erlaubt oder angeordnet wurde, oder dies zur Erfüllung eigener Geschäftszwecke gem. § 28 BDSG zulässig ist. Gem. § 28 I Nr.1 BDSG ist dies zulässig bei Vertragsverhältnissen, worunter ein Arbeitsvertrag fällt und gem. § 28 I Nr.2 BDSG zur Wahrung berechtigter Interessen des Arbeitgebers. Bei dieser zulässigen Erhebung, Verarbeitung und Nutzung muss das allgemeine Persönlichkeitsrecht gewahrt bleiben, sofern der Arbeitgeber nicht, wie eben genannt, ein berechtigtes Interesse hat und somit ein Eingriff gerechtfertigt wird.

Gerechtfertigte Eingriffe des Arbeitgebers bestehen demnach bei

- dienstlichen E-Mails
- Gefahr der Weitergabe von Firmengeheimnissen
- Störung, Überlastung oder zum Schutz des Firmennetzwerks

[96] Vgl. Denzel/Alfes/u.a., S. 63.

- zur Vermeidung zusätzlicher Kosten
- Einsatz von Arbeitszeit zur privaten Nutzung.[97]

Ungerechtfertigt erscheinen demnach Eingriffe bei

- privaten E-Mails bei gestatteter privater Nutzung
- Einträge in z.B. einem privaten Onlinetagebuch.[98]

Egal ob die Eingriffe gerechtfertigt oder ungerechtfertigt sind, so hat der Arbeitgeber auf jeden Fall gem. § 9 BDSG die Datensicherheit zu gewährleisten. Hierzu müssen angemessene technische und organisatorische Maßnahmen getroffen werden.[99]

Zusätzlich hat der Arbeitgeber eine Pflicht den Beschäftigten über den Gebrauch der Daten zu benachrichtigen und ggf. Auskunft zu geben gem. §§ 33, 34 BDSG. Hiervon gibt es eine Reihe von Ausnahmetatbeständen, so muss der Arbeitgeber den Beschäftigten z.B. nicht benachrichtigen, wenn die Daten aufgrund gesetzlicher Vorschriften gespeichert werden (§ 33 II Nr.2 BDSG).

Werden die Daten z.B. nicht mehr für den bestimmten Zweck benötigt (§ 35 II Nr.3 BDSG), oder ist ihre Speicherung unzulässig (§ 35 II Nr.1 BDSG), so sind diese gem. § 35 BDSG wieder zu löschen. Hier finden sich zudem weitere Fälle, bei denen die Daten zu löschen sind, wobei noch § 35 II Nr.2 BDSG genannt sei, wonach die Daten zu löschen sind, wenn die Daten über die rassische oder ethnische Herkunft, politische Meinungen, etc. Auskunft geben. Im Fall der privaten Nutzung des Internets und der Überwachung wäre § 35 II Nr.3 BDSG zutreffend, so dass die Daten zu löschen sind, so bald der Zweck für den sie erhoben wurden nicht mehr vorhanden ist.

---

[97] Vgl. Denzel/Alfes/u.a., S. 63-64; vgl. Krauß, C., Internet am Arbeitsplatz, Herberger, M. (Hrsg.), Saarbrücken 2009, Abs. 23-27, [Abruf: 12.02.2009], http://www.jurpc.de/aufsatz/20040014.htm.

[98] Vgl. Krauß, C., Abs. 23-27.

[99] Vgl. Denzel/Alfes/u.a., S. 64.

Die Vorschriften des Bundesdatenschutzgesetzes sind unter bestimmten Voraussetzungen abdingbar. Dazu zählt zum einen die Einwilligung des Betroffenen gem. § 4 I BDSG, sofern die Einwilligung den Voraussetzungen des § 4a BDSG genügt. Hierunter zählt vor allem, dass die Einwilligung auf freier Entscheidung des Betroffenen getroffen wurde und das Schriftformerfordernis. [100]

Eine weitere Möglichkeit um die Vorschriften des Bundesdatenschutzgesetzes abzubedingen, besteht in der Betriebsvereinbarung als „andere Rechtsvorschrift" gem. § 4 I BDSG. Hierbei wurde unter 2.1 bereits das Fernmeldegeheimnis kurz angesprochen, welches nicht durch Betriebsvereinbarung abbedungen werden kann. Ebenso darf nicht das Recht des Beschäftigten auf informationelle Selbstbestimmung umgangen werden, welches sich aus dem Allgemeinen Persönlichkeitsrecht gem. Art. 2 I GG ergibt. Eine Abdingbarkeit kann deshalb nur unter den Beschränkungen von § 75 II BetrVG erfolgen.

3.2.2 Landesdatenschutzgesetz Baden-Württemberg

Das Landesdatenschutzgesetz Baden-Württemberg beinhaltet weitgehend Vorschriften mit ähnlichen Inhalten wie das Bundesdatenschutzgesetz mit ein paar Abweichungen, die hier kurz genannt werden. In anderen Bundesländern können ähnliche, jedoch auch abweichende Regelungen vorhanden sein, die je nachdem, in welchem Bundesland man sich befindet, zu prüfen sind.

Zum ersten findet das Landesdatenschutzgesetz gem. § 2 LDSG nur Anwendung bei Behörden und öffentlichen Stellen, juristischen Personen und sonstigen Vereinigungen, die öffentliche Aufgaben wahrnehmen, sowie solche an denen juristische Personen des öffentlichen Rechts mit absoluter Anteils- oder Stimmmehrheit beteiligt sind.

Die Begriffsbestimmungen des § 3 LDSG ähneln denen des § 3 BDSG und sind nur in Teilen noch deutlicher erläutert, werden hier aber nicht weiter vertieft.

[100] Vgl. Denzel/Alfes/u.a., S. 64.

Ebenso ähnelt der § 4 LDSG dem § 4 BDSG. Denn ebenso ist gem. § 4 I Nr.1 und 2 LDSG eine Verarbeitung personenbezogener Daten nur aufgrund eines Gesetzes oder aufgrund einer Einwilligung des Betroffenen zulässig. Die Einwilligung des § 4 LDSG ist hierbei der Einwilligung des § 4a BDSG ähnlich, wobei nach § 4 II S.4 LDSG der Betroffene noch darauf hinzuweisen ist, dass er die Einwilligung widerrufen kann. Ansonsten ist ebenso die Schriftform erforderlich.

Neben dem Datengeheimnis in § 6 LDSG hat der Arbeitgeber auch zu beachten, welche Rechte dem Betroffenen nach § 5 LDSG zustehen. Dort sind alle Rechte des Betroffenen wie Auskunft, Berichtigung, Löschung, etc. aufgelistet. Diese Rechte können gem. § 5 I S.2 LDSG nicht durch Rechtsgeschäfte ausgeschlossen oder beschränkt werden.

Im Bezug auf den Punkt 3.1.1, den Mitbestimmungsrechten der Personalvertretungen (bzw. hier wenn Dritte mit der Überwachung betraut werden), sei der § 7 LDSG erwähnt, welcher dem Arbeitgeber vorschreibt, dass er trotz der Vergabe der Datenverarbeitung an eine andere Stelle, weiterhin für die Einhaltung der Vorschriften des Landesdatenschutzgesetz und anderer Gesetze verantwortlich bleibt.

Zuletzt ist noch § 33 LDSG anzusprechen, welcher die Verarbeitung besonderer Arten von personenbezogenen Daten regelt. Nach § 35 II Nr.2 BDSG sind Daten über rassische oder ethnische Herkunft, politische Meinungen, etc. zu löschen. Nach § 33 LDSG dürfen diese Daten jedoch unter gewissen Voraussetzungen verarbeitet werden. Dies wäre z.B. der Fall aufgrund einer Rechtsvorschrift, aufgrund einer Einwilligung des Betroffenen oder zum Schutz lebenswichtiger Interessen des Betroffenen.

3.2.3 Telekommunikationsgesetz

Eine weitere gesetzliche Grundlage stellt das Telekommunikationsgesetz dar. Bevor nun begonnen wird das Telekommunikationsgesetz genauer zu durchleuchten, sei erwähnt, dass die Telekomunikations-Datenschutzverordnung mit Wirkung vom 26.06.2004 gem. § 152 II TKG im Wesentlichen in das Telekommunikationsgesetz übernommen wurde.

Im Fall der privaten Nutzung des Internets am Arbeitsplatz hat das Telekommunikationsgesetz als einfacher Gesetzesvorbehalt gem. Art. 10 II S.1 GG, den Zweck, das sich aus Art. 10 GG ergebende Fernmeldegeheimnis zu wahren. Das Fernmeldegeheimnis umfasst gem. § 88 I TKG den Inhalt, sowie die näheren Umstände, insbesondere die Beteiligung an einem Telekommunikationsvorgang, also auch die Verbindungsdaten. Dasselbe gilt bei erfolglosen Verbindungsversuchen, was z.B. bei der privaten E-Mail-Nutzung eine E-Mail sein könnte, die nicht an den Empfänger zugestellt werden konnte.

Verpflichtet zur Wahrung des Fernmeldegeheimnisses ist gem. § 88 II S.1 TKG jeder Diensteanbieter, wobei zu definieren ist, wer ein Diensteanbieter ist. Eine Definition ist in § 3 Nr. 6 TKG zu finden. Demnach ist ein Diensteanbieter „jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt“. Telekommunikation ist gem. § 3 Nr. 22 TKG „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“, welche in § 3 Nr. 23 TKG nochmals genau definiert sind und zu denen z.B. Computer zählen. Als geschäftsmäßiges Erbringen von Telekomunikationsdiensten versteht man gem. § 3 Nr. 10 TKG „das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“. Ein Unternehmen oder eine Behörde hat bei der Erbringung von Telekommunikation an seine Beschäftigten keine Gewinnerzielungsabsichten, was jedoch unerheblich ist.

Was Telekommunikationsdienste sind, wird in § 3 Nr. 24 TKG als „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen“ definiert. Die Erbringung von diesen Diensten an die Beschäftigten des eigenen Unternehmens stellt hierbei eine Ausnahme der Regel dar. Abschließend ist nun jedoch noch zu klären wer „Dritte“ sind, was umstritten ist.

Nach einer Ansicht der Literatur ist der Beschäftigte Dritter egal ob er das Internet privat oder dienstlich gebraucht, weil i.S.v. § 3 Nr.10 TKG Dritter der ist, dem der Telekommunikationsdienst technisch erbracht wird. Der Gegenmeinung nach liegt eine Erbringung des Telekommunikationsdienstes an Dritte nicht vor bei lediglich

dienstlicher Nutzung. Dieser Gegenmeinung ist auch zu folgen, da aufgrund der Begründung des § 82 II TKG a.F.[101], welcher nun fast wortgleich als § 88 II TKG zu finden ist, eine Erbringung von Telekommunikationsdiensten in Betrieben und Behörden nur besteht, wenn die Möglichkeit besteht die Anlage privat zu nutzen. Der Beschäftigte ist also nur bei gestatteter privater Nutzung als Dritter zu sehen und somit auch nur dann das Telekommunikationsgesetz anzuwenden.

Besteht nun also eine Gestattung der privaten Nutzung des Internets, so darf sich der Arbeitgeber (Diensteanbieter) nur in soweit Kenntnis von der Telekommunikation verschaffen, wie es für die Erbringung der Telekommunikationsdienste nötig ist gem. § 88 III TKG. Eine weitere Nutzung der Daten außer für diese Telekommunikationszwecke ist, bis auf Ausnahmefälle wie z.B. zur Störungsbeseitigung gem. § 100 TKG, untersagt.[102] Er hat den Beschäftigten gem. § 93 I TKG bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten zu unterrichten. Hierbei muss jedoch nicht über die eingesetzte Technik aufgeklärt werden. Es wird sich in der Praxis anbieten diese Unterrichtung in ein Vertragsformular und Merkblatt für den Beschäftigten aufzunehmen um einen Beweis für die Unterrichtung zu haben und für den Beschäftigten die Möglichkeit im Zweifel nachzuschauen.[103]

Des Weiteren hat der Arbeitgeber entsprechende technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses, der personenbezogenen Daten und gegen den Unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme zu treffen gem. § 109 I TKG.[104]

---

[101] Vgl. Bundesgesetzblatt Teil I 1996, 25.07.1996, S. 1120.

[102] Vgl. Denzel/Alfes/u.a., S. 54-55.

[103] Vgl. Büttgen, P., Kommentar zu § 93 TKG, in: Abel, H. (Hrsg.): Praxiskommentare Telemediengesetz, Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, Kissing 2007, S. 121-122 (im Folgenden zitiert als „Praxiskommentar TMG, TKG, TKÜV“).

[104] Vgl. Denzel/Alfes/u.a., S. 55-56.

3.2.4 Telemediengesetz

Das Telemediengesetz hat am 01.03.2007 die bisher geltenden Regelungen des Teledienstegesetz, des Teledienstedatenschutzgesetz und des auf Landesebene geltenden Mediendienste-Staatsvertrags in sich vereint.

Damit das Telemediengesetz angewendet werden kann, dürfen gem. § 1 I S.1 TMG keine Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, vorliegen. Dies ist i.d.R. nicht der Fall, denn im Normalfall wird in einer Firma eine E-Mail, oder ein Abruf einer Seite im Internet nicht nur übermittelt, sondern auch verfasst, beantwortet, etc. Es liegt also eine Komponente vor, die sich auch mit dem Inhalt dieser Sachen befasst. Es liegt somit kein Telekommunikationsdienst vor, der ganz mit der Übertragung zu tun hat.[105] Des Weiteren ist ausdrücklich in § 1 I S.2 TMG genannt, dass diese Vorschrift für private wie öffentliche Stellen gilt, egal ob diese ein Entgelt dafür verlangen oder nicht.[106] Diese Regelung ist ähnlich der des § 3 Nr. 10 TKG, wonach es unerheblich ist, ob die Telekommunikation mit oder ohne Gewinnerzielungsabsicht erfolgt.

Nun sind die Begriffsbestimmungen des § 2 TMG zu bestimmen. Ein Dienstean-bieter ist gem. § 2 Nr.1 TMG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.“ Unter diesen Begriff kann eindeutig der Arbeitgeber subsumiert wer-den, ebenso wie hier u.a. auch öffentlich-rechtliche Körperschaften oder ähnliche öffentlich-rechtliche Rechtsformen. Eine Ausnahme hiervon stellt lediglich der Konzern dar, bei dem die Verantwortlichkeit den einzelnen Konzerngesellschaften zuzurechnen ist.[107]

---

[105] Vgl. Geis, I., Internetzugang und E-Mail, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 13 m.w.N..

[106] Vgl. Geis, I., Private Anbieter und öffentliche Stellen, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 14.

[107] Vgl. Geis, I., Kommentar zu § 2 TMG, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 19.

Als nächstes ist zu prüfen ob der Beschäftigte Nutzer im Sinne des § 2 Nr.3 TMG ist. Nach dem Wortlaut „jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen“ ist dies zu bejahen. Hierbei ist es egal ob die Telemedien dazu genutzt werden private oder dienstliche Zwecke zu erfüllen.[108]

Gem. § 7 II TMG ist der Arbeitgeber (Diensteanbieter) nicht verpflichtet übermittelte oder gespeicherte Informationen auf rechtswidrige Inhalte zu überwachen unter den Voraussetzungen der §§ 8-10 TMG.

Nach § 8 I TMG sind die Voraussetzungen bei der Durchleitung von Informationen:

- dass der Arbeitgeber die Übermittlung nicht veranlasst,
- den Adressaten der Informationen nicht ausgewählt und
- die übermittelten Informationen nicht ausgewählt oder verändert hat.

Ist dies der Fall, so ist der Arbeitgeber bei der Durchleitung (und gem. Abs. 2 bei der automatischen,[109] kurzzeitigen Zwischenspeicherung) nicht für rechtswidrige Informationen verantwortlich.

Diese automatische, kurzzeitige Zwischenspeicherung wird in § 9 TMG noch konkretisiert. Demnach darf der Arbeitgeber, um nicht für die Übermittlung der Informationen verantwortlich zu sein, die Informationen nicht verändern, er muss die Bedingungen für den Zugang zu den Informationen, sowie die festgelegten Industriestandards zur Aktualisierung und Sammlung der Informationen beachten. Zusätzlich muss er unverzüglich handeln, wenn er Kenntnis erlangt, dass die Informationen an ihrem ursprünglichen Ausgangsort, oder von einem Gericht oder einer Verwaltungsbehörde gesperrt oder gelöscht wurden.

---

[108] Vgl. Geis, I., Kommentar zu § 2 TMG, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 21.

[109] Vgl. Geis, I., Kommentar zu § 8 TMG, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 57.

Als Drittes ist die Speicherung von Informationen in § 10 TMG konkretisiert. Hierbei kann sich der Arbeitgeber gem. § 10 S.2 TMG nicht der Verantwortung entziehen. Der Beschäftigte untersteht dem Arbeitgeber und dieser hat Möglichkeiten auf den Beschäftigten Einfluss zu nehmen, z.B. durch Abmahnungen, Kündigung.[110] Allerdings kann hier nicht gemeint sein, dass der Arbeitgeber für rechtswidrige Handlungen und die Speicherung von rechtswidrigen Informationen durch den Beschäftigten die komplette Verantwortung übernimmt. Viel mehr wird man prüfen müssen in welchem Umfang der Arbeitgeber eine Mitverantwortung hat. Diese Mitverantwortung wird man verringern können wenn der Arbeitgeber nochmal ausdrücklich die Speicherung rechtswidriger Informationen verboten hat und diese gelegentlich kontrolliert.

Als nächstes ist in Abschnitt 4 des Telemediengesetzes der Datenschutz geregelt. Man muss wieder differenzieren zwischen privater und dienstlicher Nutzung. Denn gem. § 11 I Nr.1 TMG gelten diese Vorschriften nicht, wenn die Daten im Rahmen eines Dienst- oder Arbeitsverhältnisses erhoben und verwendet werden. Ist die private Nutzung jedoch gestattet, so sind die folgenden Vorschriften zu beachten.

In § 12 TMG sind grundsätzliche Dinge geregelt. So darf der Arbeitgeber personenbezogene Daten nur erheben, oder für andere Zwecke als die Bereitstellung der Telemedien nutzen, wenn dies das Telemediengesetz, oder eine anderen Rechtsvorschrift es erlaubt, die sich ausdrücklich auf Telemedien bezieht, oder der Nutzer eingewilligt hat. Eine solche andere Rechtsvorschrift kann auch eine Betriebsvereinbarung wie unter 3.2.1 sein. Außerdem besteht gem. Abs.3 ein Koppelungsverbot. Dieses Verbot soll den Nutzer (Beschäftigter) schützen, indem man die Bereitstellung der Telemedien nicht davon abhängig machen darf, dass der Beschäftigte zustimmt, dass seine Daten auch für andere Zwecke genutzt werden dürfen. In Abs.4 werden diese Daten zusätzlich geschützt, auch wenn sie nicht automatisiert verarbeitet werden, sprich auch eine Auswertung die nicht

[110] Vgl. Geis, I., Kommentar zu § 10 TMG, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 65.

durch einen Computer o.ä. erfolgt steht unter dem Schutz des Telemediengesetzes.[111]

§ 13 TMG regelt die Pflichten des Arbeitgebers (Diensteanbieters). Er hat nach Abs.1, ähnlich wie in § 93 I TKG, den Nutzer (Beschäftigter) über Art, Umfang und Zweck der Erhebung und Verwendung der Daten zu unterrichten. Eine solche Unterrichtung muss erfolgen bevor der Beschäftigte die Telemedien nutzt. Dies stellt kein Problem dar, wenn der Beschäftigte bereits bei Abschluss des Arbeitsvertrags eine entsprechende Einwilligung unterschrieben und ein Merkblatt erhalten hat. Zusätzlich muss jedoch noch gem. Abs.3 der Nutzer auf sein Recht gem. § 13 II Nr.4 TMG hingewiesen werden, wonach er seine Einwilligung mit Wirkung für die Zukunft jeder Zeit wiederrufen kann.

Wichtig zu wissen für den Arbeitgeber ist noch, dass er gem. § 13 IV TMG umfassende Vorkehrungen zu treffen hat um den Schutz der Daten technisch und organisatorisch sicherzustellen.

Die §§ 14 und 15 TMG unterscheiden im Folgenden noch zwischen Bestands- und Nutzungsdaten. Bestandsdaten sind danach gem. § 14 I TMG Daten die für das Vertragsverhältnis maßgebend oder von Nöten sind, während Nutzungsdaten gem. § 15 I TMG solche sind die für die Inanspruchnahme und Abrechnung der Nutzung von Telemedien nötig sind.

3.2.5 Telekommunikations-Überwachungsverordnung

Abschließend sei noch kurz die Telekommunikations-Überwachungsverordnung angesprochen. Weshalb diese nur kurz angesprochen wird, wird sich gleich zeigen.

Gem. § 3 I TKÜV sind Verpflichtete nach dieser Vorschrift jene, die Telekommunikationsdienste für die Öffentlichkeit erbringen. In der Regel wird bei Behörden und Unternehmen eine geschlossene Benutzergruppe vorliegen die aufgrund ihres Dienst- oder Arbeitsverhältnisses Zugriff auf die Telekommunikationsdiens-

[111] Vgl. Geis, I., Kommentar zu § 12 TMG, in: Abel, H. (Hrsg.): Praxiskommentar TMG, TKG, TKÜV, S. 75-76.

te des Arbeitgebers hat. Eine Ausnahme wäre hingegen, wenn z.B. in der Kantine oder im Eingangsbereich ein öffentlich zugänglicher Internetzugang bereitgestellt wäre. Denn dann könnte jedermann auf diese Telekommunikationsdienste zugreifen.

In der Regel sind somit die meisten Unternehmen und die Behörden von der Telekommunikations-Überwachungsverordnung befreit. Weiterhin können jedoch Verpflichtungen bestehen die Aufzeichnung oder Überwachung der Telekommunikationsanlagen gem. des G-10-G oder AWG zu ermöglichen.[112]

3.3 Schadensersatzanspruch des Arbeitsgebers

Damit der Arbeitgeber gegenüber seinem Beschäftigten einen Schadensersatzanspruch geltend machen kann, muss der Beschäftigte vertragswidrig handeln. Bei einer lediglich dienstlich gestatteten Nutzung ist dies in der Regel nicht problematisch wenn eine private Nutzung nachgewiesen wird. Ist jedoch die private Nutzung erlaubt, muss geprüft werden in welchem Umfang der Beschäftigte vertragswidrig gehandelt hat. Hierbei ist es nun von Vorteil wenn ein Nutzungsumfang der privaten Nutzung wie unter 2.3.2 genauer bestimmt wurde. Letztendlich muss jedoch der Arbeitgeber in beiden Fällen nachweisen, dass die private Nutzung nicht erlaubt war, der beschuldigte Beschäftigte den Computer in diesem Moment genutzt hat, welcher Art und Dauer die Nutzung war, sowie in welcher Höhe ein Schaden entstanden ist.[113]

Verletzt nun ein Beschäftigter seine Vertragspflichten indem er privat surft, so könnte der Arbeitgeber seinen Anspruch entweder aus einer positiven Forderungsverletzung gem. § 280 I BGB oder gem. § 823 I BGB als Eigentumsverletzung oder Eingriff in den ausgeübten Gewerbebetrieb geltend machen. Diese Schadensersatzansprüche greifen auch ein, wenn der Beschäftigte vertragswidrig

[112] Vgl. Denzel/Alfes/u.a., S. 61-62.

[113] Vgl. Besgen/Prinz, § 1 Rn. 135.

gehandelt hat, indem durch seine private Nutzung Daten verloren gegangen sind, oder das Netzwerk oder der Computer durch Viren geschädigt wurde.[114]

Ist die private Nutzung gestattet worden und der Beschäftigte hat trotzdem gegen seine vertraglichen Pflichten verstoßen, so sind zudem die Grundsätze des innerbetrieblichen Schadensausgleichs zu beachten, wobei die Haftung nach leichtester, mittlerer und grober Fahrlässigkeit sowie Vorsatz zu unterscheiden ist.[115]

Zu klären ist nun noch, welche Kosten denn für den Schadensersatzanspruch überhaupt geltend gemacht werden können. In erster Linie wäre dies einmal der Ersatz der „verbummelten" Arbeitszeit, sowie von Kosten für die Datenübertragung oder Nutzungsdauer des Internet. Allerdings auch nur, wenn der Arbeitgeber keine Flatrate besitzt sondern eben so nach Datenübertragung oder Nutzungsdauer bei seinem Internetanbieter bezahlen muss. Hinzu kommen die zur Aufdeckung des Vertragsverstoßes nötig gewesenen Recherchekosten, worunter auch Detektivkosten fallen können falls der Arbeitgeber einen konkreten Tatverdacht hat und der Beschäftigte dessen überführt wird. Des Weiteren kommen ein Ersatz von Schäden der durch Viren entstanden ist und ein Ersatz der Aufwendungen um die Viren wieder zu entfernen und ggf. Dokumente, Dateien, etc. wieder herzustellen in Frage.

Für den überführten Beschäftigten kommt am Ende zwar dasselbe heraus, aber der Vollständigkeit halber sei noch erwähnt, dass eine Lohnkürzung rechtlich grundsätzlich unzulässig ist um die Schadensersatzansprüche geltend zu machen. Stattdessen kann der Schadensersatz durch eine Aufrechnung bei der Lohnzahlung geltend gemacht werden, bei der jedoch die Pfändungsfreigrenzen zu beachten sind.[116]

---

[114] Vgl. Denzel/Alfes/u.a., S. 95.

[115] Vgl. Besgen/Prinz, § 1 Rn. 136; Denzel/Alfes/u.a., S. 95; Hanau/Hoeren, S. 40; Pauly, S./Osnabrügge, Dienstliche und private Nutzung von Internet, Überlassung und Nutzung von Arbeitsmitteln, in: Besgen, N./Prinz, T. (Hrsg.): Neue Medien und Arbeitsrecht, Bonn 2006, § 6 Rn. 21.

[116] Vgl. Besgen/Prinz, § 1 Rn. 135, 137.

3.4 Abmahnung

Soll dem Beschäftigten deutlich gemacht werden, dass sein Verhalten nicht geduldet wird, so gibt es natürlich die Möglichkeiten dies in Form von Mitarbeitergesprächen, mündlichen Ermahnungen, Sperrung des Internets und ähnlichem zu erreichen.[117] Wird jedoch in Erwägung gezogen, das Arbeitsverhältnis mit dem Beschäftigten aufgrund seines Verstoßes nicht mehr weiterführen zu wollen, so muss man, sofern nicht ein wichtiger Grund gem. § 626 I BGB vorliegt der eine außerordentliche Kündigung (dazu später unter 3.6) rechtfertigt, zuerst einmal den Beschäftigten abmahnen um ihm beim nächsten Verstoß ordentlich kündigen zu können. Hierdurch wird das Ultima-Ratio-Prinzip erfüllt, demnach zuerst das mildeste Mittel zu wählen ist. Für ein Verfahren vor Gericht ist die Abmahnung als mildestes Mittel und bei einer ordentlichen Kündigung die wichtigste Voraussetzung. Als Vorgriff auf den nächsten Punkt sei hierbei auch gesagt, dass es sich bei einer ordentlichen Kündigung um eine verhaltensbedingte Kündigung handelt.

Der Betriebs- oder Personalrat ist bei einer schriftlichen Abmahnung grundsätzlich nicht zu beteiligen. Eine Ausnahme bildet hier der § 80 I Nr. 8 Buchstabe c LPersVG, wonach der Personalrat bei der Abmahnung mitwirkt wenn der Beschäftigte dies beantragt.

Grundsätzlich sei zur Abmahnung gesagt, dass diese eine Doppelfunktion erfüllt, zum einen ist sie Voraussetzung für eine ordentliche Kündigung (dazu dann unter 3.5) und zum anderen wirkt sie mit ihrer Warnfunktion darauf hin, dem Beschäftigten sein Fehlverhalten aufzuzeigen und das Arbeitsverhältnis mit ihm fortzusetzen.

Damit eine Abmahnung jedoch wirksam wird, sind eine Reihe formaler Wirksamkeitsvoraussetzungen einzuhalten und zu beachten. Da diese dieselben sind wie bei Abmahnungen aufgrund anderer arbeitsrechtlicher Verstöße, werden im Folgenden nur ein paar wichtige Punkte angerissen. Hierunter zählt z.B., dass eine Abmahnung trotz ihrer Formfreiheit schriftlich erfolgen sollte um für ein mögli-

[117] Vgl. Besgen/Prinz, § 1 Rn. 128-133.

ches Gerichtsverfahren einen Beweis in den Händen zu halten. Der Inhalt der Abmahnung muss unter anderem Inhalt, Ort und Zeitpunkt des Fehlverhaltens sein, im Rahmen der erlaubten Überwachung der Beschäftigten bei der Internetnutzung kann dies mittels Logdateien recht genau erfolgen. Um der angesprochenen Warnfunktion der Abmahnung gerecht zu werden, sollte diese möglichst innerhalb von zwei Wochen erfolgen, nachdem der Arbeitgeber Kenntnis von dem Verstoß erhalten hat.[118] Aufpassen muss man jedoch, wenn man den Beschäftigten aufgrund desselben oder ziemlich ähnlicher Verstöße bereits abgemahnt hat. Werden mehr als drei Abmahnungen wegen desselben oder sehr ähnlicher Verstöße ausgesprochen, so können diese ihre Warnfunktion verlieren.[119]

3.5 Ordentliche Kündigung

Soll einem Beschäftigten ordentlich gekündigt werden, so sind grundsätzlich die Kündigungsfristen des § 622 BGB, sowie das Schriftformerfordernis des § 623 BGB mit Namensunterschrift gem. § 126 I BGB, mit Besonderheiten beim Mutterschutz-, Seemanns- und Berufsbildungsgesetz zu beachten. Eine nicht schriftlich erklärte Kündigung ist gem. § 125 I BGB nichtig.[120]

Bevor eine Kündigung gegenüber dem Beschäftigten erfolgt, ist vorher noch die Personalvertretung gem. § 102 I S.1 BGB zu hören, bzw. darf gem. § 79 I S.1 BPersVG; § 77 I S.1 LPersVG mitwirken. Des Weiteren ist zu beachten ob das Kündigungsschutzgesetz Anwendung findet.

Das Kündigungsschutzgesetz findet gem. § 23 I KSchG nur Anwendung auf Verträge nach dem 31. Dezember 2003, wenn das Unternehmen in der Regel zehn oder mehr Beschäftigte ausschließlich Lehrlinge hat. Bei Verträgen vor dem 31. Dezember 2003 sind es lediglich fünf oder mehr Beschäftigte ausschließlich Lehrlinge. Außerdem muss das Vertragsverhältnis gem. § 1 I KSchG zu dem betroffenen Beschäftigten länger als sechs Monate bestehen um das Kündigungsschutzge-

[118] Vgl. Besgen/Prinz, § 1 Rn. 67-73.

[119] Vgl. Besgen/Prinz, § 1 Rn. 82.

[120] Vgl. Denzel/Alfes/u.a., S. 91.

setz anwenden zu können. Das Kündigungsschutzgesetz findet keine Anwendung bei Angestellten in leitender Stellung gem. § 14 KSchG.

Liegt nun ein Fall vor mit einem Beschäftigten auf den das Kündigungsschutzgesetz anzuwenden ist, so muss gem. § 1 II KSchG der Kündigungsgrund in der Person oder dem Verhalten des Beschäftigten liegen. In Frage kommt hierbei nur ein Grund, der im Verhalten des Beschäftigten liegt. Grundsätzlich kann der Beschäftigte durch eine unerlaubte private Nutzung des Internets entweder gegen den Leistungs- oder Vertrauensbereich verstoßen. Ein Verstoß gegen den Vertrauensbereich z.B. durch das Abrufen rechtswidriger Inhalte wird regelmäßig ein Grund für außerordentliche Kündigungen sein, was im nächsten Punkt erst angesprochen wird. Eine ordentliche Kündigung kommt daher in Betracht, wenn der Beschäftigte den Leistungsbereich, also den Anspruch des Arbeitgebers auf Leistungserbringung verletzt, wobei kleinere Verstöße auch kumulativ gewertet werden können. Es ist hierbei zudem von Nöten, dass neben einer Abmahnung auch eine negative Zukunftsprognose erstellt wird, die darlegt, dass der Beschäftigte wiederholt gegen seine Vertragspflicht zur Leistungserbringung durch eine unerlaubte private Nutzung des Internets verstoßen wird.[121]

3.6 Außerordentliche Kündigung

Für eine außerordentliche Kündigung ist ein wichtiger Grund gem. § 626 I BGB nötig.[122] Ähnlich wie bei der ordentlichen Kündigung, ist gem. § 102 I BetrVG der Betriebsrat, bzw. Personalrat gem. § 79 III BPersVG und § 77 III LPersVG zu hören.

Genauer zu prüfen ist nun, ob der Sachverhalt einen wichtigen Grund darstellen kann. Es muss hierbei ein Pflichtverstoß vorliegen, dessen Rechtswidrigkeit und dass dessen Entdeckung nicht ohne Konsequenzen bleiben wird, selbst dem Beschäftigten einleuchtet. Dies ist der Fall, wenn

[121] Vgl. Denzel/Alfes/u.a., S. 91-92.

[122] Vgl. Denzel/Alfes/u.a., S. 92.

- der Beschäftigte das Internet exzessiv nutzt, also in einem die das übliche Maß überschreitendem Umfang nutzt[123],
- der Beschäftigte den Ruf des Unternehmens durch sein Verhalten schädigt, was wiederum der Fall ist, wenn er
    - rechtsradikale, pornographische, pädophile, sodomistische Seiten besucht,[124]
    - seinen Arbeitgeber im Internet, z.B. in Foren oder ähnlichem beleidigt,[125]
    - im Internet straftätig wird, durch z.B. Beziehung kinderpornographischer Schriften gem. § 184b I Nr.3 StGB, Verletzung von Geschäftsgeheimnissen gem. § 203 StGB, § 17 UWG, Ausspähen von Daten gem. § 202a StGB, Computerbetrug gem. § 263a StGB[126].

Des Weiteren muss eine umfassende Abwägung der Interessen an dem Bestandsschutz und der Beendigung des Arbeitsverhältnisses erfolgen. Unter Berücksichtigung des Ultima-Ratio-Prinzips, der negativen Zukunftsprognose und des Übermaßverbots muss sich ergeben, dass eine außerordentliche Kündigung das richtige anzuwendende Mittel ist.[127]

Exkurs: Onlinesucht

Bevor nun auf die krankheitsbedingte Kündigung eingegangen wird, soll vorher der Begriff der Onlinesucht oder auch Onlineabhängigkeit näher erläutert werden. Richtig lautet der Begriff Abhängigkeit oder Missbrauch, nach dem die WHO 1964 den Begriff der Sucht umformulierte. Im Folgenden wird daher die Online-

[123] Vgl. BAG, NZA 2/2006, S. 98-101.

[124] Vgl. ArbG Düsseldorf, NZA 24/2001, S. 1387-1388; ArbG Hannover, NZA 18/2001, S. 1022-1024.

[125] Vgl. Denzel/Alfes/u.a., S. 95.

[126] Vgl. Denzel/Alfes/u.a., S. 95.

[127] Vgl. Denzel/Alfes/u.a., S. 93-94.

abhängigkeit genannt, auch wenn umgangssprachlich weiterhin von Onlinesucht gesprochen wird.

Eine Onlineabhängigkeit gehört zu der Gruppe der stoffungebundenen, oder auch psychischen[128] Abhängigkeiten, da diese eine bestimmte Verhaltensweise darstellt und nicht den Konsum von Suchtmitteln.[129] Die Definition dessen, was Onlineabhängigkeit ist, bleibt jedoch je nach Zweck sehr unterschiedlich. Für diese Diplomarbeit eignet sich am besten folgende: „Die normalen Lebensgewohnheiten, berufliche und persönliche Pflichten werden dabei meist vernachlässigt, das Internet ist das einzige was noch zählt. Im Extremfall wird die virtuelle Welt zu einem Ersatz für die sonst üblichen realen sozialen Kontakte“.[130]

Fraglich bleibt jedoch ob Onlineabhängigkeit eine Krankheit darstellt. Um dies zu beurteilen fehlen bisher ausreichende und wissenschaftlich korrekt ermittelte Studien, Kriterien und Ursachen. Die bisher vorhandenen Studien zur Onlineabhängigkeit befindet die Deutsche Hauptstelle für Suchtfragen e.V. als „unbefriedigend“. [131] Man kann lediglich wage sagen was die Gründe für eine Onlineabhängigkeit sein können. Hierunter zählen „Einsamkeit, Unzufriedenheit, Stress, Langeweile, Depressionen, Probleme, Unsicherheit oder Angst“. [132]

Aufgrund der fehlenden Kriterien und Bestimmbarkeit, wann jemand onlineabhängig ist, wird es in der Praxis sehr schwer werden dies nachzuweisen. Wichtig ist hierbei, wie bei allen anderen Abhängigkeiten auch, auf eventuelle Anzeichen zu achten. Hilfestellungen hierzu bietet für Arbeitgeber, aber auch Betroffene und

---

[128] Vgl. Thommes, N., Onlinesucht am Arbeitsplatz, Saarbrücken 2007, S. 23.

[129] Vgl. Thommes, S. 16.

[130] O.A., Überdosis www...wenn chatten zur Sucht wird, [Stand: 24.04.2006], http://www.t-online.at/toat2/generator/at/Multimedia/Computer/TippsundTricks/TippsundTricks,CmC=434354,CmPart=www.t-online.at.html zitiert bei Thommes, S. 22.

[131] Deutsche Hauptstelle für Suchtfragen e.V., Stellungnahme zum Thema „Online-Sucht“ für die Anhörung des Deutschen Bundestags – Ausschuss für Kultur und Medien – am 9. April 2008, Hamm 2008, S. 1.

[132] Thommes, S. 27.

Angehörige, der Verein HSO 2007 e.V., welcher ironischer weise im Internet unter http://www.onlinesucht.de zu finden ist.

Bei krankheitsbedingten Kündigungen wegen einer Onlineabhängigkeit muss man daher, aufgrund der fehlenden wissenschaftlichen Erkenntnisse, sehr vorsichtig umgehen. Eine Onlineabhängigkeit wird bisher auch nur in Extremfällen als Krankheit eingeordnet. Entscheidende Kriterien sind hierfür der Verlust der Kontrolle über die Onlinezeit, ein starkes Verlangen, Entzugserscheinungen, soziale Probleme durch die Onlineabhängigkeit und ein sozialer Rückzug, trotz der möglichen, negativen Folgen für den Betroffenen[133], was mitunter sogar bis dahin führen kann Freundschaften und Beziehung abzubrechen um mehr Zeit für die Onlineabhängigkeit zu haben.

3.7 Krankheitsbedingte Kündigung

Entgegen einiger Meinungen, dass eine Kündigung während oder wegen einer Krankheit unzulässig wäre, so gibt es im Arbeitsrecht jedoch keine Norm die dem Arbeitgeber untersagt einem Beschäftigten wegen oder während einer Krankheit zu kündigen. Das haben sogar Tarifvertragsparteien erkannt und entsprechend tarifvertragliche Regelungen getroffen, indem z.B. die ordentliche Kündigung wegen Krankheit beschränkt und die außerordentliche sogar ganz ausgeschlossen wird.[134]

Es gibt bei einer krankheitsbedingten Kündigung eine ordentliche und eine außerordentliche Kündigung. In beiden Fällen hat die Personalvertretung ein Recht auf Anhörung bzw. Mitwirkung wie es bereits unter 3.5 und 3.6 angesprochen wurde. Bevor nun jedoch auf die Kündigung eingegangen wird, sollte vorher der Krankheitsbegriff genauer unter Augenschein genommen werden, vor allem unter Berücksichtigung der Arbeitsunfähigkeit.

[133] Vgl. Lepke, A., Kündigung bei Krankheit, Berlin 2003, S. 138.

[134] Vgl. Lepke, S. 141-148.

Als erstes ist der medizinische Krankheitsbegriff zu nennen. Nach diesem ist es ohne Bedeutung ob ein Verschulden vorliegt und es ist ebenso egal ob die Erkrankung durch das Berufs- oder Privatleben hervorgerufen wurde.[135] Der medizinische Krankheitsbegriff ist daher wie folgt formulierbar: „Unter Krankheit im medizinischen Sinne wird nach dem derzeitigen Erkenntnisstand der Wissenschaft ein ärztlich diagnostizierbarer, nach außen in Erscheinung tretender, auf die Funktionstauglichkeit abgestellter Körper-, Geistes- oder Seelenzustand verstanden, der in der Regel durch eine ärztliche Heilbehandlung behoben, die Krankheit erträglich zu machen und ihre Folgen zu lindern oder zumindest vor einer drohenden Verschlimmerung bewahrt werden kann.“[136] Es ist hierbei unerheblich ob die Krankheit geheilt werden kann, sie muss nur behandelbar sein.[137]

Von diesem medizinischen Krankheitsbegriff wird auch der arbeitsrechtliche Krankheitsbegriff abgeleitet, jedoch mit dem Zusatz, dass die Krankheit den Beschäftigten in seiner Leistungsfähigkeit einschränken muss.[138] Deshalb ist es auch möglich, dass je nach Einzelfall, eine Krankheit zwar vorliegt, diese aber nicht zur Arbeitsunfähigkeit führt. Eine Person die z.B. lediglich im Schreibdienst tätig und mal heiser ist, kann noch sehr gut arbeiten, während eine Telefonistin wohl kaum ihre Arbeit erledigen können wird.[139] Der zuvor angesprochene Fall der Onlineabhängigkeit kann hierbei zu einem der besonderen Fälle krankheitsbedingter Arbeitsunfähigkeit gezählt werden.[140] Wie man hierzu vorgehen kann um dem Beschäftigten ordentlich oder außerordentlich zu kündigen, kann jedoch mangels Erfahrungen nicht deutlich geklärt werden. Man wird als Arbeitgeber evtl. wie bei anderen Abhängigkeiten dem Beschäftigten die Chance geben müssen durch eine Therapie seine Abhängigkeit zu bekämpfen, zusätzlich muss man als Arbeitgeber

[135] Vgl. Lepke, S. 119-121.

[136] Lepke, S. 119-120.

[137] Vgl. Lepke, S. 120.

[138] Vgl. Lepke, S. 122.

[139] Vgl. Lepke, S. 123-124.

[140] Vgl. Lepke, S. 128 ff.

berücksichtigen, in wie weit man durch betriebliche Veränderungen die Onlineabhängigkeit des Beschäftigten bekämpfen kann. Dies könnte bereits schlichtweg dadurch erfolgen, dem Beschäftigten einen Arbeitsplatz zur Verfügung zu stellen, der keinen Internetanschluss hat.

3.8 Disziplinarverfahren

Während man bei Arbeitnehmern und Arbeitern Abmahnung und Kündigung anwenden kann, kommen bei Beamten andere Vorschriften und Instrumente zum Einsatz. Denkbar sind natürlich auch Mitarbeitergespräche, Weisungen, etc., doch wenn diese keine Wirkung zeigen, bleibt bei privater Internetnutzung nur noch die Möglichkeit eines Disziplinarverfahrens. Ohne nun auf die rechtlichen Grundlagen genau einzugehen, so richtet sich das Disziplinarverfahren nach den jeweils geltenden Landesdisziplinarordnungen oder Landesdisziplinargesetzen, sowie dem Bundesdisziplinargesetz bei Bundesbeamten. In der Regel sind in den Disziplinarvorschriften die Maßnahmen des Verweises, der Geldbuße, der Kürzung der Dienstbezüge, eine Zurückstufung, oder im schlimmsten Fall eine Entfernung aus dem Dienst vorgesehen. Je nach Schwere des Vorfalls der privaten Internetnutzung wird zu entscheiden sein, welche der Maßnahmen angemessen erscheint.

Nehmen wir nun mal an der Beamte hat während der Dienstzeit vorsätzlich kinderpornographische Seiten besucht, so kommt sogar auch die Möglichkeit des Verlustes des Beamtenstatus aufgrund eines rechtskräftigen Urteils mit einer Freiheitsstrafe von mehr als einem Jahr gem. § 48 I Nr.1 BBG, § 66 I Nr.1 LBG in Betracht.

4 Private Nutzung des Internets als Motivationsfaktor

Nachdem nun vor allem davon gesprochen wurde wie man die private Nutzung des Internets einschränken oder verbieten kann, um die Beschäftigten dazu zu bringen ihrer Arbeit nachzugehen, so gibt es jedoch auch die Möglichkeit die private Nutzung des Internets als Motivationsfaktor zu nutzen. Dies wird natürlich nur in Unternehmen möglich sein, in denen die private Nutzung sonst nicht mög-

lich oder untersagt ist, denn wenn eine private Nutzung bereits gestattet ist wird der Motivationsfaktor relativ gering ausfallen.

In den meisten Unternehmen werden bereits Instrumente eingesetzt um die Leistung der Beschäftigten zu erfassen und zu beurteilen. Diese Instrumente könnte man sich zu Nutze machen, um guten Beschäftigten einen zusätzlichen Bonus zu geben indem sie das Internet privat nutzen dürfen. Das kann man, wenn ein Internetanschluss sowieso vorhanden ist, bereits einfach umsetzen, indem man diesen Beschäftigten schlichtweg die Erlaubnis dazu gibt. Wobei auch wieder ein gewisser Nutzungsumfang begrenzt werden sollte wie unter 2.3.2. Die Signalwirkung sollte auf jeden Fall sein, dass der Arbeitgeber dem Beschäftigten zeigt, dass er gute Arbeit leistet und er ihm deswegen das Vertrauen schenkt, das Internet in gewissem Umfang privat zu nutzen. Vorausgesetzt werden sollte, dass die Arbeitsleistung weiterhin gut bleibt und es sollte bemerkt werden, dass der Bonus bei einer schlechten nächsten Beurteilung zurückgenommen werden kann.

Die Möglichkeit die Beschäftigten durch eine private Internetnutzung zu motivieren ist zudem gem. § 3 Nr.45 EStG steuerfrei.[141]

5 Fazit und Ausblick

In dieser Arbeit sollte das Thema der privaten Nutzung des Internets am Arbeitsplatz erläutert und erklärt werden. Voraussetzung dafür ist, dass arbeitsrechtliche Grundkenntnisse vorhanden sind, da man sonst zur genauen Erläuterung und Erklärung der allgemeinen arbeitsrechtlichen Aspekte wesentlich ausführlicher schreiben müsste. Daher wurden insbesondere die kritischen Punkte herausgearbeitet, durch die man gewisse Stolpersteine des Arbeitsrechts sowie anderer Vorschriften erkennen kann. Insbesondere kamen beamtenrechtliche und landesrechtliche Aspekte hinzu, auf Grundlage der Vorschriften des Landes Baden-Württemberg, z.B. zum Personalvertretungs- und Beamtenrecht sowie Datenschutz.

[141] Vgl. Denzel/Alfes/u.a., S. 102-103.

Zusätzlich zu den angesprochenen Vorschriften sollte die Theorie nicht nur einen abstrakten Sachverhalt wiedergeben, sondern es wurden an den möglichen Stellen kurze, praktische Beispiele eingebaut. Diese wurden teilweise aus der Literatur übernommen, zusätzlich zu der Literatur ergänzt oder gar selbst erdacht. Hinzu kommt, dass die Vorschriften des Telekommunikations- und Telemediengesetzes aufgrund des Außerkrafttretens bzw. der Vereinigung einiger alter Gesetze völlig neu berücksichtigt werden mussten, was in der bisher erschienen Literatur noch nicht der Fall war.

Das Thema wurde außerdem hauptsächlich aus der Sicht des Arbeitgebers geschrieben. Diese Sichtweise erschien die sinnvollste zu sein, da regelmäßig der Arbeitgeber derjenige ist, der durch dieses Thema stärker berührt ist, da er seine Produktivität aufrecht und die Sicherheit seiner Netzwerke erhalten möchte. Der Beschäftigte hat dahingegen oft ein geringeres Interesse das Internet am Arbeitsplatz privat zu nutzen.

Wichtig war es vor allem auch darzustellen, dass im Fall der Internetnutzung am Arbeitsplatz, ob jetzt dienstlich oder privat, es nicht nötig ist darauf zu warten, dass der Gesetzgeber oder die Rechtsprechung eindeutige Regelungen schaffen. Es gibt zwar in einigen Punkten gewiss Differenzen bei denen man entweder der einen oder der anderen Ansicht folgen kann und bei denen natürlich noch Klarheit geschaffen werden muss. Doch der Arbeitgeber und auch die Beschäftigten, bzw. ihre Vertreter in den Personalvertretungen, können bereits jetzt durch sinnvolle und klar formulierte Regelungen einem Rechtsstreit vorbeugen. Dies ist im beiderseitigen Interesse. Hierbei sollte jedoch von beiden Seiten beachtet werden, dass nicht nur Regelungen über vorhandene Sachverhalte getroffen werden, sondern dass man auch den Blick in die Zukunft wahrt, da sich weder Computer- und Telekommunikationstechnik, noch Internet auf einer gewissen Stufe einpendeln, sondern immer noch weiter entwickeln werden. In den nächsten Jahren wird hierzu insbesondere das Thema des „Mitmach-Internet“, oder Web 2.0 verstärkt auftreten da hierdurch der Einzelne noch mehr an das Internet gebunden wird. Dies erfolgt insbesondere durch die Möglichkeit soziale Kontakte vermehrt im Internet wahrzunehmen, insbesondere bei sog. sozialen Netzwerken.

Aber auch elektronische Dienstleistungen und Kommunikation via Internet werden sich stark weiter entwickeln, genannt seien hierbei Entwicklungen wie das e-Government, oder die DE-Mail, wodurch sich der Kontakt zu Behörden verbessert und sicherer wird. Aus Sicht der Unternehmen und Behörden im Blick auf ihre Kunden verändert sich die Kommunikation ebenfalls zusehends, indem immer mehr Informationen und Hilfestellungen im Internet angeboten werden, z.B. Softwareupdates oder Hilfekataloge für Produkte, oder durch das Steuerprogramm Elster der Finanzämter.

Ebenso wird es zukünftig wichtig sein, die Mitarbeiter im sinnvollen Einsatz des Internets zu unterstützen. Es gibt genügend Seiten auf denen man sich sowohl sinnvoll im Hinblick auf die Arbeit gute Informationen holen, sich jedoch auch privat beschäftigen kann. Um hier nicht Grauzonen zu schaffen und insbesondere zu verhindern, dass Mitarbeiter unnötig Zeit im Internet vergeuden, indem sie u.a. auch aufgrund mangelnder Kenntnisse nicht gut genug oder falsch recherchieren, kann man diese in mehrfacher Hinsicht schulen. Die Mitarbeiter sollten dabei lernen Informationen sinnvoll zu unterscheiden, Suchmaschinen richtig einzusetzen und verschiedene Wissensplattformen richtig zu nutzen.

Als Alternative zu dieser Unterstützung der Mitarbeiter, kann man als Arbeitgeber auch die Nutzung des Internets gezielt in seinem Sinne steuern. Dies kann durch die Möglichkeit erfolgen, für Beschäftigte mit einfachen Tätigkeiten Mitarbeiterportale einzurichten. Diese bestehen meist aus einer oder einer geringen Anzahl von Seiten, auf denen die Mitarbeiter eine begrenzte Anzahl von Seiten finden auf denen sie sich dienstlich informieren können. Gerade Arbeitsplätze mit einfachen Tätigkeiten eignen sich hierfür besonders, da die Beschäftigten nur selten Informationen aus dem Internet benötigen und dann meist ganz gezielte.

6 Literaturverzeichnis

Abel, Horst G. (Hrsg.): Praxiskommentare – Telemediengesetz, Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, Kissing 2007

Besgen, Nicolai/Prinz, Thomas (Hrsg.): Neue Medien und Arbeitsrecht – Internet, E-Mail und andere moderne Kommunikationsmittel, Bonn/Berlin 2006

Büttgen, Peter: Kommentar TKG, in: Abel, Horst G. (Hrsg.): Praxiskommentare – Telemediengesetz, Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, Kissing 2007

Däubler, Wolfgang: Internet und Arbeitsrecht, Frankfurt am Main 2004

Denzel, Berthold/Alfes, Kerstin/Heide, Sven/u.a.: Private Nutzung des Internet am Arbeitsplatz – personalpolitische und rechtliche Überlegungen, Norderstedt 2003

Deutsche Hauptstelle für Suchtfragen e.V.: Stellungnahme zum Thema „Online-Sucht“ für die Anhörung des Deutschen Bundestags – Ausschuss für Kultur und Medien am 9. April 2008, Hamm 2008 [Anlage 1 - Seite LXIV]

Ernst, Stefan: Der Arbeitgeber, die E-Mail und das Internet, in: NZA, 19. Jahrgang, 11/2002, S. 585-591

Geis, Ivo: Kommentar TMG, in: Abel, Horst G. (Hrsg.): Praxiskommentare – Telemediengesetz, Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, Kissing 2007

Hanau, Peter/Hoeren, Thomas (Hrsg.): Private Internetnutzung durch Arbeitnehmer – Die arbeits- und betriebsverfassungsrechtlichen Probleme, Schriftenreihe Information und Recht, Band 34, München 2003

Kiper, Manuel: Dienstvereinbarungen zu Telekommunikations- und Telediensten (DV E-Mail und Internet), in: Der Personalrat, 3/2002, S. 104-109

Koeppen, Thomas: Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz – Deutschland, Großbritannien und USA im Vergleich, Schriftenreihe Arbeitsrechtliche Forschungsergebnisse, Band 92, Hamburg 2007

Lepke, Achim: Kündigung bei Krankheit – Handbuch für die betriebliche, anwaltliche und gerichtliche Praxis, Berlin 2003

Markus, Wolfram: Bits, Bytes und Papier, in: Der Gemeinderat, 52. Jahrgang, 1/2009, S. 14-16

Markus, Wolfram: Workflow und mehr Wissen, in: Der Gemeinderat, 52. Jahrgang, 1/2009, S. 18-19

O.A., Vernetzte Verwaltungen, in: Der Gemeinderat Spezial, August 2008, S. 24-25.

Pauly, Stephan/Osnabrügge, Stephan: Überlassung und Nutzung von Arbeitsmitteln, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.): Neue Medien und Arbeitsrecht – Internet, E-Mail und andere moderne Kommunikationsmittel, Bonn/Berlin 2006

Servati, Al/Bremner, Lynn/Iasi, Anthony: Die Intranet Bibel, Las Vegas 1996

Thommes, Nicola: Onlinesucht am Arbeitsplatz – Die Bewertung aus der Sicht des Sektors Unternehmen, Saarbrücken 2007

7 Internet-Literaturverzeichnis

Arbeitskreis der Datenschutzbeauftragten: Datenschutz bei der Nutzung von Internet und Intranet, Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern (Hrsg.), Schwerin 2000, [Abruf: 12.02.2009], http://www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/default.htm [Anlage 2 - auf CD beiliegend]

Arbeitskreis Medien: Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, o.O. 2007, [Abruf: 12.02.2009], http://www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/oh-arbeitsplatz.pdf [Anlage 3 - auf CD beiliegend]

Bauer, Oliver/Tenz, Beate, Acht von Zehn Unternehmen in Deutschland haben Zugang zum Internet, in: Statistisches Bundesamt (Hrsg.): Informations- und Kommunikationstechnologie in Unternehmen, Wiesbaden 2008, [Abruf: 15.01.2009], http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Querschnittsveroeffentlichungen/WirtschaftStatistik/Informationsgesellschaft/IKTUnternehmen1207,property=file.pdf [Anlage 4 - auf CD beiliegend]

Feil, Thomas: Private E-Mail- und Internetnutzung am Arbeitsplatz: Viele Fragen, wenig Antworten, Hannover 2006, [Abruf: 12.02.2009], http://www.recht-freundlich.de/download/eMail-Nutzung_2006-02-13.pdf [Anlage 5 - auf CD beiliegend]

Gehlen, Benjamin: Dürfen Chefs jede E-Mail lesen und Internetnutzung kontrollieren?, Europa-Kontakt e.V. (Hrsg.), o.O. 2002, [Abruf: 12.02.2009], http://www.verdi-innotec.de/upload/m3dbe933223f78_verweis1.pdf [Anlage 6 - auf CD beiliegend]

Heidrich, Joerg: Private Internetnutzung am Arbeitsplatz/I, Hannover 2003, [Abruf: 12.02.2009], http://www.heise.de/ix/artikel/2003/01/110/default.shtml [Anlage 7 - auf CD beiliegend]

Heidrich, Joerg: Private Internetnutzung am Arbeitsplatz/II, Hannover 2003, [Abruf: 12.02.2009], http://www.heise.de/ix/artikel/2003/02/094/ [Anlage 8 – auf CD beiliegend]

Hensche, Martin: Informationen zum Thema Kündigung wegen Krankheit, Berlin 2008, [Abruf: 12.02.2009], http://www.hensche.de/Rechtsanwalt_Arbeitsrecht_Handbuch_Kuendigung_Krankheitsbedingt.html [Anlage 9 - auf CD beiliegend]

Jouran, Karim R.: Internet am Arbeitsplatz – Irrtümer, Feil, Thomas (Hrsg.), Hannover 2005, [Abruf: 12.02.2009], http://www.recht-freundlich.de/download/Internet_am_Arbeitsplatz_Irrtuemer_2005-07-29.pdf [Anlage 10 - Seite LXVII]

Klass, Jürgen: Private Internet-Nutzung am Arbeitsplatz: Maßnahmen gegen Vielsurfer, München 2000, [Abruf: 12.02.2009], http://www.channelpartner.de/sonstiges/616523/ [Anlage 11 – Seite LXX]

Krauß, Claudia: Internet am Arbeitsplatz, in: Herberger, Maximilian (Hrsg.): JurPC Web-Dok. 14/2004, Abs. 1-52, Völklingen/Saar 2004, [Abruf: 12.02.2009], http://www.jurpc.de/aufsatz/20040014.htm [Anlage 12 - auf CD beiliegend]

Landesbeauftragter für den Datenschutz Baden-Württemberg: Internet und Datenschutz, Stuttgart 2006, [Abruf: 12.02.2009], http://www.baden-wuerttemberg.datenschutz.de/service/lfd-merkblaetter/internet.htm [Anlage 13 - auf CD beiliegend]

Reinermann, Heinrich: Vom Intranet zum Mitarbeiterportal: E-Government für die Mitarbeiter – was gehört dazu?, Speyer 2004, [Abruf: 12.02.2009], http://www.egovernment-akademie.de/academy/content/medien/sendfiles.cfm?key=7&pw=023CFCBA87BD7B671A9675FB6C052C23 [Anlage 14 - auf CD beiliegend]

Rühle, Gottlob: Folge 80: Private Internetnutzung am Arbeitsplatz, Schriftenreihe Bewerbungsrecht/Arbeitsrecht, Marburg o.J., [Abruf: 12.02.2009], http://www.bewerbungsmappen.de/links/ArbeitsrechtVII/Arbeitsrecht_80/arbeitsrecht_80.html [Anlage 15 - Seite LXXIII]

Sakowski, Klaus: Private Internetnutzung am Arbeitsplatz – Rechtslage im Überblick, Heidenheim 2007, [Abruf: 12.02.2009], http://www.sakowski.de/105.3.html [Anlage 16 - auf CD beiliegend]

Von Hentig, Hartmut: Einführung in den Bildungsplan 2004, Bildungsrat Baden-Württemberg (Hrsg.), o.O. 2004, [Abruf: 12.02.2009], http://www.bildung-staerkt-menschen.de/service/downloads/Sonstiges/Einfuehrung_BP.pdf [Anlage 17 - auf CD beiliegend]

Wasert, Julia: Private Internetnutzung am Arbeitsplatz, Köln 2004, [Abruf: 12.02.2009], http://www.contentmanager.de/magazin/artikel_415_private_internetnutzung_am_arbeitsplatz.html [Anlage 18 - Seite LXXVI]

8 Anlagen

Anlage 1:

DEUTSCHE HAUPTSTELLE
FÜR SUCHTFRAGEN E.V.

DHS

59003 Hamm, Postfach 1369
59065 Hamm, Westenwall 4
Tel. (0 23 81) 90 15-0
Telefax (0 23 81) 9015-30
Internet: http://www.dhs.de
eMail: gassmann@dhs.de

Stellungnahme zum Thema „Online-Sucht“ für die Anhörung des Deutschen Bundestags Ausschuss für Kultur und Medien am 9. April 2008

Die Deutsche Hauptstelle für Suchtfragen bedankt sich für die Gelegenheit einer Stellungnahme zur intensiven Nutzung von Internetangeboten. Zum vorgelegten Fragenkomplex ist aus fachlicher Sicht der Suchthilfe in Deutschland wie folgt zu antworten:

1. Die allgemeine Nutzung des Internets ist in den vergangenen 10 Jahren um einen vierstelligen Prozentbetrag gestiegen. Nach Angaben des Statistischen Bundesamtes befindet sich insbesondere in den Bevölkerungsgruppen bis 54 Jahre die Internetnutzung auf hohem Niveau. Im Jahr 2007 besaßen 73% der privaten Haushalte in Deutschland einen Computer, was einer relativen Marktsätigung entsprechen dürfte. Insgesamt 61,4% aller Internetnutzer sind dabei „jeden oder fast jeden Tag“ im Internet. Nach Angaben des Statistischen Bundesamtes nutzten ca. 23% der 35-54Jährigen (Hauptnutzergruppe) im vergangenen Jahr das Internet, bei den unter 15Jährigen lag dieser Prozentsatz bei 10% (Mädchen) bzw. 12% (Jungen).
2. Es ist davon auszugehen, dass die gestiegene Nutzerzahl mit einer steigenden Zahl von Menschen einhergeht, für die ihre Tätigkeiten im Internet zum beruflichen und / oder auch privaten Lebensmittelpunkt werden.
3. Dies kann, wie wir aus Informationen psychiatrischer Klinken wie auch aus Suchtberatungsstellen wissen, mit sozialen wie auch gesundheitlichen Problemen einhergehen. Dabei ist das Ursache- und Wirkungsgefüge weitgehend unerforscht. Die Gesamtzahl von Personen, die sich wegen problematischen Internetkonsums in Beratung und Behandlung begeben, ist mangels Erfassung nicht bekannt.
4. Auch insgesamt ist die Forschungssituation zur intensiven Internetnutzung derzeit noch sehr unbefriedigend. Vorliegende Studien stützen sich i. d. R. auf relativ kleine Untersuchungsgruppen, haben in der Gewinnung größerer Gruppen

methodische Mängel und liefern insgesamt ein keineswegs eindeutiges Bild. Dies wird in der Forschungsliteratur selbst regelmäßig betont.

5. Vor diesem Hintergrund hat unlängst die American Medical Association gegen den Antrag entschieden, eine neue Diagnose „Internet- und Computerspielsucht" in die kommende Ausgabe des Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) aufzunehmen, das von der American Psychiatric Association herausgegeben wird.
6. Fallbeispielhafte Analogien zu den anerkannten Störungsbildern stoffbezogener Süchte begründen dabei noch keine Klassifizierung als „Sucht". Derzeit ist die Klassifizierung problematischer Internetnutzung im Feld von Zwangsstörungen, Impulskontrollstörungen und Suchterkrankungen nicht geleistet.
7. Da weder Prävalenzdaten noch Behandlungsdaten vorliegen, kann nicht eingeschätzt werden, welcher Prozentsatz der Nutzer des Internets an welchen Störungen leidet und wodurch diese verursacht wurden bzw. werden.
8. Gesichert ist allerdings das Auftreten behandlungsrelevanter Störungsbilder bei einem Teil intensiver Internetnutzer.
9. Die vorgeschlagene kostenneutrale Maßnahme einer Nutzungsdaueranzeige erscheint vor diesem Hintergrund als empfehlenswert. Auch die Vermittlung von Medienkompetenz wird zur Recht seit Jahrzehnten gefördert und ist dennoch leider weitgehend uneingelöst. Eine sehr gute präventive Wirkung scheint vor allem einem adäquaten Freizeitangebot insbesondere für junge Menschen wie einer allgemeinen Verbesserung der Beschäftigungslage zuzuschreiben.
10. In diesem Zusammenhang verwundert die vollständige Nichtbeachtung des intensiven TV-Konsums. Auch die diesbezüglichen Daten steigen seit vielen Jahren kontinuierlich an. Bei einer Zuschauerreichweite von 73,4% lag bereits im Jahr 2005 die durchschnittliche tägliche Nutzungsdauer bei 210 Minuten, was die private Internetnutzung deutlich übersteigt. Die demgegenüber absolut vorrangige Diskussion problematischen Internetkonsums scheint unter epidemiologischen und gesundheitspolitischen Gesichtspunkten nicht gerechtfertigt.
11. Ebenso irrtümlich konzentrieren sich sowohl Forschung als auch öffentliche Diskussion auf das Internet-Konsumverhalten insbesondere Jugendlicher. Dies ist angesichts vorliegender Nutzungsdaten wissenschaftlich unangemessen, epidemiologisch unbegründet und trägt zu einer wenig hilfreichen Stigmatisierung der nachkommenden Generationen bei. Zudem führt es perspektivisch zu einem eklatanten Mangel präventiver und therapeutischer Angebote für erwachsene Problemkonsumenten.

Insgesamt empfiehlt die Deutsche Hauptstelle für Suchtfragen insbesondere verstärkte Forschungsbemühungen zur Definition pathologischen Internetkonsums sowie zu einer aussagekräftigen epidemiologischen Studie. Diese sollte unbedingt den TV-Konsum miteinschließen und alle relevanten soziodemographischen Merkmale erfassen. Eine ausschließliche Konzentration auf biomedizinische Grundlagenforschung ist dabei dringend zu vermeiden.

Die DHS hofft auf eine intensive gesundheitspolitische Diskussion der seit Jahrzehnten zunehmenden Mediennutzung und begrüßt in diesem Zusammenhang das Interesse des Deutschen Bundestages ganz besonders.

Dr. Raphael Gaßmann
stellv. Geschäftsführer

Anlage 10:

Rechtsanwalt Thomas Feil
Spezialist für IT-Recht · Fachanwalt für Arbeitsrecht

Internet am Arbeitsplatz - Irrtümer

Die Internet-Nutzung am Arbeitsplatz wirft immer wieder zahlreiche rechtliche Probleme auf – für Arbeitnehmer und Arbeitgeber. Beide Seite des Arbeitsverhältnisses unterliegen dabei immer wieder Irrtümern über ihre Rechte und Pflichten und die möglichen Konsequenzen ihres Handelns.

Irrtum 1: Privatnutzung immer zulässig

Grundsätzlich gilt: Allein die Tatsache, dass der Arbeitgeber die private Internetnutzung nicht ausdrücklich untersagt hat, führt noch nicht zu einer Erlaubnis. Sämtliche vom Arbeitgeber zur Verfügung gestellten Mittel dürfen nämlich zunächst grundsätzlich nur für dienstliche Zwecke eingesetzt werden. Etwas anderes gilt nur bei der ausdrücklichen oder konkludenten (= stillschweigende) Gestattung der Privatnutzung.

Die ausdrückliche Gestattung der Privatnutzung kann erfolgen durch

- Arbeitsvertrag,
- Gesamtzusage,
- Betriebsvereinbarung,

während die stillschweigende Zustimmung vorliegen kann durch

- Duldung, betriebliche Übung über einen längeren Zeitraum (ca. 6-12 Monate),

  aber auch die

- Bereitstellung von Bookmarks auf Seiten, die nur privat nutzbar sind (Spiele, Verbrauchsgüter für den Privatkunden etc.)

Daneben muss der Arbeitgeber in dringenden Ausnahmefällen (etwa beim Unfall eines Familienangehörigen) z.B. die private Email-Nutzung gestatten, ebenso wie die private Nutzung aus dienstlichem Anlass – also etwa die private Mitteilung des Ar-

beitsnehmers an Familie/Partner, dass er/sie arbeitsbedingt später nach Hause kommt.

Als Folge der Vertragsautonomie (Vertragsschlussfreiheit) besteht aber kein Anspruch des Arbeitnehmers auf private Nutzung der betriebseigenen EDV zur privaten Nutzung.

Eine solche private Nutzung liegt indes nicht vor, wenn jemand beim dienstlichen Gebrauch versehentlich nur privat nutzbare Web-Seiten anwählt (mittels Suchmaschinen-Ergebnissen etc.).

Irrtum 2: Kündigung nicht möglich

Sofern eine Zustimmung des Arbeitgebers zur Privatnutzung fehlt, handelt es sich um eine Verletzung arbeitsrechtlicher Pflichten, die zum einen Unterlassungs- und Schadensersatzansprüche des Arbeitgebers auslösen können, zum anderen aber auch zu Abmahnungen und letztlich sogar zu „verhaltensbedingte Kündigungen" führen kann.

Hinzu kommt, dass während der vertraglich vereinbarten Arbeitszeit der Arbeitnehmer seine Arbeitskraft grundsätzlich uneingeschränkt zur Verfügung zu stellen hat, was einer privaten Internetnutzung in dieser Zeit widerspricht. Die Kompensation dieser „versäumten" Arbeitszeit durch qualitative oder quantitative Mehrarbeit ist nur in sehr engen Grenzen möglich,

Irrtum 3: Der Arbeitgeber darf alles kontrollieren

Auf Seiten des Arbeitgebers hingegen besteht häufig der Irrtum, dass er aufgrund seines Eigentums an den zur Verfügung gestellten Kommunikationsmitteln auch eine uneingeschränkte Kontrollbefugnis hat. Dem stehen aber nicht nur das allgemeine

Persönlichkeitsrecht der Arbeitnehmer aus Art. 2 Abs. 1 Grundgesetz (GG) entgegen, sondern auch die datenschutzrechtlichen Vorschriften aus dem Telekommunikationsrecht, so etwa dem TKG (Telekommunikationsgesetz), der TDSV (Telekommunikationsdiensteunternehmen-Datenschutzverordnung), dem TDDSG (Teledienstedatenschutzgesetz), dem BDSG (Bundesdatenschutzgesetz) und den Datenschutzgesetzen der Länder.

Viele Arbeitgeber sind sich zudem nicht bewusst, dass sie bei ausdrücklicher oder konkludenter Gestattung der privaten Nutzung des Internets geschäftsmäßig Telekommunikationsdienste erbringen im Sinne von § 3 Nr. 5 TKG und damit – auch ohne eine Gewinnerzielungsabsicht – den speziellen gesetzlichen Anforderungen genügen müssen, wie etwa der Sicherstellung der Wahrung des Fernmeldegeheimnisses gemäß §§ 85 ff. TKG.

Die Nutzung und Verarbeitung personenbezogener Daten – wie etwa Verbindungsdaten, Protokolle der Mail- und URL-Adressen – sind dem Arbeitgeber dann nur für Abrechnungszwecke und zur Missbrauchsaufklärung gestattet. Insbesondere ist eine heimliche Überwachung des Internetverkehrs unzulässig.

Hält sich der Arbeitgeber bei seiner Kontrolle nicht an diese Beschränkungen, so dürfen die gewonnenen Daten nicht gegen den Arbeitnehmer verwendet werden, weder im Rahmen einer Beurteilung, Abmahnung noch der Kündigung.

Rechtsanwalt Karim R. Jouran, MLE

Anlage 11:

PRIVATE INTERNET-NUTZUNG AM ARBEITSPLATZ: MAßNAHMEN GEGEN VIELSURFER

Aus Sicht von Handel und Gewerbe sind die Vorteile des Internet in puncto Informationsaustausch, -beschaffung und Kostensenkung unbestritten. Die Kehrseite der Medaille ist aus Arbeitgebersicht jedoch schnell ausgemacht: Immer mehr Arbeitnehmer klicken während der Arbeitszeit fleißig E-Finanzdienste, Sport-News und Sexsites an, verschicken E-Mails an Freunde und betreiben in diversen Chat-Räumen Konversation.

Es liegt auf der Hand, dass die privaten Surf-Trips am Arbeitsplatz äußerst problematisch sind. Eine Studie des Software-Anbieters Surfwatch bei Betrieben in den USA, Südamerika und Europa hat ergeben, dass fast ein Viertel der Online-Zeit während der Arbeit für private Zwecke genutzt wird. Dass darunter die Produktivität der Mitarbeiter leidet und Arbeitsmittel - also letztlich Kosten - unnötig verbraucht werden, ist offensichtlich. Weitaus schwerer wiegt aber, dass vielfach Folgendes übersehen wird: Die Firma ist juristisch für jedes Bit verantwortlich, das auf ihrem Server liegt. Häufig sind die Ermittlungsbehörden in der Lage, die Spur bis zum Dienstcomputer zurückzuverfolgen. Werden strafbare Inhalte auf dem Zentralrechner gespeichert, kann die Staatsanwaltschaft den Firmenrechner beschlagnahmen. Die Folgen sind dann nicht mehr wieder gutzumachende Schäden für das Image des Unternehmens sowie drastische Störungen des Betriebsablaufs. Für viele Betriebe wäre dies unter Umständen das Ende. Das ungehemmte Surfen der Mitarbeiter kann im Übrigen auch dann zu einem Prob-lem werden, wenn durch das Herunterladen privater Software die Gefahr besteht, dass Viren und Trojanische Pferde in die EDV-Sys-teme und Programme des Arbeitgebers eindringen. Es verwundert deshalb nicht, dass immer mehr Firmen zu recht harten Maßnahmen greifen, um das Surf-Verhalten ihrer Angestellten zu überprüfen. Zunehmend wird Über- wachungs-Software eingesetzt, um dem exzessiven Internet-Surfen Einhalt zu gebieten. Gerade der amerikanische Markt bietet umfangreiche Software zum Registrieren und Protokollieren der Aktivitäten im Intra- und Internet, aufgeschlüsselt nach Mitarbeitern und Arbeitsplatz. Das Bedürfnis des Arbeitgebers, Angestellten auf die Finger zu sehen, findet allerdings seine Grenzen in den bestehenden Persönlichkeits- und Datenschutzrechten. Und diese sind zumindest in Deutschland relativ rigide. In der Praxis bieten sich deshalb zwei Lösungswege an, die parallel zu beschreiten sind: Zum einen ist der Einsatz dynamischer Internet-Filter erwägenswert, die den Besuch bestimmter Homepages, welche keine firmenrelevanten Inhalte aufweisen, verhindern. Der Markt bietet auf diesem Sektor zwischenzeitlich eine ganze Reihe von Programmen an. Zum anderen sollte ein juristischer Drei-Stufen-Plan gegen Vielsurfer aufgestellt werden. Dieser besteht aus den Stufen Anweisung, Abmahnung und Kündigung.

Betriebliche Anweisung

Weder ist das private Surfvergnügen am Arbeitsplatz bislang gerichtlich geregelt worden, noch kennt das deutsche Arbeitsrecht spezifische "Internet-Paragrafen". Der Arbeitgeber ist deshalb gut beraten, sich der herkömmlichen Rechtssystematik zu bedienen, um gegen unerwünschte Internet-Aktivitäten mit Erfolg vorgehen zu können. Zunächst einmal ist zu empfehlen, in Arbeitsverträgen künftig den Passus mit aufzunehmen, dass das Internet prinzipiell nur zu dienstlichen Zwecken benutzt werden darf und ein Besuch nicht betrieblich genutzter Seiten untersagt ist. Was die bestehenden Arbeitsverhältnisse angeht, so hat der Arbeitgeber die Möglichkeit, kraft seines Direktionsrechts Regeln für die Nutzung des Internet aufzustellen, womöglich sogar ein generelles Verbot auszusprechen. Eine solche Weisung kann mittels Rundschreiben oder eines Aushangs verbreitet werden. Vorstellbar ist auch, in regelmäßigen Abständen eine Warnung auf den einzelnen Bildschirmen im Büro aufscheinen zu lassen, der Hinweise zur korrekten Nutzung des dienstlichen Internet-Anschlusses entnommen werden können.

Aber auch in denjenigen Betrieben, die sich scheuen, klare Regelungen und eindeutige Warnungen auszusprechen, ist Vorsicht auf Seiten der Arbeitnehmer angebracht. Eine Beurteilung des privaten Internet-Surfens kann nämlich ohne weiteres in Anlehnung an die Rechtsprechung zum privaten Telefonieren während der Arbeitszeit erfolgen. Ob der Arbeitnehmer das Telefon seines Arbeitgebers benutzen darf, richtet sich danach nach dem Inhalt des Arbeitsvertrages, der durch betriebliche Übung ausgestaltet sein kann. Jedoch gilt: Auch wenn das Führen von Privatgesprächen ohne Einschränkung gestattet ist, hat der Arbeitnehmer hierbei Maß zu halten (Landesarbeitsgericht Niedersachsen, Urteil vom 13.01.1998, Az. 4 Ca 30/96). Das ausschweifende Gebrauchmachen von der Möglichkeit, den dienstlichen Internet-Anschluss auch für private Zwecke während der Arbeitszeit zu nutzen, ist deshalb auf keinen Fall erlaubt. Um in diesem Punkt Unklarheiten von vornherein zu vermeiden, sollte jedoch stets eine Betriebsanweisung - eventuell in Absprache mit dem Betriebsrat - erlassen werden, die bestimmte Regeln für die erlaubte und nichterlaubte Web-Nutzung aufstellt.

Zumeist unverzichtbar: die Abmahnung

Stellt der Arbeitgeber fest, dass ein surfender Mitarbeiter fortlaufend seine Anweisung missachtet beziehungsweise den Rahmen des Üblichen bei weitem überschreitet, ist auf keinen Fall vorschnell zur Kündigung des Arbeitsverhältnisses überzugehen. Eine solche Kündigung würde - wenn der Betroffene dagegen Klage erhebt - vor dem Arbeitsgericht nur selten Bestand haben. Denn die Kündigung ist nach der Rechtsprechung nur das äußerste Mittel zur Beilegung von Meinungsverschiedenheiten. Im Falle einer verhaltensbedingten Kündigung ist grundsätzlich eine vorangegangene Abmahnung Voraussetzung.

In der Praxis werden förmliche Abmahnungen oftmals ohne die Hilfe eines Anwalts angefertigt. Die Folge ist, dass viele Abmahnungen rechtsfehlerhaft sind, so dass sie allenfalls als Rüge oder Ermahnung betrachtet werden können. Solche Erklärungen können jedoch nicht als Vorstufe zur Kündigung angesehen werden.

Ohne hier auf alle Einzelheiten eingehen zu können, seien folgende Besonderheiten herausgestellt:

- Der Arbeitgeber muss dem Arbeitnehmer für den Wiederholungsfall mit Kündigung drohen. Diese Formulierung muss klar und eindeutig sein.

- Die Abmahnung muss das beanstandete Verhalten des Arbeitnehmers möglichst genau bezeichnen. Die einzelnen Internet-Aktivitäten müssen also präzise bezeichnet werden. Voraussetzung für eine Abmahnung ist, dass das beanstandete Verhalten eine vertragliche Relevanz entweder aufgrund der Schwere oder der Häufigkeit des Vorfalls hat.

- Der Empfang der Abmahnung ist aus Beweisgründen vom Arbeitnehmer zu quittieren, außerdem ist eine Durchschrift der Abmahnung zur Personalakte zu nehmen. Die Abmahnung verliert übrigens ihre Wirkung nach einer längeren Zeit einwandfreier Führung des Arbeitnehmers durch Zeitablauf.

Letzter Ausweg: die Kündigung

Juristische Datenbanken verzeichnen derzeit nur drei besonders krasse Fälle für Kündigungen aus mit den Internet verbundenen Gründen. Ein Angestellter im Jugendfürsorge-Bereich war dabei ertappt worden, dass er Bilder kinderpornografischen Inhalts auf seinem Rechner gespeichert hatte (Arbeitsgericht Braunschweig, Urteil v. 22.1.1999, Az. 3 Ca 370/98). In zwei anderen Fällen entschieden die Landesarbeitsgerichte, dass die Verbreitung beleidigender Äußerungen über den Arbeitgeber per Internet ein Kündigungsgrund sei (LAG Köln, Urteil v. 4.11.1998, Az. 2 Sa 330/98; LAG Schleswig- Holstein, Urteil v. 4.11.1998, Az. 2 Sa 330/98). In beiden Fällen war also nicht die Surf- und E-Mail-Aktivität des Arbeitnehmers der Grund für die Kündigung, sondern der Verstoß gegen geltendes Recht.

Bezogen auf die hier zu erörternde Thematik ist festzustellen, dass der Arbeitgeber, wenn sein Mitarbeiter beharrlich gegen die betriebliche Ordnung verstößt und "auf Abwegen" surft, eine Kündigung aussprechen kann. Im Regelfall ist allerdings die erwähnte Abmahnung erforderlich. Ob je nach den Umständen des Einzelfalles eine ordentliche oder eine außerordentliche Kündigung in Betracht zu ziehen ist, sollte mit einem Rechtsanwalt besprochen werden. Die unverhältnismäßige private Nutzung des Internet im Büro dürfte jedenfalls einen nachhaltigen Vertragsbruch des Arbeitnehmers darstellen, der durchaus zur fristlosen Kündigung führen kann. Dies vor allem dann, wenn die Verletzung von Straftatbeständen im Raum steht (etwa durch Herunterladen von kinderpornographischen oder rechtsradikalem Material). Ein großzügiges Laissez-faire ist in diesem Punkt aus Sicht der Geschäftsführung nicht angezeigt.

Anlage 15:

Folge 80: Private Internetnutzung am Arbeitsplatz

Der Fall:

Arbeitgeber Mephistopheles beschäftigt den Verkaufsmanager Faust seit 3 Jahren. Wegen der Internationalisierung der Geschäfte richtet Mephistopheles für Faust einen Internet-Zugang ein.
Mephistopheles kennt das Problem der Versuchung. Um vorzubeugen, vereinbart er mit Faust schriftlich einen Zusatz zum Arbeitsvertrag. Darin ist geregelt:
– Der Internet-Zugang darf nur für dienstliche Zwecke verwendet werden.
– Das Herunterladen von Daten mit gesetzwidrigem, rechtsradikalem oder pornografischem Inhalt ist unzulässig.
– Bei Verstößen gegen diese Vereinbarung kann der Arbeitgeber den Internet-Zugang vorübergehend oder dauernd sperren.
Nach 1 Jahr führt Mephistopheles eine Überprüfung der Internet-Nutzungen sämtlicher Mitarbeiter durch. Dabei stellt er fest, daß Faust während seiner Arbeitszeit Dateien mit pornografischem Inhalt heruntergeladen hat. Faust hat mindestens 22 Stunden mit pornografischen Dateien verbracht. Auf dem geschäftlichen Laptop sind mindestens 15 einschlägige Videoclips gespeichert. Außerdem hat Faust über seine geschäftliche E-Mail Kontakte mit diversen Gespielinnen geführt.
Arbeitgeber Mephistopheles kündigt nach Bekanntwerden sofort fristlos. Faust klagt gegen die Kündigung und trägt vor, daß die Überprüfung der E-Mails des Klägers einen unzulässigen Eingriff in die Privatsphäre darstelle.
Eine Kündigung sei auch deshalb ausgeschlossen, weil für den Fall von Verstößen gegen die Internet-Vereinbarung nur die Sperrung des Internet-Zugangs vereinbart sei. Zumindest aber hätte wegen der massiven Versuchungen und Möglichkeiten des Internet Arbeitgeber Mephistopheles erst einmal abmahnen müssen, bevor er kündigt.
Wird Faust obsiegen?

Die Lösung:

1. Ultima-Ratio-Prinzip

Nach dem Willen des Gesetzgebers und der Rechtsprechung soll die Kündigung des Arbeitsverhältnisses bei Vertragspflichtverletzungen stets nur als letztes Mittel angewandt werden (ultima-ratio-Prinzip). Ist dem Arbeitgeber eine weniger einschneidende Maßnahme, wie z.B. eine Ermahnung oder Abmahnung, eine Versetzung oder Umsetzung zumutbar, so muß er zunächst diese Maßnahme ergreifen.
Fristlos kann nach § 626 BGB das Arbeitsverhältnis nur aus wichtigem Grund gekündigt werden, nämlich dann, wenn Tatsachen vorliegen, aufgrund derer dem kündigenden Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls und unter Berücksichtigung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnis bis zum Ablauf einer Kündigungsfrist nicht mehr zugemutet werden kann.

Dabei ist zunächst zu prüfen, ob der Sachverhalt, d.h. der Vorwurf und die Vertragspflichtverletzung an sich überhaupt geeignet ist, eine außerordentliche, fristlose Kündigung zu rechtfertigen.

2. Private Internet-Nutzung

Die private Internet-Nutzung im Arbeitsverhältnis kann je nach Umständen des Einzelfalles zum Ausspruch einer ordentlichen oder außerordentlichen Kündigung ausreichen, muß es aber nicht. Es ist zunächst einmal festzustellen, wie die Gebräuchlichkeiten und Anweisungen in dem Unternehmen sind und welche vertraglichen Vereinbarungen getroffen oder nicht getroffen wurden.
Vom Prinzip her verhält es sich ähnlich wie mit der privaten Telefon-Nutzung während der Arbeitszeit. Die Nutzung des Internet zu Privatzwecken während der Arbeitszeit ohne ausdrückliche Erlaubnis des Arbeitgebers ist für den Arbeitnehmer immer gefährlich. Der Arbeitnehmer kann ohne ausdrückliche Erlaubnis nicht davon ausgehen, daß er dazu berechtigt ist. Arbeitnehmer Faust mußte daher mit arbeitsrechtlichen Maßnahmen des Mephistopheles rechnen.
Sofern im Betrieb von seiten der Vorgesetzten oder des Arbeitgebers die private Internet-Nutzung während der Arbeitszeit, jedenfalls bis zu einem gewissen Grad, geduldet wurde, muß von einer entsprechenden betrieblichen Übung ausgegangen werden. In diesem Falle darf der Arbeitgeber jedenfalls das Arbeitsverhältnis nicht ohne vorherige Abmahnung kündigen.
Auch wenn eine solche betriebliche Übung nicht existiert, muß Arbeitgeber Mephistopheles zunächst prüfen, ob eine Abmahnung ausreicht, um das Fehlverhalten abzustellen. Dies gilt jedenfalls dann, wenn die Privatnutzung des Internet nicht gewisse Grenzen und Schwellenwerte überschritten hat.

3. Ausdrückliches Verbot

Etwas anderes gilt, wenn der Arbeitgeber die private Internet-Nutzung ausdrücklich verboten oder gar – wie im vorliegenden Fall – eine entsprechende Vereinbarung mit dem Arbeitnehmer getroffen hat.
Die Frage der unberechtigten Internet-Nutzung zu privaten Zwecken durch den Arbeitnehmer ist bislang zwar in der Rechtsprechung noch nicht geklärt. Die Rechtsprechung zur privaten Telefon-Nutzung kann jedoch dazu herangezogen werden. Deshalb gilt auch hier der Grundsatz, daß eine Kündigung des Arbeitsverhältnisses durch den Arbeitgeber immer dann gerechtfertigt sein kann, wenn ein ausdrückliches Verbot von Arbeitgeberseite vorliegt.

4. Vertrauensbereich

Mit der privaten Internet-Nutzung gegen das ausdrückliche Verbot des Arbeitgebers oder gegen die hier vorhandene Vereinbarung zwischen Mephistopheles und Faust, hat der Arbeitnehmer Faust den Arbeitgeber massiv geschädigt und in zweifacher Weise Betrug begangen. Er hat nämlich seine private Internet-Nutzung vom Arbeitgeber bezahlen lassen und außerdem hat er sich für diese Zeit auch noch Lohn bezahlen lassen (Zeitbetrug).
Die Vertragsverletzung von Faust stellt eine Störung im Vertrauensbereich des

Arbeitsverhältnisses dar. Da es sich um eine schwere Pflichtverletzung im Vertrauensbereich handelt, ist regelmäßig eine Abmahnung des Arbeitnehmers vor Ausspruch einer Kündigung entbehrlich.
Faust konnte aufgrund der von ihm unterzeichneten Vereinbarung ohne weiteres erkennen, daß Arbeitgeber Mephistopheles seine privaten Internet-Praktiken nicht akzeptieren würde.

5. Vertraglicher Kündigungsausschluß

Zwar haben Mephistopheles und Faust in ihrer Vereinbarung als Folge eines Verstoßes den Entzug der Internet-Nutzung für den Arbeitnehmer geregelt. Diese Regelung beseitigt jedoch nicht das Recht des Arbeitgebers, bei schwerwiegender Vertragsverletzung eine außerordentliche Kündigung auszusprechen. Dieses Recht kann vertraglich nicht ausgeschlossen werden.

6. Interessenabwägung

Die bei einer fristlosen Kündigung stets vorzunehmende Interessenabwägung führt nicht zur Rechtswidrigkeit der Kündigung. Der Arbeitnehmer hat in besonders grober Weise gegen seine vertraglichen Pflichten verstoßen, indem er sich stundenlang auf Kosten des Arbeitgebers mit Pornoprogrammen beschäftigt hat und dieses sogar auf die Einrichtungen des Arbeitgebers herunterlud.
Auch die Dauer des Arbeitsverhältnisses ist nicht geeignet, diesen Vertrauensverstoß zu relativieren. Mephistopheles kann den Manager Faust nicht bei der Internet-Nutzung ständig kontrollieren.

7. Merke

Der Arbeitgeber kann zur Vornahme einer außerordentlichen Kündigung berechtigt sein, wenn der Mitarbeiter trotz ausdrücklicher entgegenstehender Vereinbarung das Internet zu privaten Zwecken nutzt. In diesem Fall ist eine vorherige Abmahnung nicht erforderlich.

Anlage 18:

PRIVATE INTERNETNUTZUNG AM ARBEITSPLATZ

E-Bay im Büro: Private Internetnutzung am Arbeitsplatz

Viele Mitarbeiter in Unternehmen haben heute vom betrieblichen Arbeitsplatz aus Zugang zum Internet und damit auch die Möglichkeit einer privaten Kommunikation per E-Mail. Der Blick in die einschlägigen Nachrichtenplattformen oder die Überprüfung der privaten Mailbox gehören schon zum Tagesauftakt eines Arbeitnehmers. Die Frage, ob und gegebenenfalls in welchem Umfang dieses Kommunikationsmittel zu privaten Zwecken genutzt werden darf, kann im Arbeitsvertrag geregelt werden.

Um Rechtsklarheit hinsichtlich der Internetnutzung zu schaffen, ist es sowohl im Sinne des Arbeitgebers als auch im Sinne des Arbeitnehmers, eine möglichst umfassende und klare Regelung der privaten Internetnutzung verbindlich in einem Arbeitsvertrag oder einer Betriebsvereinbarung festzulegen.

Regelung durch Betriebsvereinbarung

Nach § 87 I Nr. 1 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Regelung von Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer im Betrieb. Davon umfasst ist auch der Umgang mit dem Internet-Zugang. Dem entsprechend muss sich der Arbeitgeber bei einer Regelung mit dem Betriebsrat abstimmen und eine Betriebsvereinbarung schließen.

Entscheidet sich der Arbeitgeber für eine teilweise Untersagung, so muss in einer Regelung eine zeitliche Begrenzung, eine örtliche Benutzung und die Art bzw. der Umfang der Nutzung genau festgeschrieben werden. Ferner dürfte es sinnvoll sein, die Abgrenzung von privater zu dienstlicher Nutzung vorzunehmen. Dies kann bereits in Einzelfällen zu Schwierigkeiten führen. Als dienstlich dürfte der Blick ins Internet zu beurteilen sein, wenn ein spezifischer Bezug zum Aufgabenbereich des Arbeitnehmers erkennbar ist. Der Arbeitnehmer muss also gerade durch den Gang ins Internet seine Arbeit voran treiben wollen.

Hat der Arbeitgeber die Internetnutzung geregelt, kann der Arbeitnehmer in Ruhe den gewährten Rahmen nutzen ohne eine Rüge durch den Arbeitgeber zu gegenwärtigen. Der Arbeitgeber kann, sofern die festgelegten Grenzen überschritten werden, mit einer Abmahnung oder in besonders schweren Fällen mit einer Kündigung reagieren.

Keine Vereinbarung

Sofern keine betriebsinterne Vereinbarung getroffen wurde, die die Grenzen einer privaten Nutzung eindeutig festlegt, ist das selbstverständlich kein Freibrief für Arbeitnehmer. Dennoch ist in diesem Fall eine geringfügige Nutzung des Inter-

nets kein Grund für eine fristlose Kündigung, solange sie sich innerhalb eines gewissen Rahmens hält.

Das Arbeitsgericht Wesel sah im Falle einer Arbeitnehmerin, die einen Internetzugang in einem Jahr rund 100 Stunden privat genutzt hatte, zwar einen Grund für eine Abmahnung, nicht jedoch für eine fristlose Kündigung. Im Urteil heißt es "...die private Internetnutzung wird von einem Großteil der Arbeitnehmer oft als bloße Spielerei oder zumindest als Kavaliersdelikt empfunden. Dass dies seitens des Arbeitgebers nicht so bewertet wird, hat er dem Arbeitnehmer bei einer Internetnutzung, wie sie möglicherweise durch die Klägerin erfolgt ist, durch eine Abmahnung deutlich zu machen."

Betriebliches Verbot

Etwas anderes gilt dagegen bei einem eindeutigen betrieblichen Verbot der Privatnutzung. Hier dürfte schon eine deutlich geringere Anzahl von im Internet ohne Arbeitsbezug verbrachten Stunden eine Kündigung ohne vorherige Abmahnung rechtfertigen. Das Landesarbeitgericht Hannover hielt eine außerordentliche Kündigung ohne Abmahnung in einem Falle für gerechtfertigt, in dem ein ausdrückliches Verbot der privaten Internetnutzung galt und der Mitarbeiter gleichwohl das Internet zu privaten Zwecken nutzte - nämlich um pornographisches Material herunterzuladen.

Überwachungsmöglichkeiten

Technisch ist eine Überwachung recht einfach zu bewerkstelligen. Jeder Internet-Browser gibt Auskunft darüber, wohin sein Benutzer in der letzten Zeit gesurft ist. Überdies ist auf dem Markt ausgeklügelte Software zur Mitarbeiterüberwachung erhältlich.

Doch findet die Überwachung ihre Grenzen in Vorschriften des Datenschutzes und des Telekommunikationsrechts. In der Regel ist der Arbeitgeber "normaler Zugangs-Provider". Als solcher darf er grundsätzlich die persönlichen Daten verlangen, die er benötigt, um den Internetzugang zu realisieren und abzurechnen. Sämtliche sonstigen, für diesen Zweck nicht oder nicht mehr notwendigen Informationen müssen jedoch unmittelbar nach dem Ende der Nutzung gelöscht werden. Da keine Abrechnung erfolgt, darf der Arbeitgeber nur solche Daten speichern, die technisch notwendig sind, um einen reibungslosen Betrieb des Unternehmensnetzwerkes zu ermöglichen. Detaillierte Logfiles über die Aktivitäten einzelner Nutzer oder Inhalte von E-Mails fallen sicherlich nicht unter diese Daten.

Fazit

Es ist dringend anzuraten, die private Nutzung des Internets am Arbeitsplatz bereits im Arbeitsvertrag oder durch eine Betriebsvereinbarung zu regeln. Durch klare Vorgaben und Verhaltensregeln wird das Bewusstsein für einzelne Problemfelder sowohl auf Arbeitgeber- als auch auf Arbeitnehmerseite geschärft.

9 Erklärung

Ich versichere, dass ich diese Diplomarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

_____ _____

Ort, Datum Unterschrift

Arbeitskreis Technik der Datenschutz-
beauftragten des Bundes und der Länder

Datenschutz bei der Nutzung von Internet und Intranet

Herausgeber:

Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin
19053 Schwerin
Telefon: (03 85) 5 94 94-0
Telefax: (03 85) 5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: http://www.lfd.m-v.de

Verantwortlich: Dr. Werner Kessel

Redaktionsschluss: 15. Dezember 2000

Herstellung: CLUB WIEN und cw Obotritendruck GmbH, Schwerin

Vorwort

Das Internet wird im Zeitalter der Informationsgesellschaft zu einem immer wichtigeren Kommunikationsmittel. Auch die Verwaltungen nutzen im Zuge ihrer Modernisierung in zunehmendem Maße dieses weltweite Computernetz und die dort eingesetzten Technologien. Künftig sollen nicht nur Informationen zwischen den einzelnen Behörden ausgetauscht, sondern den Bürgerinnen und Bürgern auch Dienstleistungen "online" angeboten werden.

Der Anschluss von lokalen Netzen an das Internet ist jedoch mit erheblichen Risiken für den Datenschutz und die Datensicherheit verbunden. Die Rechner und Übertragungswege des Internet sind nur eingeschränkt kontrollierbar. Da bei der Entwicklung des Internet Sicherheitsfragen lange Zeit eine untergeordnete Rolle gespielt haben, wurden keine Maßnahmen getroffen, um die Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit in angemessener Weise zu minimieren. Der erste Teil dieser Broschüre, die *Orientierungshilfe "Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet"*, die von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt wurde, beschreibt vorhandene Risiken und erläutert Maßnahmen, mit denen ihnen in angemessener Weise begegnet werden kann. Es werden verschiedene Firewallarchitekturen dargestellt und Strategien erläutert, mit denen das stets verbleibende Restrisiko minimiert werden kann.

Die zunehmende Nutzung neuer Kommunikationsformen, beispielsweise E-Mail, erfordert unter anderem auch eine neue Art der Verbreitung von Kommunikationsadressen. Hierzu werden elektronische Verzeichnisdienste eingesetzt. Der elektronische Zugriff auf die dort gespeicherten personenbezogenen Daten übersteigt die Möglichkeiten konventioneller Adress- und Telefonverzeichnisse erheblich und birgt ebenfalls neue Risiken für die Vertraulichkeit und die Integrität dieser Daten. Jede datenverarbeitende Stelle muss deshalb sorgfältig prüfen, welche Daten in derartige Verzeichnisse aufgenommen werden. Der zweite Teil der Broschüre, die *Orientierungshilfe "Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten"* des Arbeitskreises Technik, enthält Hinweise, wie mit elektronischen Verzeichnisdiensten umgegangen werden sollte, damit schutzwürdige Belange der ver-

zeichneten Personen nicht unangemessen beeinträchtigt werden. Obwohl hier nur Verzeichnisdienste in einer definierten Netzwerkumgebung (Intranet) der öffentlichen Verwaltung betrachtet werden, sind die Empfehlungen prinzipiell auch auf den erweiterten Bereich des Internet anwendbar.

Der dritte Abschnitt der Broschüre ist dem *Arbeitspapier "Vom Bürgerbüro zum Internet"* entnommen, das eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Leitung der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen erstellt hat. Dieses Arbeitspapier befasst sich mit datenschutzrechtlichen Fragen bei der Modernisierung der Verwaltung. Die hier veröffentlichten Abschnitte "Informationsangebote öffentlicher Stellen" und "Interaktive Verwaltung" enthalten zwei weitere Aspekte der Internetnutzung öffentlicher Stellen aus datenschutzrechtlicher Sicht. Zum einen wird erläutert, welche datenschutzrechtlichen Anforderungen Behörden beachten müssen, wenn sie eigene Informationsangebote im Internet bereitstellen. Zum anderen werden Hinweise gegeben, wie die Verwaltung den Bürgerinnen und Bürgern interaktive Kommunikation anbieten und Verwaltungsvorgänge über das Internet abwickeln sollte, damit datenschutzrechtliche Vorschriften nicht verletzt werden.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Inhaltsverzeichnis

Teil 1
Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

1 Einleitung 11

2 Vorbereitung und Planung 13
2.1 Nutzungs- und Anschlussmöglichkeiten 13
2.1.1 Nutzungsarten 13
2.1.2 Anschlussarten 13
2.1.2.1 Direktanschluss eines Rechners an das Internet 14
2.1.2.2 Zentrale Kopplung eines lokalen Netzes an das Internet 14
2.1.2.3 Dezentrale Zugänge zum Internet 15
2.2 Kommunikations- und Risikoanalyse 15
2.3 Sicherheitsrisiken und Schutzmaßnahmen 17
2.3.1 Protokollimmanente Sicherheitsrisiken 17
2.3.2 Dienstespezifische Sicherheitsrisiken 20
2.3.2.1 E-Mail und Usenet-News 20
2.3.2.2 Telnet 20
2.3.2.3 FTP 21
2.3.2.4 WWW 22
2.3.2.5 DNS 22
2.3.2.6 Finger 22
2.3.2.7 SNMP 23
2.3.3 Aktive Inhalte/Aktive Elemente 24
2.3.3.1 ActiveX 24
2.3.3.2 Java 25
2.3.3.3 JavaScript 26
2.3.3.4 Plug Ins 27
2.3.3.5 Cookies 28

3 Firewall-Systeme 29
3.1 Grundlagen 29
3.1.1 Charakteristika von Firewall-Systemen 29

3.1.2 Schutzniveau 30
3.2 Firewall-Technologien 30
3.3 Firewall-Architekturen 33
3.3.1 Zentrale Firewalls 33
3.3.2 Gestaffelte Firewalls 35
3.3.3 Entmilitarisierte Zone 37
3.3.4 Screened Gateway 38

4 Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall
4.1 Allgemeines 39
4.2 Kontrolle von Inhaltsdaten bei E-Mail-Kommunikation 41
4.2.1 Kontrolle auf Virenbefall mittels automatischem Virencheck 41
4.2.2 Kontrolle eingehender dienstlicher E-Mails 41
4.2.3 Kontrolle eingehender privater E-Mails 41
4.2.4 Kontrolle ausgehender E-Mails 42
4.3 Protokollierung von Internet-Zugriffen mittels einer Firewall 43
4.3.1 Protokollierung der von innen erfolgenden Zugriffe (Protokollierung von Mitarbeiterdaten) 44
4.3.1.1 Dienstliche Nutzung 44
4.3.1.2 Private Nutzung 45
4.3.2 Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe 46
4.3.2.1 Nur Anschluss des internen Netzes an das Internet; keine Angebote der öffentlichen Stelle nach außen 46
4.3.2.2 Angebot nach außen (Web-Server) 46

5 Auswahl und Umsetzung der Sicherungsmaßnahmen; Betriebsphase . 47
5.1 Security Policy und Sicherheitskonzept 47
5.2 Auswahl, Konfiguration und Wartung von Firewall-Systemen 48
5.3 Rahmenbedingungen für Konfiguration und Betrieb 49
5.4 Empfehlungen für den Betrieb einer Firewall 51

6 Zusatzmaßnahmen bei der Verarbeitung sensibler Daten 53
6.1 Sensible Daten 53
6.2 Schutzniveau von Firewalls 53
6.3 Kommunikationsverbindungen als verdeckte Kanäle 54

6.4 Risiken und Maßnahmen im Einzelnen 55
6.4.1 Beschränkung der aktiven lokalen Komponenten 56
6.4.2 Eingeschränkte Kommunikationskanäle 56
6.4.3 Begrenzung der Kommunikationspartner 57
6.4.4 Verminderung des lokalen Schadenspotenzials 57
6.5 Vorgeschlagene Systemkonfigurationen 57
6.5.1 Proxy mit Positivliste (inhaltliche Begrenzung) 58
6.5.2 Umgebungsmodell (zeitliche Begrenzung) 58
6.5.3 Grafischer Internetzugang (logische Systemtrennung) 59
6.5.4 Stand-alone-System (physikalische Systemtrennung) 60

7 Ausblick 60

8 Anhang 62
8.1 Weiterführende Informationen und Literatur 62
8.1.1 Fundstellen im WWW 62
8.1.2 Broschüren 63
8.1.3 Literatur 64
8.2 Abbildungsverzeichnis 66
8.3 Abkürzungsverzeichnis 67
8.4 Wichtige Dienste und Begriffe 67

Teil 2
Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“

1. Einleitung 79

2. Verzeichnisdienste 80
2.1 Verzeichnisdienst X.500 80
2.2 Network Directory System (NDS) 82
2.3 Domain Name System (DNS) 83

3. Komponenten und Beteiligte 83

4. Datenschutzaspekte von Verzeichnisdiensten 84
4.1 Rechtliche Einordnung von Verzeichnisdiensten 85
4.2 Veröffentlichung von Klarnamen 85
4.3 Beschäftigtendaten in Verzeichnisdiensten 86

5. Maßnahmen 87

Teil 3
Internetnutzung durch öffentliche Stellen

Auszug aus dem Arbeitspapier “Vom Bürgerbüro zum Internet” der Arbeitsgruppe “Serviceorientierte Verwaltung” der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1 Informationsangebote öffentlicher Stellen im Internet 90
1.1 Inhaltsebene und Tele-/Mediendienste 90
1.2 Inhaltsdaten: Was darf ins Internet? 91
1.2.1 Bedienstetendaten 93
1.2.2 Bürgerdaten 94
1.2.3 Webcams 95
1.3 Nutzungsdaten: Was darf wie verarbeitet werden? 96
1.3.1 Speicherung von Nutzungsdaten 97
1.3.2 Cookies 98
1.3.3 Active-X, Java, JavaScript, Plug-Ins 99
1.4 Gestaltung des Angebots 99
1.4.1 Datenschutzhinweise 99
1.4.2 Anbieterkennzeichnung, Impressum 101
1.5 Technische Absicherung 102

2 Interaktive Verwaltung 104
2.1 Welche Verwaltungsvorgänge können über das Internet abgewickelt werden? 105
2.2 Wie ist die internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen? 108
2.3 Müssen die Verwaltungen Verschlüsselungsverfahren anbieten? 110
2.4 Ist der Einsatz von Signierverfahren erforderlich? 111
2.5 Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar? 112

Teil 1

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

erstellt von den
Arbeitskreisen "Technik" und "Medien"
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Überarbeitete Fassung vom November 2000

1 Einleitung

Das Internet ist ein weltweites Computernetz, in dem hunderttausende größere Rechnerverbünde und somit Millionen einzelner Computer zusammengeschlossen sind. Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Der Internet-Boom hat auch vor den öffentlichen Verwaltungen nicht Halt gemacht. Seit geraumer Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internet-Dienste vgl. Anhang).

Dabei ist der Anschluss an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von bereits weit mehr als 100 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe wurde von den Arbeitskreisen „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt[1]. Sie soll den für den Betrieb von Netzen der öffentlichen Ver-

[1] Aufgrund der Zuständigkeit der Mitglieder dieses Gremiums vor allem für den Datenschutz im öffentlichen Bereich richtet sich diese Orientierungshilfe in erster Linie an öffentliche Verwaltungen. Die Aussagen lassen sich aber im Allgemeinen auch auf andere Bereiche übertragen.

waltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der "internen" Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, in welchen Fällen und unter welchen Bedingungen es zulässig ist, dass Verwaltungen personenbezogene Daten mit Hilfe des Internet übertragen oder veröffentlichen, ist nicht Gegenstand der Orientierungshilfe und muss jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der "Entdeckung" neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluss an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen hinreichend beherrscht werden können.

2 Vorbereitung und Planung

Grundlage für eine datenschutzgerechte Nutzung des Internet ist eine genaue Planung der Internet-Aktivitäten einer Verwaltung. Je nach dem Informations- und Kommunikations-Bedarf ist eine der möglichen Nutzungsarten unter Berücksichtigung einer der Anschlussmöglichkeiten vorzusehen. Es bedarf einer genauen Analyse sowohl dieses Bedarfs als auch der mit der jeweiligen Anschlussart verbundenen Risiken.

2.1 Nutzungs- und Anschlussmöglichkeiten

2.1.1 Nutzungsarten

Grundsätzlich sind drei Konstellationen der Internet-Nutzung einer Behörde zu unterscheiden:

1. Eine Behörde nutzt einen Internet-Zugang nur, um Informationen im Internet suchen zu können, und/oder
2. eine Behörde stellt eigene Informationen im Internet zum (potentiell weltweiten) Abruf zur Verfügung (wobei im Internet von Informationsanbietern erwartet wird, dass sie auch per E-Mail erreichbar sind [siehe 3.]) oder
3. eine Behörde stellt eigene Informationen im Internet zum Abruf zur Verfügung **und** bietet zusätzlich die **Interaktion mit Bürgerinnen und Bürgern**, z. B. per E-Mail, an.

Diese drei Konstellationen können auf verschiedene Art und Weise technisch umgesetzt werden und verlangen unterschiedliche Maßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten.

2.1.2 Anschlussarten

Die Anschlussarten an das Internet können in drei verschiedene Szenarien unterteilt werden, die unterschiedliche Sicherheitsrisiken mit sich bringen:

2.1.2.1 Direktanschluss eines Rechners an das Internet

Hier wird ein einzelner, nicht lokal vernetzter Rechner per Modem und Telefonleitung über einen Provider (dies kann ein verwaltungsinterner oder ein externer sein) an das Internet angeschlossen (Abbildung 2.1). Diese Variante spielt besonders bei kleinen Behörden und im privaten Bereich eine große Rolle. Bei eventuellen Angriffen besteht ein Sicherheitsrisiko nur für den einzelnen Rechner. Es lässt sich durch entsprechende Maßnahmen reduzieren (z. B. ausschließliche Verwendung des Rechners für den Zugang zum Internet; sicherstellen, dass Ressourcen des Rechners – wie etwa Festplattenverzeichnisse – nicht für den Zugriff über das Netz freigegeben sind).

Abbildung 2.1: Direktanschluss eines Rechners an das Internet

2.1.2.2 Zentrale Kopplung eines lokalen Netzes an das Internet

Hier hat der Rechner (evtl. über ein LAN oder aber direkt per Modem oder ISDN) einen Zugang zum Intranet der Verwaltung. Von dort besteht ein einziger zentraler Zugang zum Internet (Abbildung 2.2). Eventuelle Angriffe aus dem Internet können bereits an der zentralen Übergangsstelle vom Internet zum Intranet zum großen Teil abgefangen werden. Der Rechner bzw. das LAN ist zusätzlich aus dem Intranet heraus angreifbar.

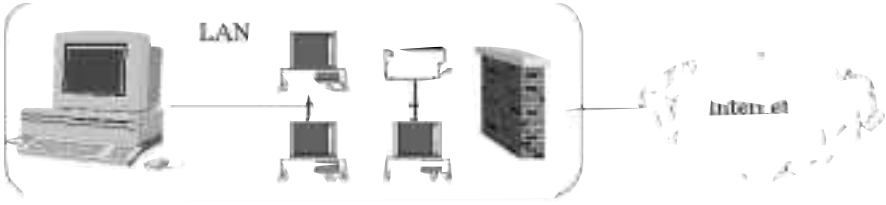


Abbildung 2.2: Zentrale Kopplung eines lokalen Netzes an das Internet

2.1.2.3 Dezentrale Zugänge zum Internet

Neben einem direkten Internet-Anschluss über einen Provider verfügt der Rechner gleichzeitig über eine Verbindung zu einem Intranet (Abbildung 2.3). Bei eventuellen Angriffen besteht nicht nur ein Sicherheitsrisiko für den an das Internet angeschlossenen Rechner, sondern auch für das LAN, in dem sich der Rechner befindet, und das Intranet. Daher ist von dieser Konstellation generell abzuraten.

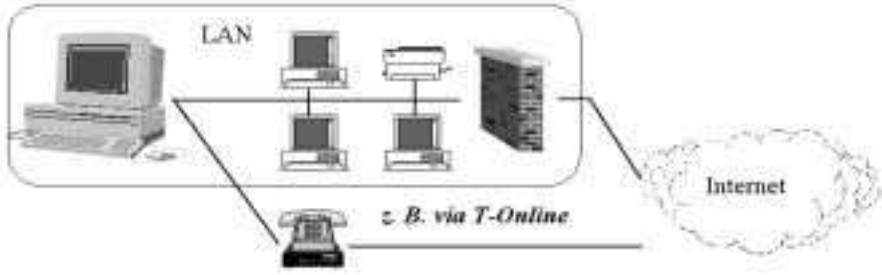


Abbildung 2.3: Dezentraler Anschluss eines lokal vernetzten Rechners an das Internet

2.2 Kommunikations- und Risikoanalyse

Vor einem Anschluss an das Internet ist eine Analyse des Kommunikationsbedarfs durchzuführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluss eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden müssen. Bei der Beurteilung der Erforderlichkeit ist ebenfalls ein strenger Maßstab anzulegen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen aufgrund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden.

Ausgangspunkte einer derartigen Analyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle sowie die Risiken der unterschiedlichen Dienste. In Anlehnung an die Empfehlungen des BSI-

Grundschutzhandbuchs sind im Rahmen einer Risikoanalyse zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z. B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert.)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, dass nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen.

Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muss und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann. Bei einem unvertretbaren Restrisiko muss auf einen Anschluss des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste kann in diesem Fall nur über solche Systeme erfolgen, die nicht mit dem Verwaltungsnetz verbunden sind und auf denen ansonsten keine sensiblen Daten verarbeitet werden.

2.3 Sicherheitsrisiken und Schutzmaßnahmen

Mit dem Zugang zum Internet sind Risiken verbunden, die großenteils daraus resultieren, dass das Datennetz nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So stellt das zugrunde liegende Protokoll beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung bereit.

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluss wider. Selbst wenn Maßnahmen gegen die bekannten Gefährdungen getroffen werden, lässt sich ein hundertprozentiger Schutz ohne Verzicht auf die Internet-Anbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

2.3.1 Protokollimmanente Sicherheitsrisiken

Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext über das lokale Netz (z. B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter der Bezeichnung LAN-Analyzer bekannt sind (z. B. Packet Sniffer), kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden.

Gegenmaßnahmen:
Verschlüsselung der Daten

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden; z. B. lassen sich die IP-Adressen von Sender und Empfänger fälschen, die TCP Sequence Number von Paketen kann häufig vorhergesagt werden, und der Übertragungsweg ist bei dynamischem Routing modifizierbar. Pakete können abgefangen werden, so dass sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin lässt sich die Kommunikation eines autorisierten Nutzers mitschneiden und später wiedereinspielen (Replay Attack), wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS [Network File System]).

Gegenmaßnahmen:
Gegen eine unerkannte Manipulation von Nachrichteninhalten können digitale Signaturen eingesetzt werden.
Für starke Authentisierung eignen sich Einmalpasswörter oder Challenge-Response-Systeme gegen Replay Attacks.
Für Router sollte nach Möglichkeit statisches Routing konfiguriert werden. Außerdem sollte das “Source Routing” abgestellt sein.

Bei vielen Internet-Diensten erfolgt die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers. Dies kann sich ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen (IP-Spoofing) ans fremde Rechnersystem schickt. Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit unbeschränkter Administratorberechtigung, gewährt.

Gegenmaßnahmen:
Konfiguration eines Packet Filters, so dass alle Pakete mit ungültigen IP-Adressen*) und mit offensichtlich gefälschten IP-Adressen (z. B. IP-Pakete von außen mit internen Adressen) verworfen werden und nicht ins System gelangen können. Hierbei sollte man ebenfalls verhindern, dass IP-Pakete mit ungültigen Adressen das eigene System verlassen können. **)

*) definiert im RFC 1597

**) Weitere Hinweise: RFC 2267 (Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing)

Angriffe mit gefälschten Paketen von ARP (Address Resolution Protocol) oder ICMP (Internet Control Message Protocols) basieren ebenfalls darauf, dass sich Rechner allein durch ihre IP-Adresse als legitimer Absender ausgeben können. So kann ein Angreifer bei einem Missbrauch von ARP die IP-Adresse eines anderen Benutzers in einem lokalen Netz übernehmen und damit selbst Verbindungen herstellen oder die Erreichbarkeit des anderen Rechners vollständig verhindern. Auch Firewalls, die aufgrund von IP-Adressen entscheiden, ob eine Verbindung zulässig ist, lassen sich dadurch täuschen. Bei ICMP-Angriffen werden gefälschte Statusmeldungen verschickt, die beispielsweise eine Umleitung der Pakete über einen Router des Angreifers bewirken oder die gesamte Kommunikation eines Rechners nach außen verhindern (Denial of Service Attack). Der "Ping of Death" ist ein besonderer ICMP-Angriff, bei dem zu große Pakete beim Empfänger einen Überlauf des Empfangspuffers verursachen und den Rechner zum Absturz bringen. Ein ähnlicher Effekt wird bei vielen Windows-Rechnern durch das Senden spezieller Pakete (Out-of-Band [OOB]) bevorzugt auf den Port 139 erreicht. Gegen diesen Winnuke-Angriff können einige Windows-Versionen durch Patches geschützt werden.

Gegenmaßnahmen:
Installation von Patches,
starke Authentisierung

Durch den "TCP Syn Flood"-Angriff können ebenfalls Rechner blockiert werden. Dabei wird ein WWW-Server mit einer großen Anzahl von IP-Paketen mit ungültigen Absenderadressen bombardiert, auf die das System vergeblich zu antworten versucht. Dadurch kann der ganze Server über einen längeren Zeitraum lahmgelegt werden.

Gegenmaßnahmen:
Installation von Patches

2.3.2 Dienstespezifische Sicherheitsrisiken

2.3.2.1 E-Mail und Usenet-News

Elektronische Post (E-Mail) kann mitgelesen werden, sofern sie nicht verschlüsselt ist. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können – wie bei einem Transfer per Diskette – Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Gegenmaßnahmen:
Verschlüsselung und digitale Signatur,
Virenschutzsysteme

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, wies lange Zeit eine ganze Reihe von Sicherheitslücken auf, die zu einer Zugangsmöglichkeit von Administratorrechten führen konnten. Mittlerweile steht sendmail mit der Version 8.10 zur Verfügung, in dem diese Sicherheitslücken beseitigt wurden. Auch nach der Installation dieser neuen sendmail-Version ist es jedoch sinnvoll, regelmäßig die Meldungen über neue sicherheitsrelevante Fehler zu verfolgen und gegebenenfalls entsprechende Patches einzuspielen.

2.3.2.2 Telnet

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Selbst wenn sich ein Angreifer keinen Zugang mit Administratorrechten verschaffen kann, gelingt es ihm häufig, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

Gegenmaßnahmen:
Einschränkung der Telnet- und verwandten Dienste auf die notwendigen Adressen und Ports an einer Firewall

Mit Hilfe verschiedener Programme (z. B. das Cracker-Tool “Juggernaut”) können mittlerweile Telnet-Verbindungen “entführt” werden, d. h., der Angreifer

kann damit nicht nur Passwörter mitlesen, sondern auch in die Verbindung eingreifen, den ursprünglichen Benutzer abhängen und statt dessen sich selbst einklinken. Ähnliche Sicherheitsrisiken bestehen für "R-Utilities" wie rlogin.

Gegenmaßnahmen:
Vollständiger Verzicht auf den Telnet-Dienst sowie auf rlogin, rsh und rcp, statt dessen Verwendung von SSH (Secure Shell), einem Software-Paket, mit dem man durch anerkannte kryptographische Verfahren eine zuverlässige gegenseitige Authentisierung und eine transparente Verschlüsselung des gesamten Datenstroms erreichen kann. Dabei werden statt rlogin, rsh und rcp neue Programme ssh und scp eingesetzt. Das SSH-Paket steht für alle gängigen Betriebssysteme zur Verfügung (z. B. für UNIX: ftp://ftp.cs.hut.fi/pub/ssh/ oder ftp://ftp.cert.dfn.de/pub/tools/net/ssh; für Windows (kommerziell): http://www.europe.datafellows.com/f-secure/fssh-reg.htm).

2.3.2.3 FTP

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen bestimmter FTP-Server (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsrelevante Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Passwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Lässt man zu, dass Benutzer eines FTP-Servers anonym eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

Gegenmaßnahmen:
Ersatz des FTP-Dienstes (incl. rcp) durch Programme aus dem SSH-Paket (scp) oder Konfiguration eines SSH-Kanals mit Verschlüsselung und Authentisierung, Beschränkung durch Vergabe von entsprechenden Zugriffsrechten

2.3.2.4 WWW

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) oder anderen Verschlüsselungen lässt sich die Kommunikation abhören. Außerdem können Skripte zur dynamischen Generierung von Dokumenten Sicherheitslücken aufweisen.

Ende 1996 wurde die Angriffsmethode Web-Spoofing bekannt, bei der ein Angreifer seinen Server zwischen das eigentliche Zielsystem und den Rechner des Benutzers schaltet. Der Angreifer erstellt auf seinem System eine täuschend echte Kopie der Daten, die er komplett kontrollieren und für seine Belange modifizieren kann. Danach hat er nach Belieben die Möglichkeit, vom Benutzer verschickte Informationen abzufangen oder zu manipulieren.

Gegenmaßnahmen:
Verschlüsselung und digitale Signatur für die Kommunikation,
Zertifikate für Web-Server,
gegenseitige Authentisierung von Nutzer und Web-Server

2.3.2.5 DNS

Mit Hilfe des Domain Name Service (DNS) lassen sich Rechnernamen in IP-Adressen umsetzen und umgekehrt. Dabei besteht die Gefahr, dass Informationen über die Struktur des internen Netzes nach außen gelangen. Auch beim DNS gibt es mittlerweile die Angriffsmethode des Spoofing. Mit gefälschten Informationen im DNS können Datenströme in beliebige Bahnen gelenkt werden, wenn der Benutzer statt der numerischen IP-Adresse den leichter zu merkenden Rechnernamen angibt.

Gegenmaßnahmen:
Verbergen der Struktur des internen Netzes durch geeignete Anordnung von DNS-Servern,
Adressierung durch die numerische IP-Adresse, soweit praktikabel,
Einsatz eigener Domain Name Server

2.3.2.6 Finger

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen

Angriff genutzt werden können. Berühmt geworden ist dieser Dienst 1988 durch den so genannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, dass die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer passten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden (Buffer Overflow Bug). Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmierfehler finden sich auch heute noch in vielen anderen Serverprogrammen.

Gegenmaßnahmen:
Abschalten der Dienste, über die sich Angreifer sicherheitsrelevante Informationen aus dem System beschaffen können: finger, rup, rusers, rwho, SMTP EXPN, SMTP VRFY,
Installation von Patches gegen den Buffer Overflow Bug

2.3.2.7 SNMP

Mit Hilfe des Simple Network Management Protocol-Dienstes können Netzwerkkomponenten von zentraler Stelle aus verwaltet werden. Dazu können Informationen über die Konfiguration und den Betriebszustand der Komponenten abgefragt und verändert werden. Dies bietet dem Angreifer u. U. wertvolle Hinweise über die eingesetzte Hard- und Software, die für weitergehende Attacken ausgenutzt werden können.

Besondere Bedeutung kommt dabei den sog. Community Strings zu, die eine einfache Form der Authentisierung bei SNMP darstellen. Häufig ist bei Auslieferung der Community String “public” eingestellt, der einen unberechtigten Zugriff auf den Dienst sehr erleichtert.

Gegenmaßnahmen:
Verwendung schwer zu erratender Community Strings,
jedenfalls nicht “public”
Begrenzung der von SNMP zur Verfügung gestellten Informationen auf das Erforderliche

2.3.3 Aktive Inhalte/Aktive Elemente

2.3.3.1 ActiveX

ActiveX ist eine Entwicklung der Firma Microsoft. Es steht für eine Reihe von Technologien, die dafür sorgen, dass Windows-Anwendungen mit dem Internet oder Intranet zusammenarbeiten. WWW-Seiten können mit dieser Technologie um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden. Die Technologie besteht im Wesentlichen aus folgenden Elementen: ActiveX-Controls, Active Documents und Active Scripting.

ActiveX-Controls sind Programme, die auf einer WWW-Seite dargestellt oder als eigene Programme aufgerufen werden können. Active Documents ermöglicht die Anzeige und Betrachtung von Nicht-HTML-Dokumenten (z. B. Word oder Excel) innerhalb eines Browsers. ActiveX Scripting ermöglicht das Verwalten und die Kommunikation von ActiveX-Controls, beinhaltet einen Java-Compiler und ist eine Umgebung zur serverseitigen Nutzung von ActiveX-Controls. Eine ActiveX-Sicherheitsarchitektur gibt es nicht. Die vorhandenen Sicherheitsmechanismen bieten kein in sich konsistentes Sicherheitssystem. Microsoft setzt auf die Nachvollziehbarkeit der Herkunft der heruntergeladenen Codes durch Codesignierung. Für die Codesignierung setzt Microsoft die selbstentwickelte Authenticode Technologie ein. Sie beruht auf einer digitalen Signatur und erlaubt neben der sicheren Identifikation des Absenders den Nachweis der Echtheit der übertragenen Codes. Dieses Verfahren macht aber keine Aussage über die Funktionsweise der Software selbst und ob sie gewollt oder ungewollt (Programmierfehler) schadensstiftende Wirkung entfalten kann.

Microsoft arbeitet mit der Firma Verisign als Zertifizierungsstelle zusammen und vergibt zwei unterschiedliche Zertifikate: Individualzertifikate und kommerzielle Zertifikate. Es existiert ein mehrstufiges Sicherheitssystem im Zusammenspiel von ActiveX und den unterschiedlichen Browsern. Neben der Möglichkeit, die ActiveX-Funktionalität (gilt für alle Browser) abzuschalten, besteht auch die Option, im Internet-Explorer einen Sicherheitslevel (hoch, mittel und niedrig) vorzugeben. Bei einem hohen Sicherheitslevel werden nur zertifizierte ActiveX-Controls akzeptiert. Bei einem mittleren Level müssen nicht zertifizierte ActiveX-Controls explizit freigegeben werden. Ein niedriger Level bietet gar keinen Schutz. Eine weitere Möglichkeit, sich zu schützen, bieten ActiveX-Filter, die Listen mit Servern definieren, von denen ActiveX-Komponenten akzeptiert werden. Der Einsatz des Internet-Explorer-Administration-Kit (IEAK) ermöglicht die Erstellung von spezifisch angepassten Internet-Explorern.

ActiveX-Komponenten stellen, da sie keinerlei Einschränkungen bzgl. der Windows- und System-Funktionalität unterliegen, ein immenses Sicherheitsrisiko dar. Folgende Sicherheitsrisiken sind bisher bekannt: Ausforschung von Nutzern und Computersystemen, Installieren und Ausführen von Viren und Trojanischen Pferden, Beschädigung von Systemressourcen und Überlasten des Systems. Aus Sicherheitsgründen empfiehlt es sich daher, die ActiveX-Unterstützung gänzlich abzuschalten.

Gegenmaßnahmen:
Abschalten der ActiveX-Unterstützung,
Verwendung des Microsoft-Authenticodes,
Aktivieren einer hohen Sicherheitsstufe im Internet-Explorer,
Einsatz von ActiveX-Filtern und des Internet-Explorer-Administration-Kits in Netzwerken

Abschließend sei noch auf die unzureichenden Sicherheitsmechanismen der Betriebssystemplattformen hingewiesen. Die Plattform Windows 95 verfügt über keinerlei eingebaute Sicherheitsmechanismen zur Abwehr von Angriffen, und unter Windows NT laufen ActiveX-Controls im Rechteraum (mit den Zugriffsrechten) des gerade angemeldeten Benutzers.

2.3.3.2 Java

Java ist eine objektorientierte Programmiersprache, die unabhängig von der jeweiligen Systemplattform nutzbar ist. Sie wurde von SUN Microsystems entwickelt. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikations) sowie Anwendungen für das WWW (Java-Applets) zu schreiben. Java-Applets können in HTML-Seiten integriert, über das Internet angefordert und auf beliebigen Rechnern ausgeführt werden, ohne dass der Entwickler die lokale Umgebung des Anwenders kennen muss. Einzige Bedingung für die Lauffähigkeit ist die Verfügbarkeit der JVM (virtuelle Java Maschine) auf der Plattform. Java verfügt über ein integriertes Sicherheitssystem. Das Sandbox-System ist mehrstufig, bezogen auf die vier Softwareebenen, die bei der Herstellung und Ausführung von Java-Funktionen beteiligt sind:

1. Programmiersprache Java,
2. Virtuelle Java Maschine,
3. Lader für Java-Klassen und
4. Java Bibliotheken.

Ist JVM Bestandteil des HTML-Viewers, werden Applets ausgeführt, die sehr strengen Sicherheitskontrollen unterliegen. Applets, die über das Netz geladen werden, haben auf dem Client keine Lese- und Schreibrechte, können keine fremden Programme starten, keine Systemfunktionen aufrufen, keine Netzwerkverbindung zu anderen Rechnern aufbauen, keine zusätzlichen Bibliotheken laden und kennzeichnen Fenster besonders, die durch Applets gestartet wurden.

Applets können im Standardfall auch nur definierte Systemeigenschaften (z. B. Betriebssystem NT) lesen. SUN bietet in neueren Versionen die Möglichkeit, mit **signierten Applets** zu arbeiten. Die Applets werden zertifiziert und mit einer digitalen Signatur versehen, bevor sie im Netz zur Verfügung gestellt werden. Somit kann der Client die Authentifikation und die Herkunft prüfen. Die Signierung sagt nichts über die Funktionalität des Programmes. Die Java-Spezifikation bietet mit ihren durchdachten Mechanismen eine ausreichende Sicherheit, aber durch Implementierungsfehler wurden Angriffe durch Java-Applets möglich. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen modifizieren (durch Programmier- und Implementationsfehler in den Ablaufumgebungen), die eine weitere Nutzung des Systems verhindern (**Überlasten des Systems**) oder die Nutzer ausforschen oder belästigen.

Um sich vor Angriffen zu schützen, bieten sich mehrere Optionen an. Zusätzlich zu dem eigenen Sicherheitssystem können noch folgende Maßnahmen ergriffen werden. Man kann z. B. im Browser **die Java-Funktionalität abschalten**. Einen weiteren Schutz bieten **Java-Filter**, die Listen mit Servern definieren, von denen Java-Applets akzeptiert werden. In neueren Browser-Versionen ist das **Arbeiten mit signierten Applets** möglich.

Gegenmaßnahmen:
Abschalten der Java-Funktionalität, Einsatz von Java-Filtern, Arbeiten mit signierten Applets,
Verwendung von Browsern, bei denen JVM sauber implementiert ist

2.3.3.3 JavaScript

JavaScript ist eine von der **Firma Netscape Communication** entwickelte **Skriptsprache,** die plattformunabhängig ist. Sie wird direkt in die HTML-Seiten eingebettet und über einen Interpreter interpretiert und ausgeführt. Die Motivation für die Entwicklung von JavaScript waren die Unzulänglichkeiten der vorhandenen Techniken (HTML und CGI) für Benutzer-Interaktivitäten. Jede Interaktion musste an den Server gesendet werden, um mit Hilfe des CGI-Pro-

grammes Plausibilitätsprüfungen durchzuführen. Durch den Einsatz von JavaScript wurde die Anzahl der notwendigen Verbindungen zum Server drastisch verringert. Dynamisch zur Laufzeit können mit JavaScript beispielsweise Eingaben überprüft oder auch Berechnungen durchgeführt werden. Außerdem lassen sich wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formularelementen oder das Anpassen von Browser-Einstellungen, verwirklichen. Ein Zugriff auf Dateisysteme auf anderen Rechnern ist nicht möglich.

Netscape bietet die Möglichkeit, mit **zertifizierten JavaScript-Codes** zu arbeiten. Es wurden jedoch Sicherheitsprobleme in zwei Bereichen bekannt, zum einen in der **Ausforschung von Nutzern und Computersystemen** und zum anderen in der **Überlastung von Rechnern**. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen durch Programmierfehler und Implementierungsfehler in den Ablaufumgebungen modifizieren oder eine weitere Nutzung des Systems – vorsätzlich erzeugt oder ungewollt durch Programmierfehler – verhindern, und Angriffen, die das Lesen von fremden Nachrichten, Ändern von Nachrichten und Verschicken von Texten ermöglichen. Die meisten Sicherheitslöcher sind implementierungsabhängig.

Gegenmaßnahmen:
Arbeiten mit zertifizierten JavaScript-Codes oder das Abschalten der JavaScript-Funktionalität,
Verwendung von Browsern, bei denen die Anwendung sauber implementiert ist

2.3.3.4 Plug Ins

Browser Plug Ins sind auf dem Client laufende Software-Module, die den Funktionsumfang des Browsers erweitern und beispielsweise die Darstellung von Audio- und Videodaten erlauben. Plug Ins sind plattformabhängig, belegen lokalen Plattenspeicher und müssen vom Benutzer beschafft und installiert werden.

Gegenmaßnahmen:
Schulung der Benutzer, um unbeabsichtigtes Installieren der Software zu verhindern

2.3.3.5 Cookies

Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Die Anwendungsmöglichkeiten gehen jedoch weit darüber hinaus.

Typischerweise werden Cookies eingesetzt, damit der Nutzer das Angebot des angewählten Webservers auf seine persönlichen Belange hin abstimmen kann, bzw. um dem Webserver zu ermöglichen, sich selbsttätig auf die (vermuteten) Bedürfnisse des Nutzers einzustellen. Ein Betreiber von WWW-Diensten kann jedoch aus geeignet gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über den Benutzer gibt und ihn so als geeignete Zielperson (z. B. für Werbebotschaften) identifiziert. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist mit dem Cookie-Mechanismus selbst nicht möglich. Da die Cookie-Informationen, die auch benutzerbezogene Passwörter für Web-Seiten umfassen können, jedoch in einer Datei im Dateisystem auf dem Rechner gespeichert werden, kann ein Unberechtigter beispielsweise mit Hilfe von ActiveX-Controls (siehe Abschnitt 2.3.3.1) darauf zugreifen.

Problematisch sind Cookies trotz dieses vergleichsweise geringen Gefährdungspotentials für die Computersicherheit aufgrund ihrer geringen Transparenz für den Benutzer. Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert wird, sofern er keine besonderen Maßnahmen ergreift. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden somit allein vom Betreiber des WWW-Servers bestimmt; der Internet-Nutzer hat hierauf im normalen Betrieb keinen Einfluss. Es hängt wesentlich von der Initiative des Nutzers und seiner technischen Kenntnis und Ausrüstung ab, ob er Cookies bemerkt und sich ggf. vor ihnen schützen kann.

Gegenmaßnahmen:
Konfiguration des Browsers, so dass Cookies nicht oder wenigstens nicht automatisch akzeptiert werden und Cookies, die gespeichert werden sollen, angezeigt werden, Löschen bereits gespeicherter Cookies (z. B. Datei cookies.txt bei Netscape-Browsern), Einsatz von Cookie-Filtern

3 Firewall-Systeme

3.1 Grundlagen

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen oder durch mehrere dezentrale Zugänge erfolgen. Aus Sicherheitsgründen ist für ein (Teil-) Netz mit einheitlichem Schutzbedarf ein zentraler Zugang vorzuziehen. Die durch die Anbindung hervorgerufenen Sicherheitsrisiken lassen sich durch Einsatz einer Firewall reduzieren.

Unter einer Firewall ("Brandschutzmauer") wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin zu erreichen, dass jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und dass Missbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, dass die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleichwohl sind Firewall-Lösungen auch geeignet, die "grenzüberschreitenden" Aktivitäten der internen Nutzer, d. h. den Übergang zwischen verschiedenen Teilnetzen (z. B. Ressortnetze) innerhalb eines Verwaltungsnetzes, zu begrenzen. Mit Hilfe von Firewall-Systemen lassen sich die vorher in der Kommunikationsanalyse definierten Anforderungen weitgehend technisch erzwingen (Policy-Enforcer).

3.1.1 Charakteristika von Firewall-Systemen

Firewalls weisen die folgenden Charakteristika auf:

- Die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz.
- Im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau. Eine weitere Differenzierung nach Sicherheitsstufen geschieht – zumindest auf der Ebene des Netzes – nicht.
- Die Firewall setzt eine definierte Sicherheitspolitik (**Security Policy**) für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen.
- Es besteht die Notwendigkeit, die Benutzerprofile der internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen, auf die Firewall abzubilden.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die EDV-Infrastruktur.

3.1.2 Schutzniveau

Von besonderer Relevanz ist es, für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau zu definieren. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

1. einheitlich hohes Schutzniveau im internen Netz, d. h. Orientierung am höchsten vorhandenen Schutzbedarf;
2. einheitlich niedriges Schutzniveau, d. h. Orientierung am niedrigsten vorhandenen oder an einem insgesamt geringen oder mittleren Schutzbedarf;
3. einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netzkomponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten Variante 2 indiskutabel und mit den Anforderungen des Datenschutzrechts unvereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d. h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u. a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Missbrauch.

3.2 Firewall-Technologien

Eine Firewall kann durch verschiedene Konzepte realisiert werden. Im Wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (Packet Screen, Screening Router)
- Application Level Gateway (Dual-homed Gateway)
- Stateful Inspection (Stateful Packet Filter, Dynamic Packet Filter)

Ein **Packet Filter** (auch **Packet Screen** oder **Screening Router**) ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und der unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell-

und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist sowohl einschränkbar, welche Rechner im zu schützenden und welche im unsicheren Netz an der Kommunikation beteiligt sein dürfen, als auch, welche Kommunikationsdienste erlaubt sind. Die Filterregeln sind an die Netzschnittstellen gebunden. Sie werden vom Packet Filter in der Reihenfolge abgearbeitet, in der sie angegeben sind.

Ein **Application Level Gateway** ist ein speziell konfigurierbarer Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Level Gateway arbeitet im Gegensatz zum Packet Filter auf der Anwendungsschicht, d. h., die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Für jeden Dienst (Telnet, FTP usw.) werden **Security Proxys** eingeführt, die den direkten Zugriff auf den Dienst verhindern. Hierbei bestehen z. B. die Möglichkeiten einer ausführlichen Protokollierung (Audit) und einer benutzerbezogenen Authentisierung für die unterschiedlichen Dienste. Die meisten Application Level Gateways sind nicht in der Lage zu unterscheiden, über welche Netzschnittstelle ein Paket hereinkommt. Ein Application Level Gateway mit zwei Netzschnittstellen wird **Dualhomed Gateway** genannt.

Die Kombination von Packet Filter und Application Level Gateway wird als **Screened Gateway, Transparent Application Gateway** oder **Sandwich-System** bezeichnet und erhöht die Sicherheit der Firewall gegenüber den beiden Einzelkomponenten erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

Stateful Inspection (auch **Stateful Packet Filter** oder **Dynamic Packet Filter**) ist eine recht neue Firewall-Technologie und arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht. Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul, das dynamisch im Betriebssystemkern geladen ist, zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen. Die Regeln, nach denen das Modul agiert, können sehr differenziert vorgegeben werden. Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist. Im Out-Of-Band-Betrieb erfolgt die Wartung und Konfiguration nicht über TCP/IP. Die Firewall besitzt dann keine eigene IP-Adresse, so dass keine Möglichkeit besteht, sie über TCP/IP direkt aus

den angeschlossenen Netzen anzusprechen oder auf diesem Wege anzugreifen. Optional führt die Firewall ein Rewriting durch, d. h., Pakete werden vor dem Weitersenden nach vorgegebenen Regeln transformiert.

Stateful Inspection vereinigt bereits konzeptuell die Schutzmöglichkeiten von Packet Filter und Application Level Gateway, so dass diese beiden Funktionen nicht in getrennten Komponenten realisiert werden müssen. Experten streiten sich darüber, welches Konzept in welcher Realisierung mehr Sicherheit mit sich bringt. Inzwischen werden auch hybride Firewalls angeboten, die zusätzlich zur Stateful Inspection wie beim Application Gateway Proxys zur Verfügung stellen.

	Vorteile	**Nachteile**
Packet Filter (Router oder Rechner mit spezieller Software)	leicht realisierbar, da von vielen Routern angeboten leicht erweiterbar für neue Dienste Router auf dem Markt verfügbar Transparenz für den Benutzer Arbeitsgeschwindigkeit	Übernahme des Packet Filter durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit es ist bei den meisten Produkten nicht möglich, Dienste nur für bestimmte Benutzer zuzulassen alle Dienste, die erlaubt sind und erreicht werden können, müssen sicher sein Protokollierung nur auf unteren Netzschichten möglich keine Authentisierung möglich
Dual-homed Gateway (Application Level Gateway mit zwei Netzschnittstellen)	kein Paket kann ungefiltert passieren aussagekräftige Protokollierung auf höheren Schichten möglich interne Netzstruktur wird verborgen durch den Einsatz von Network Address Translation (NAT)	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit keine Transparenz für den Benutzer Probleme bei neuen Diensten, schlechte Skalierbarkeit

Screened Gateway (Anordnung aus Application Level Gateway mit einem oder zwei Packet Filtern (Teilnetz-Bildung))	kein direkter Zugang zum Gateway möglich interne Netzstruktur wird verborgen Network Address Translation (NAT) vereinfachte Regeln durch 2. Filter durch Einsatz mehrerer Gateways lässt sich die Verfügbarkeit steigern aussagekräftige Protokollierung möglich	keine Transparenz für den Benutzer bei Realisation mit mehreren Rechnern und Routern: erhöhter Platzbedarf Probleme bei neuen Diensten, schlechte Skalierbarkeit
Stateful Inspection (Firewall-Rechner mit zustandsabhängiger Analyse und Reaktion)	gute Skalierbarkeit arbeitet auf Netz- und Anwendungsschicht Out-Of-Band-Betrieb: keine Angriffsmöglichkeit über TCP/IP interne Netzstruktur wird verborgen Rewriting möglich (über NAT hinaus) umfangreiche Authentisierungsvarianten	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit keine Zwischenspeicherung, daher nicht volle Gateway-Funktionalität und kein Caching schneller Rechner erforderlich, da wegen der umfangreichen Analyse und Aktionsmöglichkeiten sonst Performance-Einbußen

3.3 Firewall-Architekturen

Neben den im Folgenden dargestellten Architekturen von Firewalls sind auch Abwandlungen oder Kombinationen der Anordnungen möglich.

3.3.1 Zentrale Firewalls

Rein zentrale Firewall-Lösungen (vgl. Abbildung 3.1) sind durch folgende Aspekte charakterisiert:

- Die zentrale Firewall bildet die einzige Schnittstelle (Choke Point) zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet.

- Innerhalb des gesamten Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht.
- Eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich.
- Die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus. Abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar.
- Es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muss sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muss sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, dass gerade von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

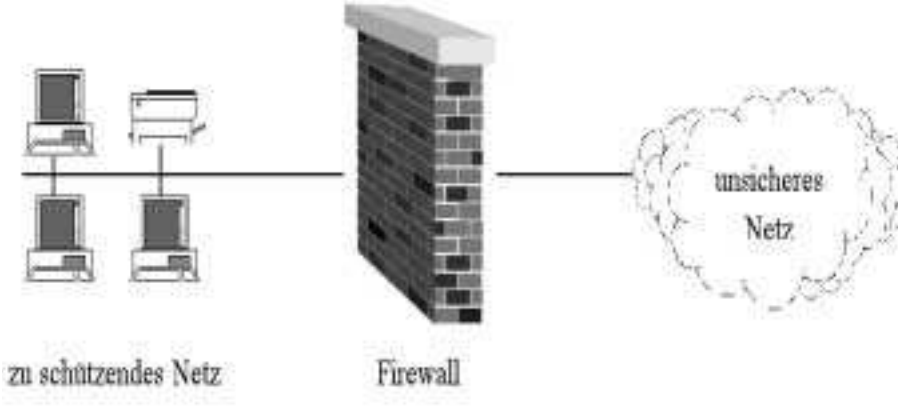


Abbildung 3.1: Zentrale Firewall-Anordnung

Ein weiterer Nachteil zentraler Firewalls besteht in dem – auch aus dem Großrechnerbereich bekannten – Problem, dass eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da eine Firewall Zugriffe innerhalb des internen Netzes nicht kontrolliert, besteht bei rein zentralen Lösungen die Gefahr, dass das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internet-Anbindung", muss bei einer Gesamtbetrachtung von Netzsicherheit jedoch unbedingt einbezogen werden.

Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Missbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

3.3.2 Gestaffelte Firewalls

Gestaffelte Firewall-Lösungen (vgl. Abbildung 3.2) sind durch folgende Aspekte charakterisiert:

- Es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen.
- Innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau.
- Eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet.
- Auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitspolitik für das Gesamtnetz voraus. Bei ihrer Definition müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen. Darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren.
- Die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.
- Auch die dezentralen Firewalls müssen qualifiziert administriert werden.

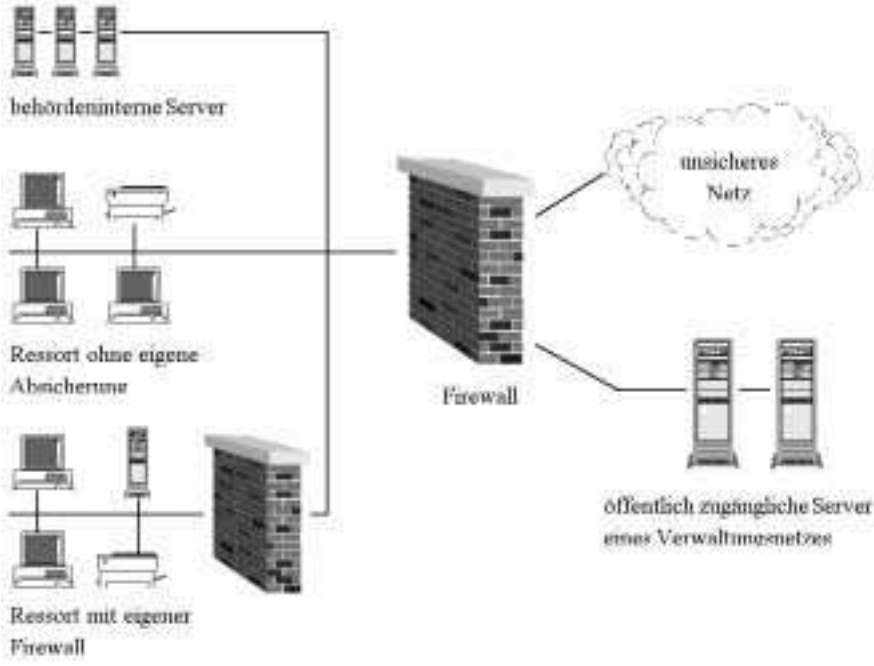


Abbildung 3.2: Gestaffelte Firewall-Anordnung

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Technologien wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden. Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung "wilder" Internet-Zugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und die dezentralen Firewalls verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im Wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

3.3.3 Entmilitarisierte Zone

Server, die Dienste für Internet-Nutzer zur Verfügung stellen (z. B. WWW oder Mail), werden häufig hinter einer Firewall in der so genannten **entmilitarisierten Zone (DMZ, Demilitarized Zone,** auch **Screened Subnet**) eingerichtet, von der das interne Netz durch eine (weitere) Firewall abgeschottet ist. Dies hat den Vorteil, dass das lokale Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum WWW-Server gelangt.

Die entmilitarisierte Zone kann beispielsweise zwischen zwei Firewalls realisiert werden (vgl. Abbildung 3.3). Durch Verwendung unterschiedlicher Firewall-Produkte lässt sich dabei eine höhere Sicherheit erreichen, da mögliche Fehlfunktionen bei unabhängiger Entwicklung der Produkte wahrscheinlich nicht gleichzeitig auftreten.

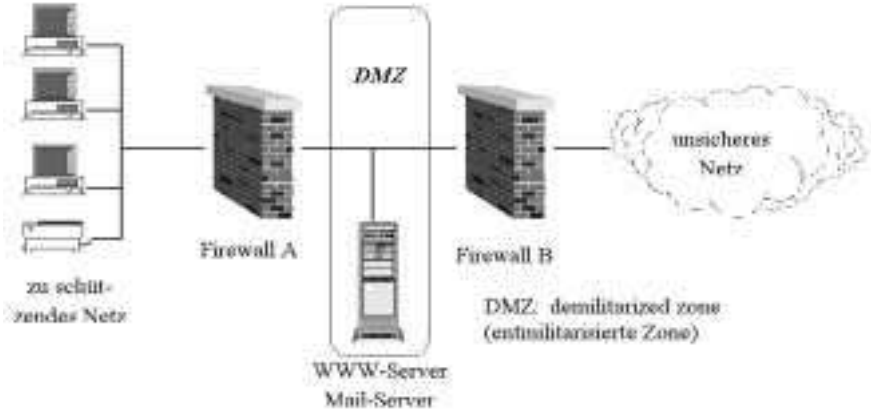


Abbildung 3.3: Kaskadierte Firewall-Anordnung mit DMZ

Die Aufgaben der beiden Firewalls können auch von nur einer Firewall mit mehreren Schnittstellen übernommen werden, mit denen sich mehrere Netze mit

unterschiedlicher Sicherheit bilden lassen. So können auch eine oder mehrere entmilitarisierte Zonen eingerichtet werden. Diese Lösung ist kostengünstiger, verzichtet aber auf die erhöhte Sicherheit.

3.3.4 Screened Gateway

Zumeist werden neben der Firewall Router eingesetzt, die oft die Funktion von Packet-Filtern übernehmen können. Damit lässt sich eine "Sandwich-Lösung" (vgl. Abbildung 3.4) realisieren, die durch Verwendung unterschiedlicher Systeme eine erhöhte Sicherheit gewährleisten kann. Auch hier ist die Einrichtung einer entmilitarisierten Zone möglich.

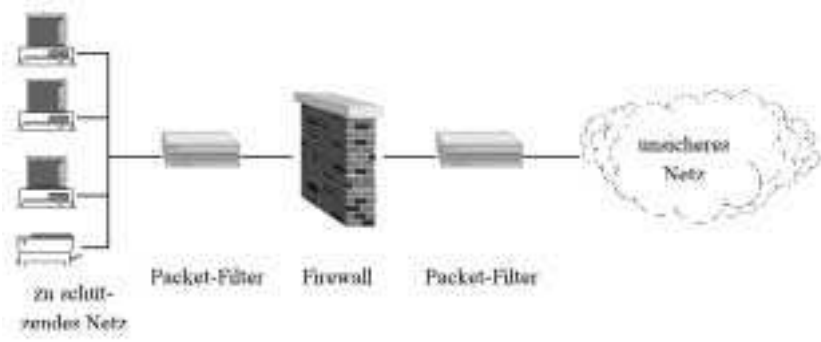


Abbildung 3.4: Screened Gateway (Sandwich-System)

Die Anordnung von Mail-, WWW- und DNS-Servern bei Sandwich-Systemen mit entmilitarisierten Zonen wird in der folgenden Abbildung beispielhaft veranschaulicht:

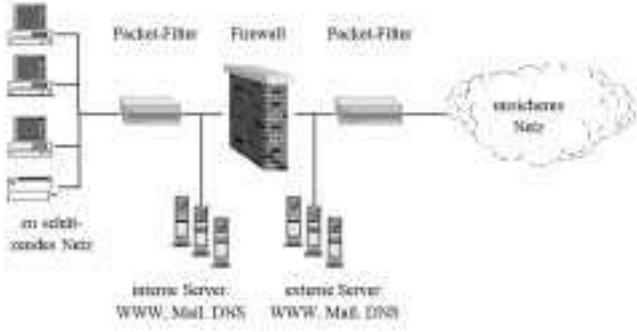


Abbildung 3.5: Screened Gateway (Sandwich-System) mit DMZ

4 Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall

4.1 Allgemeines

Firewalls sind selbst keine eigenständigen Telekommunikations-, Tele- oder Mediendienste, sondern als unselbständiger Bestandteil eines solchen Dienstes zu betrachten. Daher kommt für den Betrieb einer Firewall das Datenschutzrecht zur Anwendung, das auch für den zu Grunde liegenden Dienst gilt. Deshalb sollen im Folgenden kurz die Anwendungsbereiche der für die Dienste einschlägigen Datenschutzvorschriften erläutert werden.

Das Verhältnis zwischen Telekommunikationsdiensten einerseits und Tele- bzw. Mediendiensten andererseits wird grundsätzlich durch die in § 2 Abs. 1 Teledienstegesetz (TDG)/§ 2 Mediendienste-Staatsvertrag (MDStV) enthaltenen Begriffsdefinitionen beschrieben. Danach handelt es sich bei einem Teledienst um einen elektronischen Informations- und Kommunikationsdienst, der für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt ist und dem eine **Übermittlung mittels Telekommunikation** zu Grunde liegt. Mediendienste sind solche elektronischen Informations- und Kommunikationsdienste, die an die Allgemeinheit gerichtet sind.

Ausgehend von diesen gesetzgeberischen Vorgaben kann die Beziehung zwischen Telekommunikations- und Tele- bzw. Mediendiensten durch ein Schichtenmodell beschrieben werden. Dabei stellt die Telekommunikation die Transportebene dar, auf deren technischer Basis der jeweilige Tele- bzw. Mediendienst erfolgt. Das hierfür maßgebliche datenschutzrechtliche Rechtsregime wird durch die einschlägigen Vorschriften des Telekommunikationsgesetzes (TKG) sowie der Telekommunikations-Datenschutzverordnung (TDSV) bestimmt. Zusätzlich greifen nachrangig die Regelungen des allgemeinen Datenschutzrechts (Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze). Um im Bild zu bleiben, handelt es sich bei den Tele-/Mediendiensten demgegenüber um die Transportbehälter. Für diesen Bereich sind das TDG sowie das Teledienstedatenschutzgesetz (TDDSG) bzw. der MDStV einschlägig. Schließlich muss noch eine dritte Ebene betrachtet werden, nämlich die durch bzw. mit den Tele-/Mediendiensten vermittelten – also in diesen Transportbehältern befindlichen – Inhalte. Die rechtliche Bewertung der Inhalte richtet sich nach den jeweiligen Gesetzen, wie etwa den Verwaltungsverfahrensgesetzen, dem Strafgesetzbuch, dem Gesetz gegen den unlauteren Wettbewerb, dem BDSG oder den Landesdatenschutzgesetzen.

Die Verarbeitung und Nutzung personenbezogener Daten auf der Transportebene wird in Umfang und Grenzen maßgeblich durch das Fernmeldegeheimnis (Art. 10 GG, § 85 TKG) geprägt, das die dabei anfallenden Verbindungsdaten und die Kommunikationsinhalte schützt. Nach § 85 Abs. 2 TKG sind alle zur Wahrung des Fernmeldegeheimnisses verpflichtet, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Entsprechend den einschlägigen Begriffsbestimmungen in § 3 TKG ist es dabei unerheblich, ob diese Dienste für die Allgemeinheit bestimmt sind oder nur einem bestimmten Kreis von Berechtigten gegenüber angeboten werden. Ohne Bedeutung ist auch, ob Telekommunikationsdienste mit oder ohne Gewinnerzielungsabsicht erbracht werden. Durch diesen weiten Anwendungsbereich soll ein umfassender Schutz des Fernmeldegeheimnisses gewährleistet werden. Vor diesem Hintergrund muss beispielsweise auch eine Behörde, die ihren Mitarbeitern die private Nutzung der vorhandenen Telekommunikationsanlage erlaubt, als Telekommunikationsdiensteanbieter mit all den sich daraus ergebenden Verpflichtung beurteilt werden. Auch die bei Tele- und Mediendiensten entstehenden Nutzungsdaten unterliegen dem Schutz durch das Fernmeldegeheimnis, weil diese Dienste definitionsgemäß auf Grundlage der Telekommunikation abgewickelt werden.

Bei der Protokollierung sind deshalb nicht nur die Bestimmungen des TDDSG bzw. des MDStV, sondern auch das Fernmeldegeheimnis und ggf. einschlägige Bestimmungen über kommunizierte Inhalte (z. B. Arzt- oder Sozialgeheimnis) zu beachten. Betroffen von einer Protokollierung durch Firewalls sind in erster Linie die Bediensteten oder Arbeitnehmer der Stelle, deren Datenverarbeitungsanlage von der Firewall geschützt werden soll, im Fall der E-Mail-Kommunikation und bei interaktiven Angeboten aber auch die externen Kommunikationspartner. Bei Angriffen auf die Firewall können zudem personenbezogene Daten der Angreifer registriert werden.

Hinsichtlich des Umfangs und der Zulässigkeit der Protokollierung von Zugriffen, die über eine Firewall erfolgen, und der Kontrolle von Inhaltsdaten lassen sich die im Folgenden beschriebenen Fallkonstellationen unterscheiden.

4.2 Kontrolle von Inhaltsdaten bei E-Mail-Kommunikation

Die Frage nach der Zulässigkeit der Kontrolle von Inhaltsdaten wird insbesondere relevant bei eingehenden E-Mails, die nicht an die Mail-Adresse einer zentralen Poststelle, sondern an die Mail-Accounts einzelner Arbeitnehmer der betreffenden Dienststelle gerichtet sind. Hierbei können folgende Fallkonstellationen unterschieden werden:

4.2.1 Kontrolle auf Virenbefall mittels automatischem Virencheck

Sowohl bei dienstlicher als auch bei privater Nutzung bestehen grundsätzlich gegen eine Kontrolle auf Virenbefall mittels automatischem Virencheck keine Bedenken, soweit die Kontrolle ausschließlich automatisch erfolgt und die Kenntnisnahme von den Inhalten privater E-Mails durch Vertreter der Dienststelle (z. B. den Systemadministrator) nicht ohne Einwilligung des Benutzers erfolgt.

Dadurch kann allerdings eine dezentrale Überprüfung der Dateien auf Viren nicht bzw. nicht vollständig ersetzt werden, da Virencheckprogramme Viren, die in verschlüsselten E-Mails enthalten sind, nicht erkennen können. Mindestens für diese E-Mails muss daher nach der Entschlüsselung eine Virenüberprüfung beim Benutzer selbst erfolgen.

4.2.2 Kontrolle eingehender dienstlicher E-Mails

Wie bei herkömmlicher Post können Vorgesetzte sich auch eingegangene dienstliche E-Mails von den betreffenden Mitarbeitern vorlegen lassen. Der Arbeitnehmer hat auf Verlangen dem Arbeitgeber Ausdrucke der E-Mails auszuhändigen bzw. diesem den Zugang zu den E-Mails zu ermöglichen.

4.2.3 Kontrolle eingehender privater E-Mails

Soweit die private Nutzung des E-Mail-Dienstes gestattet ist, ist der Arbeitgeber insoweit als Anbieter von Telediensten einzuordnen und unterliegt damit in Bezug auf die Protokollierung den Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) über die Verarbeitung personenbezogener Daten. Im Hinblick auf den Inhalt der privaten E-Mails der Beschäftigten hat er auch das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz (TKG) zu wahren. Daraus folgt insbesondere, dass es ihm untersagt ist, sich oder anderen über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Die Weitergabe von Informationen, die dem Fernmeldegeheimnis unterliegen, ist strafbewehrt.

Wenn die private Nutzung von E-Mail zugelassen wird, ergibt sich die Notwendigkeit, dienstliche und private E-Mails zu trennen. Hat der Mitarbeiter eine personalisierte E-Mail-Adresse nach dem Muster "Vorname.Name@Behörde.de", so kann nicht ausgeschlossen werden, dass eingehende Mails nicht an die Behörde, sondern an den Mitarbeiter privat gerichtet sind. Dieses Problem kann dadurch gelöst werden, dass den Beschäftigten für die dienstliche und die private Benutzung von E-Mail verschiedene E-Mail-Adressen zugewiesen werden.

Unabhängig vom Aufbau und von der Differenzierung der E-Mail-Adressen einer Behörde gilt, dass private E-Mails, die beim Posteingang fälschlich zunächst als dienstliche E-Mails angesehen wurden, so zu behandeln sind, wie bei der Behörde eingegangene, für einen Mitarbeiter bestimmte private Schreiben, deren privater Charakter nicht besonders, etwa durch den Zusatz "persönlich" gekennzeichnet ist. Sobald der private Charakter dieser E-Mails erkannt wurde, sind sie unverzüglich dem betreffenden Mitarbeiter zur alleinigen Kenntnis zu geben.

4.2.4 Kontrolle ausgehender E-Mails

Auch bei ausgehenden E-Mails kann die automatische Kontrolle auf Virenbefall sinnvoll sein. Zwar träfe der Schaden hier den Empfänger, dies kann allerdings eine Rufschädigung der absendenden Stelle zur Folge haben. Ausgehende private E-Mails sind genauso vom Fernmeldegeheimnis geschützt wie die eingehenden, so dass die inhaltliche Überprüfung ausscheidet.

Hinsichtlich ausgehender dienstlicher E-Mails gilt grundsätzlich das oben zu den eingehenden dienstlichen E-Mails Gesagte entsprechend. Die Vertreter der Dienststelle müssen feststellen können, welche Inhalte in dienstlichen E-Mails nach außen gelangt sind. Die Kontrolle der Inhalte durch die Vorgesetzten ist daher ohne weiteres zulässig. Darüber hinausgehend wäre es technisch durch den Einsatz entsprechender Auswertungsprogramme auch möglich, z. B. anhand der Absendezeiten und Länge der E-Mails oder mit der gezielten automatischen Suche nach darin verwendeten Begriffen eine umfassende Leistungs- und Verhaltenskontrolle zu bewirken. Der Einsatz derartiger Programme stellt allerdings einen weitgehenden Eingriff in das Persönlichkeitsrecht der Beschäftigten dar und ist daher lediglich in Ausnahmefällen und auch dann nur aufgrund einer Dienstvereinbarung zulässig.

4.3 Protokollierung von Internet-Zugriffen mittels einer Firewall

Für Art und Umfang der Protokollierung lassen sich vor allem zwei Szenarien unterscheiden:

- Die Firewall dient lediglich der Abschottung des internen Netzes gegen das Internet, Zugriffe von außen sind grundsätzlich nicht zugelassen. In diesem Szenario kommt die Protokollierung der zulässigerweise von innen erfolgenden Zugriffe der Mitarbeiter auf das Internet in Betracht. Dabei ist zwischen den Zugriffen bei dienstlicher und bei privater Nutzung zu unterscheiden. Außerdem kann die Protokollierung dazu dienen, den Versuch eines unzulässigen Zugriffs von außen rechtzeitig zu erkennen.
- In einem anderen Szenario geht es um Zugriffe von außen auf Komponenten des internen Netzes, die dafür grundsätzlich vorgesehen sind (z. B. Web-Server). Die selbstverständlich möglichen Mischformen bleiben der Einfachheit halber außer Betracht.

Ordnet man die Maßnahmen nach ihrer Zielrichtung, ergibt sich daraus folgendes Schema:

Abbildung 4.1: Protokollierung von Internetzugriffen

Soweit zur Aufrechterhaltung der Datensicherheit die Protokollierung erforderlich ist, stellt sich die Frage, wie lange die dabei erzeugten Logfiles aufbewahrt werden dürfen. Dies muss für den Einzelfall entschieden werden. Die Daten sind zu löschen, sobald sie für Zwecke der Datensicherheit nicht mehr erforderlich sind.

4.3.1 Protokollierung der von innen erfolgenden Zugriffe (Protokollierung von Mitarbeiterdaten)

Sämtliche Maßnahmen der Inhaltskontrolle und Protokollierung sind geeignet, die Beschäftigten einer Organisation zu überwachen und ihre Leistung und ihr Verhalten zu kontrollieren. In jedem Fall muss für die Betroffenen transparent sein, welche potenziell zur Überwachung ihres Verhaltens geeigneten Maßnahmen aktiviert sind. Derartige Maßnahmen unterliegen außerdem ohne Ausnahme der Mitbestimmung der gewählten Mitarbeitervertretungen (Personalrat bzw. Betriebsrat). Da – wie im Folgenden dargelegt wird – eine Reihe von Einzelfragen zu klären sind, bietet es sich an, zu diesen Themen eine Dienst- bzw. Betriebsvereinbarung abzuschließen.

Vorab ist festzuhalten, dass die Protokolldaten in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG) unterliegen, soweit die Protokollierung der Aufrechterhaltung der Datensicherheit dient.

Grundsätzlich ist eine pauschale, flächendeckende und "vorbeugende" Protokollierung aller Internet-Zugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig. Gleiches gilt auch bei der Nutzung eines Intranet. Hier sollte regelmäßig der Sperrung unerwünschter Angebote bzw. der Beschränkung des Zugriffs auf dienstlich erforderliche Angebote der Vorzug gegeben werden.

Für alle Kontrollmaßnahmen ergibt sich eine grundsätzliche Weichenstellung bei der Frage, ob den Nutzern die private Verwendung des dienstlichen Internetanschlusses erlaubt ist. Für den Dienstherrn bzw. Arbeitgeber besteht keine Pflicht, die private Nutzung zuzulassen. Ist die private Nutzung gestattet, so greift das Fernmeldegeheimnis nach § 85 TKG. Dieses umfasst den Inhalt der Telekommunikation und deren nähere Umstände (wer hat wann mit wem kommuniziert oder dies versucht?). Sämtliche Kontrollmaßnahmen sind dann nur noch unter sehr engen Voraussetzungen zulässig.

4.3.1.1 Dienstliche Nutzung

Beim Bereitstellen eines Internet-Zugangs für die ausschließlich dienstliche Nutzung handelt es sich nicht um einen Teledienst im Sinne des Teledienstegesetzes (TDG). Der Arbeitgeber bietet dem Arbeitnehmer keinen Dienst an, sondern stellt ihm lediglich ein Arbeitsmittel zur Verfügung; bei diesem "In-Sich-Verhältnis" fehlt das vom Teledienstegesetz vorausgesetzte Merkmal,

dass es sich bei Diensteanbieter und Nutzer um zwei unterschiedliche Rechtssubjekte handelt (vgl. § 3 TDG). Damit finden die Vorschriften des Teledienstedatenschutzgesetzes auf die Protokollierung der ausschließlich dienstlichen Nutzung von Telediensten keine Anwendung.

Zulässigkeit und Umfang der Protokollierung richten sich in diesen Fällen vielmehr nach den Vorschriften, die auf die Verarbeitung von Daten im jeweiligen Beschäftigungsverhältnis Anwendung finden, also z. B. nach dem jeweiligen Landesdatenschutz- bzw. Landesbeamtengesetz. Art und Umfang einer Protokollierung sollten durch eine Dienstvereinbarung geregelt werden.

Dagegen sollte die Protokollierung der dienstlichen Nutzung nicht auf die Einwilligung der Arbeitnehmer gestützt werden, da es auf Grund der Abhängigkeit im Beschäftigungsverhältnis häufig an der erforderlichen Freiwilligkeit der Einwilligung fehlt. Bei der dienstlichen Nutzung hat der Arbeitgeber grundsätzlich auch das Recht zu prüfen, ob das Surfen der Mitarbeiter im WWW tatsächlich vollständig dienstlich motiviert war. Allerdings gilt hier, wie bei der Kontrolle der ausgehenden dienstlichen E-Mails, dass eine automatisierte Vollkontrolle im Hinblick auf das Persönlichkeitsrecht der Beschäftigten auf erhebliche Bedenken stößt. In jedem Fall müssen die Beschäftigten auf die geplanten Überwachungsmaßnahmen und die drohenden Sanktionen ausdrücklich hingewiesen werden.

In der Regel geht es darum zu vermeiden, dass Mitarbeiter in der Arbeitszeit und unter Nutzung dienstlicher Ressourcen aus rein privatem Interesse auf Informationen zugreifen. Daher sollten nach Möglichkeit die bekanntesten Angebote (z. B. erotische Angebote, Spiele oder Börsenkurse) bereits gesperrt sein. Umgekehrt wäre es auch denkbar, die Zugriffe auf dienstlich erforderliche Angebote zu beschränken (Positivliste). Um weiteren Missbrauch zu verhindern, bietet es sich an, in einer Dienstvereinbarung datenschutzfreundliche Verfahren (z. B. stufenweise, zunächst nicht personenbezogene Protokollierung der Zugriffe) festzulegen.

4.3.1.2 Private Nutzung

Bei der privaten Nutzung eines vom Dienstherren zur Verfügung gestellten Internet-Zuganges handelt es sich um die Nutzung eines Teledienstes im Sinne des Teledienstegesetzes. Wenn der Arbeitgeber die private Nutzung gestattet, wird er damit zum Dienstanbieter im Sinne des § 3 des TDG. Art und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 des TDDSG. Außerdem gilt das Fernmeldegeheimnis aus § 85 TKG. Sind

bestimmte Protokollierungen aus technischer Sicht für die Aufrechterhaltung eines regelgerechten Firewall-Betriebs unabdingbar, können sie ergänzend auf § 9 BDSG nebst Anlage bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze gestützt werden.

4.3.2 Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe

4.3.2.1 Nur Anschluss des internen Netzes an das Internet; keine Angebote der öffentlichen Stelle nach außen

In diesen Fällen ist die Firewall nicht Bestandteil eines Tele- bzw. Mediendienstes. Die Vorschriften des Teledienstegesetzes bzw. des Teledienstedatenschutzgesetzes finden daher keine Anwendung. Zulässigkeit und Umfang der Protokollierung richten sich nach § 9 BDSG und Anlage. Für öffentliche Stellen des Bundes kommt als Rechtsgrundlage § 14 BDSG in Betracht; in den Ländern ggf. entsprechende Vorschriften der Landesdatenschutzgesetze.

4.3.2.2 Angebot nach außen (Web-Server)

Soll über eine Firewall der Zugriff aus dem Internet auf einen Web-Server einer öffentlichen Stelle reguliert werden, so bemisst sich die rechtliche Einordnung der Firewall nach der Einordnung des Angebotes, das die öffentliche Stelle auf dem betreffenden Web-Server macht. Dabei kann es sich – je nach Art des Angebotes – entweder um einen Teledienst im Sinne des Teledienstegesetzes handeln, aber auch um einen Mediendienst nach dem Mediendienste-Staatsvertrag (MDStV). Zulässigkeit und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 TDDSG bzw. § 15 MDStV. Für Zwecke der Datensicherung kann die Protokollierung auf § 9 BDSG und Anlage bzw. für öffentliche Stellen des Bundes ergänzend auf § 14 BDSG, in den Ländern auf entsprechende Vorschriften der Landesdatenschutzgesetze gestützt werden.

Die Protokollierung ist dabei auf das unabdingbar Notwendige zu begrenzen; der Anbieter unterliegt hier den Verpflichtungen zur datenarmen Gestaltung des Tele- bzw. Mediendienstes gemäß § 3 Abs. 4 TDDSG bzw. § 13 Abs. 5 MDStV.

Soweit die Protokollierung personenbezogen erfolgt, unterliegt der Anbieter darüber hinaus den Informationspflichten nach § 3 Abs. 5 TDDSG bzw. § 12 Abs. 6 MDStV auch hinsichtlich der Protokollierung personenbezogener Daten auf der Firewall. Soweit die Daten zur Gewährleistung der Datensicherheit oder

des Datenschutzes gespeichert werden, unterliegen sie der besonderen Zweckbindung nach § 14 Abs. 4 BDSG bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG).

Bei nach außen offenen Internet-Angeboten kann die Protokollierung an der Firewall nicht auf die Einwilligung des bzw. der Betroffenen gestützt werden, da eine rechtswirksame Einholung der Einwilligung von Betroffenen auf Grund der technischen Gegebenheiten im Internet nicht möglich ist.

5 Auswahl und Umsetzung der Sicherungsmaßnahmen; Betriebsphase

5.1 Security Policy und Sicherheitskonzept

Aus den Anforderungen der im Vorfeld gemachten Sicherheitsbetrachtungen der Kommunikations- und der Risikoanalyse ist ein Regelwerk zu erstellen. In dieser Security Policy sind die Rahmenbedingungen zur Einrichtung, zum Betrieb und zur Verwaltung der Systeme für die interne Kommunikation und die Verbindungen zum Internet festzulegen. Die Zuständigkeiten für Betrieb, Verwaltung und Administration der für den Verbund eingesetzten Kommunikationssyteme müssen aufeinander abgestimmt sein. Es müssen die notwendigen Maßnahmen aufgeführt werden, die dem Schutz nach innen und außen dienen. Bereiche mit sensiblen Datenbeständen müssen besonders berücksichtigt werden.

In Bezug auf die Firewall sollte die Security Policy folgende Festlegungen enthalten (vgl. [BSI]):

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzer werden zugelassen?
- Welche Ereignisse werden protokolliert, und wer wertet diese Daten aus?
- Welcher Datendurchsatz ist zu erwarten?

Da die Sicherheit des Gesamtsystems nicht allein von der Firewall bestimmt wird, sind in die Security Policy auch flankierende Vorgaben aufzunehmen, wie das Verbot von zusätzlichen Netzzugängen, z. B. per Modem oder ISDN, Virenschutz und Backup-Konzept. Basierend auf der Security Policy ist ein Sicherheitskonzept zu erstellen, welches die Vorgaben in konkrete Maßnahmen (Konfigurationen, Filterregeln etc.) umsetzt.

Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen einer schlüssigen Security Policy und eines davon abgeleiteten Sicherheitskonzepts sowie dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

5.2 Auswahl, Konfiguration und Wartung von Firewall-Systemen

Firewall-Systeme müssen transparent und einfach aufgebaut sein. Mit zunehmender Komplexität steigt auch die Wahrscheinlichkeit von Fehlern. Nicht für den Betrieb der Firewall benötigte Anwendungen und Systemprogramme sind daher zu löschen. Auch die Bedienung und die Konfiguration der Firewall müssen benutzungsfreundlich realisiert sein, da sonst unbeabsichtigte Fehleinstellungen Sicherheitseinbußen mit sich bringen. Vertrauenswürdige Systeme müssen ihre Funktionsweise offen legen, denn nur dann ist es Experten möglich, Hintertüren auszuschließen und die Gefahr von Sicherheitslücken fundiert zu diskutieren. Sicherheitszertifikate für Firewalls können dazu beitragen, dass sich der Grad des Schutzes, den das jeweilige Produkt bietet, leichter einschätzen lässt und Vergleiche zwischen verschiedenen Produkten möglich werden.

Durch den Einsatz verschiedener Produkte, die unabhängig voneinander entwickelt wurden und arbeiten, lässt sich das Sicherheitsniveau steigern. "Monokulturen" sollten vermieden werden, denn wenn ein Angreifer einen bisher unentdeckten Fehler ausnutzt, kann dort leicht der gesamte Schutzwall zusammenbrechen. Bei der Konfiguration einer Firewall folgt man am besten der Regel: "Alles, was nicht ausdrücklich erlaubt ist, ist verboten." Wenn man bei der Definition der Regeln etwas übersehen hat, wird nur die Funktionalität und nicht die Sicherheit eingeschränkt. Während man eine Einschränkung der Funktionalität im Bedarfsfall schnell merkt, bleiben Einbußen in der Sicherheit oft unerkannt.

Es gibt keine 100%ige Sicherheit. Hinzu kommt, dass sich meist im Laufe der Zeit die Stärke der Sicherheit verringert, z. B. durch Entdeckung von Fehlern, Herausbildung neuer Angriffsformen oder auch Verbesserung der Systemausstattung von Angreifern. Unverzichtbar ist es daher, eine ausreichende und fortlaufende Betreuung des eingesetzten Firewall-Systems durch qualifiziertes Personal zu gewährleisten (vgl. auch [CheBel]). Die Administratoren sollten ständig die Diskussion um Sicherheitslücken verfolgen[2] und sich auch weiterbilden. Das Sicherheitsniveau des Firewallsystems ist regelmäßig neu zu bewerten, damit die Systeme auf den aktuellen Stand gebracht werden.

Treten neue Bedrohungen auf, so ist die Kommunikations- und Risikoanalyse entsprechend zu aktualisieren. Eine solche Anpassung ist auch notwendig, wenn beabsichtigt ist, bisher nicht vorgesehene Internetdienste zur Verfügung zu stellen. Die Firewallsoftware ist laufend zu aktualisieren. Falls notwendig, ist das Firewallsystem umzukonfigurieren, oder es sind einzelne Module oder die gesamte Firewall auch außerplanmäßig auszutauschen. Da nicht alle Angriffsversuche auf das lokale Netz von der Firewall vollständig abgeblockt werden können, ist durch die Systemadministration der laufende Betrieb der Firewall zu überwachen. Dazu müssen die Protokolle regelmäßig ausgewertet werden, um auch solche Angriffsversuche zu entdecken, die durch die Firewall nicht abgewiesen werden können. Es ist dafür zu sorgen, dass dringende Warnmeldungen der Firewall der Bedrohungslage angemessen konfiguriert sind. Ferner müssen diese Meldungen das Wartungspersonal unverzüglich erreichen und zeitnah behandelt werden.

Die Firewalladministration kann nicht losgelöst von der Verwaltung des (lokalen) Verwaltungsnetzes gesehen werden. Kommen beispielsweise Benutzerinnen und Benutzer hinzu, scheiden sie aus oder wechseln sie ihr Aufgabengebiet, so kann sich daraus eine Veränderung in den zur Verfügung zu stellenden Diensten ergeben. Dies erfordert eine entsprechende Aktivität der Firewalladministration. Umgekehrt hat die lokale Administration den Schwachstellen im lokalen Netz besondere Aufmerksamkeit zu schenken, die durch Angriffe von außen ausgenutzt werden können. Werden aufgrund der Größe oder Struktur der Verwaltungseinheit auch zwischen verschiedenen Teilen dieser Einheit Firewalls eingesetzt, so können bestimmte Aufgaben der Firewall-Administration sinnvoll zentralisiert werden. Insbesondere zählen dazu diejenigen Tätigkeiten, die unabhängig von der Rechteverwaltung der einzelnen Benutzerinnen und Benutzer sind.

5.3 Rahmenbedingungen für Konfiguration und Betrieb

Sind bereits für die Planung und Einführung eines Firewall-Systems[3] eine Vielzahl von Fragestellungen hinsichtlich technischer, organisatorischer, planerischer und rechtlicher Art zu beachten, kommen während der Betriebsphase weitere Problemkreise hinzu, die durch den Betreiber, ggf. in Abstimmung mit den Benutzern bzw. deren Personalvertretung, zu beantworten sind. Da die in diesem Zusammenhang zu treffenden Maßnahmen teilweise auch auf die Planungs- und Einführungsphase zurückwirken, sollte auch die Betriebsphase der Firewall

2 vgl. Hinweis zum CERT im Abschnitt “Weiterführende Informationen und Literatur”

3 Mit Firewall-System ist nicht nur die Firewall im eigentlichen Sinne, sondern auch das System, das den Zugang zum Internet ermöglicht, gemeint. So sollten auf der Firewall selbst keinerlei Accountingfunktionen laufen. Diese können aber im Zugangssystem integriert sein.

bereits frühzeitig berücksichtigt werden. Die rechtlichen Rahmenbedingungen ergeben sich aus Kapitel 4.

Typische Anforderungen während des Betriebs eines Firewall-Systems sind:

A1 Schutz des ordnungsgemäßen Betriebs der Firewall, d. h. der Durchlässigkeit für zugelassenen Netzverkehr einerseits und der Undurchlässigkeit für nicht zugelassenen Netzverkehr andererseits (eingehend oder ausgehend),
A2 Schutz des internen Netzes vor Angriffen von außen, sowohl bezogen auf online-Angriffe als auch auf offline-Angriffe (z. B. durch eingeschleuste Viren),
A3 Schutz vor einer unzulässigen bzw. rechtswidrigen Nutzung der Firewall, sei es von außen (z. B. Hacking) oder von innen (z. B. unerlaubte private Nutzung oder unzulässiger Zugriff auf für dienstliche Zwecke nicht erforderliche Informationsangebote),
A4 die rechtliche, organisatorische und technische Differenzierung zwischen der dienstlichen und der privaten Nutzung des Internet-Anschlusses, soweit eine außerdienstliche Nutzung überhaupt zugelassen wird,
A5 Abrechnung von Leistungen, die durch die Firewall erbracht werden,
A6 Statistische Auswertungen der Firewall-Benutzung, z. B. zur Angebotsoptimierung.

Um diese Anforderungen umzusetzen, stehen – im Wesentlichen unabhängig von der technischen Entwicklung oder einer rechtlichen Beurteilung – folgende technisch-organisatorische Maßnahmen zur Verfügung:

M1 Gestaltung der Netzzugangspolicy und der Betriebsparameter der Firewall allgemein,
M2 Auswertung der Inhalte übertragener Daten (z. B. hinsichtlich eines potentiellen Virenbefalls),
M3 Auswertung der Verbindungsdaten, insbesondere der URL (z. B. hinsichtlich Datenvolumen, Adressen).

Dabei ergibt sich grundsätzlich folgende Eignungsmatrix für die genannten Maßnahmen, wobei die rechtliche Zulässigkeit der jeweiligen Maßnahme im Einzelfall zu prüfen bleibt:

	A1	A2	A3	A4	A5	A6
M1	x	x	x	x	x	x
M2	-	x	x	x	-	-
M3	x	x	x	-	x	x

5.4 Empfehlungen für den Betrieb einer Firewall

Die nachfolgenden Empfehlungen gelten unabhängig davon, ob öffentliche Stellen selbst die Internet-Dienste anbieten oder ob sie sich dabei eines Providers bedienen.

- Aufgrund der rechtlich unterschiedlichen Bewertung der Datenübertragung für eigene Zwecke der Stelle einerseits und für Dritte andererseits sowie der damit verbundenen praktischen Konsequenzen sollte in einer Dienst- oder Betriebsvereinbarung klar geregelt werden, ob und wenn ja welche Dienste zur privaten Nutzung freigegeben sind.
- Im Hinblick darauf, dass bei behörden- und unternehmensinternen Systemen Mitbestimmungstatbestände erfüllt sind (Verhaltens- und Leistungskontrolle), müssen die Personalvertretungen und Betriebsräte schon bei der Planung und Einführung von Firewallsystemen und insbesondere der Protokollierung beteiligt werden. Gegebenenfalls müssen entsprechende Betriebs- oder Dienstvereinbarungen abgeschlossen werden, in denen das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle verbindlich geregelt wird. Eine Einwilligung der Arbeitnehmer als Grundlage für die Protokollierung der dienstlichen Nutzung ist abzulehnen.
- Bei Datenübertragung für eigene Zwecke der Stelle sind die Mitarbeiter auf die Art und den Umfang technischer Kontrollen hinzuweisen, damit sie ihr Nutzerverhalten entsprechend steuern können; ferner müssen sie darüber informiert werden, welche Folgen es hat, wenn Nachrichten ausgefiltert werden.
- Zur Durchsetzung des Verbots einer privaten Nutzung oder des Zugriffs auf unerwünschte Adressen sollte grundsätzlich auf eine Protokollierung verzichtet werden. Die Durchsetzung dieses Verbots sollte soweit möglich durch die Beschränkung der Zugriffe auf dienstlich erforderliche Angebote (Positivliste) oder über die Sperrung der unerwünschten Adressen versucht werden. Zugriffsversuche auf gesperrte Adressen sollten protokolliert werden. Für erforderliche Protokollierungen sollte in der Dienstvereinbarung ein stufenweises, zunächst nicht personenbezogenes Verfahren festgelegt werden.
- Eine vollständige Protokollierung aller Internetzugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle ist grundsätzlich nicht erforderlich und damit unzulässig.
- Die erlaubte private Nutzung des Internet-Zugangs unterliegt dem Fernmeldegeheimnis nach § 85 TKG. Für die Protokollierung gelten § 6 TDDSG

und § 9 BDSG. Sie darf danach grundsätzlich nur insoweit erfolgen, als es für die Abrechnung der Dienste oder zur Aufrechterhaltung eines regelgerechten Firewallbetriebs unerlässlich ist.

- Die Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe oder Zugriffsversuche, die einen Angriff darstellen, ist im Rahmen von §§ 9, 14 BDSG bzw. der entsprechenden Normen der Landesdatenschutzgesetze zulässig. Darüber hinaus ist eine derartige Protokollierung auch erlaubt, wenn sie zum Erkennen potentieller Angriffe erforderlich ist.
- Für die Protokollierung der Zugriffe von außen auf Informationsangebote für die Öffentlichkeit gelten – in Abhängigkeit von der Art des Dienstes – § 6 TDDSG bzw. § 15 MDStV hinsichtlich der Nutzungs- und Abrechnungsdaten. Der Nutzer muss auf der entsprechenden Web-Site über den Umfang der Protokollierung informiert werden.
- Jede nach den voranstehenden Ausführungen zulässige Protokollierung ist so auszugestalten, dass ein datenschutzrechtlicher Missbrauch vermieden wird, d. h.:
  – der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
  – aufgrund der Datenschutzgesetze (z. B. § 14 Abs. 4 BDSG) dürfen Protokolldaten nicht für andere Zwecke verwendet werden,
  – Protokolle sind durch Zugriffsmaßnahmen gegen unbefugte Kenntnisnahme zu sichern,
  – es sind technisch-organisatorische Auswertungsverfahren festzulegen,
  – es sind möglichst kurze Löschfristen vorzusehen.
- Bei eingehenden Daten, beispielsweise E-Mails, sind, unabhängig davon, ob sie dienstlicher oder privater Natur sind, automatisiert ablaufende zentrale und dezentrale Virenchecks zulässig und angezeigt. Dies gilt auch dann, wenn die Daten im Auftrag verarbeitet werden. Dabei ist zu beachten, dass
  – nur eine automatisierte Kontrolle ohne regelmäßige Kenntnisnahme des Kontrollvorgangs oder -ergebnisses durch Administratoren o. ä. erfolgt,
  – das Inhalts-Scanning auf fest definierte Pattern (Virensignaturen) begrenzt und das Scanning nach frei wählbaren Textstellen ausgeschlossen ist,
  – der Betroffene über das Auffinden von Viren in einer für ihn bestimmten Nachricht unterrichtet wird und mit dieser nur unter seiner Beteiligung oder nach Rücksprache umgegangen wird.
- Private E-Mails der Beschäftigten unterliegen dem Fernmeldegeheimnis. Ihre Kenntnisnahme durch den Arbeitgeber über das für die Erbringung des Dienstes erforderliche Maß ist daher unzulässig.

- Der Einsatz von Programmen zur Auswertung von E-Mails ist wegen des damit verbundenen weitgehenden Eingriffs in das Persönlichkeitsrecht der Beschäftigten nur zulässig, wenn die folgenden drei Voraussetzungen kumulativ gegeben sind:
  – es handelt sich ausschließlich um dienstliche E-Mails,
  – das Vorgehen ist in einer Dienstvereinbarung geregelt,
  – es liegt ein die Auswertung rechtfertigender Ausnahmefall vor.
- Bei Datenübertragung für Dritte sind Inhaltskontrollen nur im Auftrag bzw. mit der Einwilligung des Betroffenen[4] zulässig, wobei dem Auftraggeber (z. B. beim Outsourcing) Gestaltungsmöglichkeiten hinsichtlich folgender Aspekte einzuräumen sind:
  – Nutzung bzw. Umfang der Inhaltskontrolle,
  – technische und organisatorische Folgen bei ausgefilterten Nachrichten.

6. Zusatzmaßnahmen bei der Verarbeitung sensibler Daten

6.1 Sensible Daten

Die steigende Attraktivität des Internet führt in zunehmendem Maße dazu, dass auch solche Bereiche einen Internet-Anschluss erhalten, in denen sensible personenbezogene Daten verarbeitet werden (z. B. Gesundheits- oder Personaldaten). Dies kann entweder im Zuge einer Strategie erfolgen, bei der das Internet als allgemeines Informationsmedium bedarfsunabhängig jedem Mitarbeiter zur Verfügung gestellt wird, oder aber aus einer konkreten Bedarfsermittlung, die etwa im Gesundheitsbereich die Erforderlichkeit einer medizinisch-fachlichen Recherche ergibt.

In diesem Kapitel wird erläutert, inwieweit die in den vorangehenden Kapiteln dargestellten Maßnahmen ausreichen, um auch in solchen Fällen einen datenschutzgerechten Betrieb zu gewährleisten, welche konkreten Risiken bei Betrieb einer Firewall weiterhin bestehen und welche Zusatzmaßnahmen getroffen werden sollten, um diesen Risiken zu begegnen.

6.2 Schutzniveau von Firewalls

Firewalls bieten eine Reihe von Möglichkeiten, um den Datenverkehr in das und aus dem Internet zu kontrollieren und damit das Schutzniveau gegenüber einem direkten Anschluss wesentlich zu erhöhen. Dazu gehören:

4 Bei der zulässigen privaten Nutzung kommt u. U. auch eine generelle Einwilligung durch den Personal- oder Betriebsrat in Betracht. Die Betroffenen sind hierüber ausführlich zu informieren.

- Begrenzung des Zugangs zum Internet auf einen einzigen kontrollierbaren Punkt
- Begrenzung der zugelassenen Dienste auf das Erforderliche
- Begrenzung der Internet-Nutzung auf bestimmte Stationen oder Benutzer
- Verbergen der lokalen IP-Adressen
- Verhindern eines Verbindungsaufbaus aus dem Internet nach innen
- Ausschluss bestimmter Internet-Server oder -Domains
- Ausschluss aktiver Inhalte wie Java oder ActiveX
- Kontrolle auf schädliche Inhalte wie Viren oder Trojanische Pferde
- Protokollierung von Angriffsversuchen

Ein gut konfiguriertes und administriertes Firewall-System kann daher die Gefahren, die beispielsweise durch Trojanische Pferde wie "BackOrifice" oder "NetBus" entstehen, wirkungsvoll begrenzen. Dennoch können auch große und mit erheblichem Aufwand betriebene Firewall-Installationen nicht gegen sämtliche Gefahren aus dem Internet schützen; dies zeigen Vorfälle wie die Verbreitung der E-Mail-Würmer "Iloveyou" oder "Melissa". Diese Ereignisse belegen grundsätzliche Aspekte von Firewalls:

- Jeder Kommunikationskanal, der eröffnet wird, um einen gewünschten Datenaustausch zu ermöglichen, kann auch missbraucht werden. Ein Firewall-System hat im Rahmen des Zugelassenen keine Möglichkeit, zwischen Gebrauch und Missbrauch eines Kommunikationskanals zu unterscheiden. Dies können sich Angreifer zunutze machen.
- Die zunehmende Tendenz, Daten (passive Inhalte) und Programme (aktive Inhalte) zu koppeln, indem Standardanwendungen oder das ganze Betriebssystem skriptfähig gemacht werden, führt zu immer weiteren Schwierigkeiten, den lokalen Betrieb eines PC zu kontrollieren. Neben Makros und Skripten führen auch Browser-basierte Technologien wie Java oder ActiveX immer wieder zu Problemen.
- Virenscanner, zentral oder dezentral, können nur auf bereits bekannte Schadenssoftware reagieren. Bei den rapiden Ausbreitungsgeschwindigkeiten, die das Internet für Schadenssoftware bietet, kommen Updates in der Regel zu spät, um den Schaden wirkungsvoll zu begrenzen.

6.3 Kommunikationsverbindungen als verdeckte Kanäle

Da die Anbindung an das Internet zum Ziel hat, eine Kommunikation mit anderen Rechnern außerhalb des internen Netzes zu ermöglichen, muss selbst eine

sehr restriktiv konfigurierte Firewall eine bestimmte Menge an Datenaustausch zwischen dem internen und dem externen Bereich zulassen. Sowohl der Kommunikationsbedarf als auch die zugrunde liegende Technik des Internet machen es dabei unumgänglich, dass Daten nicht nur in den internen Bereich hineinfließen, sondern auch aus diesem herausgelangen – und sei es nur in Form von Steuerungsinformationen an einen Web-Server.

Dies kann bereits genügen, um einen weitgehenden Angriff auf den geschützten Bereich hinter einer Firewall durchzuführen. So kann etwa das HTTP-Protokoll, das zum Zugriff auf das WWW verwendet wird, missbraucht werden, um – mittels eines entsprechenden Trojanischen Pferdes auf dem betroffenen PC – gespeicherte Daten auf einen Rechner im Internet zu übertragen, ohne dass der Benutzer dies merkt und ohne dass die Firewall dies als unzulässig erkennt. Zwar sind entsprechende Schadprogramme noch nicht öffentlich bekannt geworden, allerdings sind die zugrunde liegenden Konzepte bereits entwickelt und werden in der Sicherheits- und Hackerszene diskutiert. Auch der Kommunikationskanal für E-Mail könnte auf diese Weise missbraucht werden. Die erwähnten E-Mail-Würmer waren – aus Datenschutzsicht – insofern vergleichsweise harmlos, als keine schützenswerten Daten nach außen versandt wurden. Dies hätte jedoch problemlos in die entsprechenden Programme integriert werden können.

Für die Firewall ist diese Kommunikation von normalen, berechtigten Zugriffen durch den Benutzer mittels seines Browsers oder E-Mail-Programms nicht zu unterscheiden. Auch so genannte Intrusion Detection Systeme (IDS), die als Zusatzkomponente von besonders aufwändigen Firewalls den laufenden Betrieb auf Unregelmäßigkeiten hin überwachen, sind kaum in der Lage, eine solche "Nutzung" von der normalen zu unterscheiden (zu IDS siehe http://www.bsi.bund.de/literat/studien/ids/ids-stud.htm).

6.4 Risiken und Maßnahmen im Einzelnen

Das geschilderte Angriffsszenario setzt vier Komponenten voraus:

- eine aktive lokale Komponente, d. h. ein Schadprogramm auf dem betroffenen PC,
- einen Kommunikationskanal, der auf geeignete Weise missbraucht wird,
- einen oder mehrere Kommunikationspartner im externen Netz, d. h. im Internet,
- ein lokales Schadenspotenzial, z. B. in Form gespeicherter personenbezogener Daten.

Dabei müssen alle vier Bestandteile *zur gleichen Zeit* vorliegen. Sofern es gelingt, eine dieser Voraussetzungen zu unterbinden, wird das Risiko eines Datenmissbrauchs erheblich reduziert. Zwar sind prinzipiell auch Angriffe denkbar, die diese Beschränkungen umgehen, z. B. indem die schützenswerten Daten zwischengespeichert werden und damit dauerhaft zugreifbar sind. Dies setzt jedoch eine weitgehende Kenntnis der internen Systemlandschaft voraus, über die ein externer Angreifer in der Regel nicht verfügt.

6.4.1 Beschränkung der aktiven lokalen Komponenten

Die Risiken, von trojanischen Pferden oder anderer Schadsoftware befallen zu werden, sind hinreichend bekannt. Das Internet bildet dabei heute das Hauptverbreitungsmedium, indem entweder ausführbare Programme direkt oder als Bestandteil von Dokumenten (dazu gehören z. B. auch Java-Applets) von dort aktiv oder aber per E-Mail passiv bezogen werden.

Die Schutzmechanismen dagegen sind ebenfalls vergleichsweise gut entwickelt; dazu gehören Virenscanner (zentral und dezentral), Verhindern des Downloads zumindest bestimmter Dateitypen, Begrenzung der lokal ausführbaren Programme auf bekannte Software, lokales Ausschalten von Skript- und Makrokomponenten. Allerdings schränken diese Maßnahmen den Benutzer relativ stark ein und werden daher nach Möglichkeit umgangen. Zudem kann damit in der Regel nur bereits bekannte Schadsoftware kontrolliert werden.

6.4.2 Eingeschränkte Kommunikationskanäle

Die Risiken bestehender Kommunikationskanäle wurden bereits beschrieben. Zunächst einmal sollte die Internetanbindung daher auf die erforderlichen Dienste begrenzt werden; dies ist Bestandteil und Aufgabe jeder Firewall-Installation. Darüber hinaus können die Risiken dadurch begrenzt werden, dass die Kommunikationskanäle nicht dauerhaft zur Verfügung stehen, sondern nur unter bestimmten Bedingungen. Beispielsweise könnte die Verbindung nur für bestimmte Benutzer zugelassen oder sichergestellt werden, dass die Verbindung zu einem Server mit schützenswerten Daten zuvor unterbrochen wurde. Schließlich besteht die Möglichkeit, statt der Standard-Kommunikationskanäle andere, weniger bekannte oder proprietäre Protokolle zu verwenden, die den Aufwand für einen Angriff erhöhen.

6.4.3 Begrenzung der Kommunikationspartner

Wird die Verbindung zu jedem Rechner im Internet sowie von und zu jeder E-Mail-Adresse zugelassen, besteht das Risiko, von jedem Internet-Rechner weltweit attackiert zu werden. In vielen Fällen ist jedoch aus fachlicher Sicht nur ein begrenzter Internetzugang erforderlich. Dabei kann mit einer überschaubaren (und administrierbaren) Liste zugelassener Kommunikationspartner gearbeitet werden. Diese können daraufhin überprüft werden, ob von dort Angriffe zu erwarten sind. Demgegenüber kann auch eine Negativliste implementiert werden, die bekannte oder vermutete Angreifer ausschließt. Dies ist jedoch in der Regel wenig effektiv, da nicht einmal annähernd bekannt ist, von welchen Stellen aus Angriffe stattfinden oder zu erwarten sind. Zudem macht die Dynamik des Internet eine sehr aufwändige Pflege erforderlich.

Zu beachten ist in jedem Fall, dass die Überprüfung auf gute oder schlechte Kommunikationspartner nur dann hilfreich ist, wenn deren Identität zweifelsfrei feststeht. Allerdings lassen sich sowohl E-Mail- als auch IP-Adressen bzw. Domainnamen fälschen. Zudem können Angriffe durchaus auch von bekannten (und ansonsten harmlosen) Kommunikationspartnern ausgehen, wie die Beispiele der E-Mail-Würmer ”Melissa” und ”Iloveyou” zeigen.

6.4.4 Verminderung des lokalen Schadenspotenzials

Der Schaden, der auf Seite des angegriffenen Systems entstehen kann, hängt aus Datenschutzsicht vor allem damit zusammen, welche personenbezogenen Daten von dort aus direkt oder indirekt zugreifbar sind. Maßnahmen sollten daher daran ansetzen, diesen Zugriff zu begrenzen. Dies kann durch die Möglichkeiten des Betriebssystems (Dateirechte) geschehen, durch Verschlüsselung, durch die Vermeidung einer lokalen Datenhaltung, durch eine anwendungsbezogene Authentisierung etc.

6.5 Vorgeschlagene Systemkonfigurationen

Die genannten Einzelmaßnahmen müssen zu sinnvollen Gesamtkonfigurationen zusammengefasst werden. Im Folgenden werden praxiserprobte Lösungen für jeweils unterschiedliche Nutzungsprofile des Internet vorgestellt. Dabei ist teilweise auch eine Kombination der Modelle möglich, um die Sicherheit weiter zu erhöhen.

6.5.1 Proxy mit Positivliste (inhaltliche Begrenzung)

Dieses Konzept ist für solche Benutzer gedacht, die für die Erledigung ihrer fachlichen Aufgaben den Zugriff auf lediglich einen klar definierbaren und überschaubaren Ausschnitt des Internet benötigen, z. B. Arbeitsvermittlungsangebote lokaler oder regionaler Anbieter. Ein solches Nutzungsprofil ermöglicht es, die risikobehafteten Bereiche des Internet pauschal auszublenden, ohne sie im Einzelnen definieren oder bewerten zu müssen. Technisch kann dies durch eine Kontrolle der zugelassenen Internet-Adressen oder Domainnamen auf der Firewall geschehen. Sollen mehrere verschiedene solcher Ausschnitte des Internet verwaltet werden, ist es zweckmäßig, jeweils eigene Proxies vorzusehen, die lediglich dieser Adressfilterung dienen. Dabei ist darauf zu achten, dass die Benutzer dann nur noch über den zugehörigen Proxy und nicht mehr über die Firewall auf das Internet zugreifen können, z. B. indem nur die IP-Adressen der Proxies auf der Firewall eingetragen werden.

Diese Lösung eignet sich auch für solche Fälle, bei denen ein zeitgleicher Zugriff auf personenbezogene Daten und das Internet aus fachlichen Gründen erforderlich ist. Der Mehraufwand liegt in der Erstellung und Pflege der Positivliste sowie in der Beschaffung und dem Betrieb des Proxies.

6.5.2 Umgebungsmodell (zeitliche Begrenzung)

Dieses Konzept kommt für solche Benutzer in Betracht, die einen inhaltlich unbegrenzten Zugang zum Internet benötigen, der jedoch nicht dauerhaft zur Verfügung stehen muss. Die Idee beruht darauf, die Gleichzeitigkeit des Zugriffs auf schützenswerte Daten und auf das Internet (oder auf E-Mail) zu unterbinden. Dadurch kann das Risiko für die schützenswerten Daten deutlich reduziert werden.

Voraussetzung ist ein Betriebssystem wie Windows NT oder UNIX, das eine Authentisierung des Benutzers voraussetzt und mittels dieser Identität Zugriffsrechte an Objekten verwalten kann. Mit dieser Technik ist es möglich, für jeden Realbenutzer zwei Konten einzurichten, wovon eines ausschließlich für den Zugriff auf schützenswerte Daten dient, das andere ausschließlich für den Internet-Zugang. Dazu müssen für das Internetkonto sämtliche Zugriffsrechte auf die schützenswerten Daten entzogen werden. Zudem muss für das andere Konto der Kommunikationskanal ins Internet unterbunden werden. Dazu reicht es allerdings nicht aus, dem Benutzer in dieser Umgebung keinen Browser o. ä. zur Verfügung zu stellen. Vielmehr ist an zentraler Stelle eine benutzerbezogene Kon-

trolle des Internetzugangs vorzusehen. Dies kann durch geeignete Firewalls oder durch vorgelagerte Proxies, die die Benutzeridentität überprüfen, erzielt werden (z. B. MS Proxy Server).

Für die Benutzer bedeutet dies, dass sie sich jeweils auf Betriebssystem-Ebene ummelden müssen. Dies stellt zwar einen Mehraufwand dar, der jedoch bei der Nutzung des Internet nicht allzu sehr ins Gewicht fallen dürfte. Für die E-Mail-Nutzung, die in der Regel sowohl umfangreicher als auch zeitkritischer ist, kann sich jedoch eine andere Einschätzung ergeben.

6.5.3 Grafischer Internetzugang (logische Systemtrennung)

Diese Lösung ist für solche Benutzer geeignet, die eine weder inhaltlich noch zeitlich begrenzbare Internet-Nutzung benötigen. Die Idee beruht darauf, den PC lediglich als Fenster ins Internet zu nutzen. Per Terminal-Emulation wird auf einen Browser oder ein E-Mail-System auf einem anderen Gerät (Terminal-Server) zugegriffen, auf dem keine schützenswerten Daten verarbeitet werden. Nur der Terminal-Server benötigt einen Internet-Zugang, während der Arbeitsplatz-PC, obwohl in das interne Netz integriert, keinen direkten Kontakt zum Internet oder zur Firewall benötigt. Schadsoftware kann daher nur an dem Terminal-Server ansetzen, wovon jedoch keine schützenswerten Daten betroffen sind. Beispielprodukte sind VNC (www.uk.research.att.com/vnc) oder der Windows Terminal Server unter Windows NT und 2000.

Der Mehraufwand für diese Lösung besteht zum einen in dem zusätzlichen Gerät für den Internet-Zugang und zum anderen in der erhöhten Netzlast und Reaktionszeit, die die Übertragung der Bildschirminhalte zwischen Terminal-Server und Arbeitsplatz-PC mit sich bringt. Zudem kann der Benutzer heruntergeladene Dokumente oder empfangene E-Mail zwar öffnen und betrachten sowie gegebenenfalls drucken, jedoch nicht auf seinen eigenen PC übertragen. Dies erfordert einen Austausch über Datenträger oder andere gesicherte Wege.

Prinzipiell kann auf diesem Weg auch Schadsoftware importiert werden, die sich anschließend sowohl den Kommunikationskanal für die Terminalverbindung als auch den Kommunikationskanal für die Internet-Verbindung zunutze macht. Hierzu müssten allerdings lokale Komponenten auf dem Internet-Gerät und auf dem Terminal-PC installiert sowie das verwendete Protokoll für die Terminalverbindung missbraucht werden. Dies stellt eine erheblich höhere Hürde für einen Angreifer dar, insbesondere wenn die interne Systemkonfiguration nicht bekannt ist.

6.5.4 Stand-alone-System (physikalische Systemtrennung)

Diese rigideste Lösung ist für all die Fälle geeignet, in denen die verbleibenden Restrisiken der vorgenannten Modelle als zu hoch eingeschätzt werden. Eine vollständige Systemtrennung zwischen Internet und der Verarbeitung schützenswerter Daten schützt die Vertraulichkeit dieser Daten optimal. Allerdings ist der Aufwand sowohl finanzieller als auch organisatorischer Art unter Umständen erheblich. Bei einer nur sporadischen Internet-Nutzung genügt ein einzelner Internet-PC für mehrere Mitarbeiter. Eine extensive Nutzung setzt jedoch jeweils ein Zweitgerät am Arbeitsplatz voraus. Zu beachten ist dabei, dass auch bei einer vollständigen systemischen Trennung durch verschiedene Geräte bzw. Netze häufig gleichwohl der Bedarf besteht, Daten zwischen diesen Bereichen auszutauschen, z. B. ein Dokument, das im geschützten Netz erstellt wurde, per E-Mail zu versenden. Dies kann per Datenträger (Diskette o. ä.) geschehen. Auf diesem Weg kann zwar Schadsoftware importiert werden, diese kann jedoch ausschließlich Effekte im lokalen Bereich erzielen.

7 Ausblick

In der Vergangenheit war das Design und die Weiterentwicklung der TCP/IP-Protokollfamilie nicht an Zielen wie IT-Sicherheit oder Datenschutz ausgerichtet; lediglich die Ausfallsicherheit von Netzwerken ist als Designkriterium erkennbar und durchgehalten. Inzwischen werden in den einschlägigen RFCs jedoch eine Reihe von sicherheitsrelevanten Problemen behandelt. Um die Dynamik dieses Prozesses zu verdeutlichen, sei hier auf eine zentrale und für die Entwicklung der Firewallsysteme besonders bedeutsame Neuerung hingewiesen, nämlich die Sicherheitsmerkmale (IPSec) der IP-Version 6 (IPv6). Sie sollen eine konsistente Lösung einer Reihe von Sicherheitsproblemen mit IPv4 ermöglichen, siehe auch [BonWol].

IPSec wird die wesentlichen Dienste Authentifikation und Vertraulichkeitssicherung implementieren. So wird auch ein Modus zur Vertraulichkeitssicherung verfügbar sein, bei dem komplette IP-Pakete verschlüsselt und mit einem neuen IP-Header versehen werden (sog. tunnel mode). Wird ein solches Verfahren in einem Gateway oder einer Firewall implementiert, so kann dadurch nicht nur der unbefugte Zugriff auf die Inhalte der Datagramme vermieden, sondern auch die Verkehrsflussanalyse erschwert werden. Denn die IP-Pakete tragen lediglich

die Absenderadresse des Gateways oder der Firewall, und aus dem Inhalt der Datagramme kann auch kein Rückschluss gezogen werden. Verbindungen dieser Art zwischen Firewalls eignen sich zur Kopplung von LANs eines VPN. Die Migration zu einer solchen Lösung gestaltet sich problemlos, da keine weiteren (insbesondere konzeptionellen) Änderungen nötig sind.

Sollen jedoch andere Szenarien als diese Art von VPN realisiert werden, sind weitere Probleme zu lösen. Zum einen ist eine Schlüsselverwaltung notwendig, die den Zugriff auf Authentifikationsschlüssel bisher unbekannter Partner ermöglicht. Eine solche Infrastruktur ist jedoch kein originäres Problem von IPSec, sondern wird in gleicher Weise für die Sicherung der Zurechenbarkeit etwa von elektronischer Post oder von HTTP-Verbindungsinhalten benötigt. Darüber hinaus lassen sich IP-Datagramme im tunnel mode auch durch eine Firewall senden, ohne dass diese die Datagramme in der bisher üblichen Weise analysieren kann. Hier stellt sich die Frage, ob man der Firewall erlauben sollte, die Pakete mitzulesen und ihr das Schlüsselmaterial zur Verfügung zu stellen oder nicht. Die erste Alternative erfordert ein hohes Maß an Hostsicherheit, stellt dafür aber eine echte, gegen Abhören auf dem gesamten Transportweg kryptographisch gesicherte Ende-zu-Ende-Verbindung dar. Im zweiten Fall bestehen an den beteiligten Firewalls Abhörmöglichkeiten, dafür kann die Firewall aber bestimmte Angriffe abwehren, die sonst erst beim Host erkennbar und behandelbar sind.

Neben den Protokollneuerungen im Rahmen der Version 6 des Internet Protocol sind noch weitere Änderungen zu erwarten. Das betrifft Fragen, die sich aus Protokollerweiterungen für mobile Teilnehmer ergeben, ebenso wie Probleme im Zusammenhang mit der Sicherung von Hochgeschwindigkeitsverbindungen.

Festzuhalten bleibt, dass der Anschluss von Netzen der öffentlichen Verwaltung an das Internet nur dann das Attribut datenschutzgerecht verdient, wenn auf die sicherheitsrelevanten Entwicklungen auf dem Gebiet von Internet-Protokollen und -Werkzeugen bis hin zur Endgerätesicherheit zeitnah und adäquat reagiert wird.

8 Anhang

8.1 Weiterführende Informationen und Literatur

8.1.1 Fundstellen im WWW

Allgemeine Informationen und Verweise finden sich unter:
http://www.datenschutz.de

Hamburger Datenschutzhefte -
Datenschutz bei Multimedia und Telekommunikation
http://www.hamburg.de/Behoerden/HmbDSB/Material/hamdat.htm

Landesbeauftragter für den Datenschutz Schleswig-Holstein: Die wichtigsten Bestimmungen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) und des Mediendienstestaatsvertrages (MDStV)
http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/multimed/index.htm

Materialien des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:
- Arbeitspapier Datenschutzfreundliche Technologien - Privacy Enhancing Technology PET
http://www.datenschutz-berlin.de/to/datenfr.htm

- Arbeitspapier Datenschutzfreundliche Technologien in der Telekommunikation:
http://www.datenschutz-berlin.de/to/tk/ds_tk123.htm

Ergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
http://www.datenschutz-berlin.de/doc/de/konf/index.htm

Die Adressen der Landesbeauftragten für den Datenschutz:
http://www.datenschutz-berlin.de/sonstige/behoerde/ldbauf.htm

Die Adressen der Aufsichtsbehörden für den Datenschutz
http://www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm

Gesetze und datenschutzrechtliche Regelungen auf Bundesebene:
http://datenschutz-berlin.de/recht/de/rv/index.htm

– **Telekommunikationsgesetz:**
http://www.datenschutz-berlin.de/recht/de/rv/tk_med/tkg_de1.htm

– **Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)** (Art.1: Teledienstegesetz, Art. 2 Teledienstedatenschutzgesetz, Artikel 3 Signaturgesetz und weitere Artikel)
http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_de.htm

Mediendienste-Staatsvertrag:
http://www.datenschutz-berlin.de/ recht/de/stv/mdstv.htm
Das **CERT** (Computer Emergency Response Team) warnt vor neuen Angriffstechniken aus dem Internet und gibt Ratschläge für Sicherheitsmaßnahmen. CERT-Warnings erscheinen unregelmäßig in der Newsgroup comp.security.announce. Das deutsche CERT ist unter der folgenden Adresse zu erreichen:

DFN-CERT, Universität Hamburg, FB Informatik,
Vogt-Kölln-Str. 30, D-22527 Hamburg
Telefon: 040/5494-2262, Telefax: 040/5494-2241
E-Mail: dfncert@cert.dfn.de (für Mitteilungen, die konkrete Vorfälle oder Sicherheitslücken betreffen) oder info@cert.dfn.de (für sonstige Anfragen oder Kommentare),
WWW: http://www.cert.dfn.de

Technische Informationen zum Internet:
http://www.geocities.com/CollegePark/Quad/6450/menu.htm

8.1.2 Broschüren

Folgende Publikationen können beim Bundesbeauftragten für den Datenschutz[5] angefordert werden:
– Bundesdatenschutzgesetz (BfD - Info 1)
enthält u. a. das Bundesdatenschutzgesetz und Erläuterungen
– Der Bürger und seine Daten (BfD - Info 2)

[5] Der Bundesbeauftragte für den Datenschutz; Postfach 200112; 53131 Bonn; Tel.: 0228/81335-0; Fax: -50; E-Mail: poststelle@bfd.bund400.de

– Schutz der Sozialdaten (BfD - Info 3)
– Der behördliche Datenschutzbeauftragte (BfD - Info 4)
– Datenschutz und Telekommunikation (BfD - Info 5)
enthält u. a. das Telekommunikationsgesetz, TDSV, Auszüge aus dem IuKDG (Teledienstgesetz - TDG - und Teledienstedatenschutzgesetz – TDDSG -)

8.1.3 Literatur

[AKT-DFT] Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern – Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien (allgemein und in der Telekommunikation), Schwerin, 1998

[ArsRie] Arslan, Ahmet; Riekert, Wolf-Fritz: Sicherheit für Benutzer der Internet-Technologie, Studie des Forschungsinstituts für anwendungsorientierte Wissensverarbeitung (FAW) Ulm im Auftrag des Landes Baden-Württemberg, Ulm, 1997 – http://www.david-datenschutz.de/secinternet.html

[BonWol] Bonnard, Andreas; Wolff, Christian: Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall, München, 1997 – http://www.bsi.bund.de/literat/studien/fw-stud.pdf

[BSI] Bundesamt für Sicherheit in der Informationstechnik (Hg.): Sicherheit im Internet. – Bonn, 1997. – http://www.bsi.bund.de/literat/faltbl/015_netz.htm

[ChaZwi] Chapman, D. Brent; Zwickey, Elizabeth D.: Einrichten von Internet Firewalls, Bonn, 1996

[CheBel] Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet - Schutz vernetzter Systeme vor cleveren Hackern, Bonn, Paris, 1996

[HamDa] Der Hamburgische Datenschutzbeauftragte/Datenschutzbeauftragter des debis Systemhaus: Hamburger Datenschutzhefte – Datenschutz bei Multimedia und Telekommunikation; Hamburg, 1998

[MV-TuD] Der Landesbeauftragte für den Datenschutz Mecklenburg Vorpommern: Technik und Datenschutz, Schwerin, 1996 http://www.tec.informatik.uni-rostock.de/RA/LfD-MV/ak_tech/tud/index_td.html

[Nds] Der Landesbeauftragte für den Datenschutz Niedersachsen: Checkliste Grundschutz durch Firewalls, Hannover, 1998 – http://www.lfd.niedersachsen.de/dokumente/firewall.pdf

[Poh] Pohlmann, Norbert: Firewall-Systeme – Sicherheit für Internet und Intranet, Bonn, 1997

[Ran] Ranum, Marcus J.: Thinking About Firewalls, Proceedings of Second International Conference on System and Network Security, Washington DC, 1993, V2.0 ("Beyond Perimeter Security") – http://www.clark.net/pub/mjr/pubs/think/

[RanCur] Ranum, Marcus J.; Curtin, Matt: Internet Firewalls Frequently Asked Questions, 26.05.1998 – http://www.clark.net/pub/mjr/pubs/fwfaq/ oder http://www.interhack.net/pubs/fwfaq/

[TelMedR] Telekommunikations- und Multimediarecht; Becktexte im DTV, München, 1998

8.2 Abbildungsverzeichnis

Abbildung 2.1: Direktanschluss eines Rechners an das Internet

Abbildung 2.2: Zentrale Kopplung eines lokalen Netzes an das Internet

Abbildung 2.3: Dezentraler Anschluss eines lokal vernetzten Rechners an das Internet

Abbildung 3.1: Zentrale Firewall-Anordnung

Abbildung 3.2: Gestaffelte Firewall-Anordnung

Abbildung 3.3: Kaskadierte Firewall-Anordnung mit DMZ

Abbildung 3.4: Screened Gateway (Sandwich-System)

Abbildung 3.5: Screened Gateway (Sandwich-System) mit DMZ

Abbildung 4.1: Protokollierung von Internetzugriffen

8.3 Abkürzungsverzeichnis

ARP	Address Resolution Protocol
BDSG	Bundesdatenschutzgesetz
CGI	Common Gateway Interface
DMZ	Demilitarisierte Zone
DNS	Dynamic Name Service
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocols
IP	Internet Protocol
MDStV	Mediendienste-Staatsvertrag
NFS	Network File System
SSH	secure shell
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
WWW	Word wide Web

8.4 Wichtige Dienste und Begriffe[6]

Das Internet ist ein weltumspannender Zusammenschluss vieler lokaler Computernetze. Die Zahl der Benutzerinnen und Benutzer wurde Anfang 1998 auf etwa 100 Millionen geschätzt. Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten.

Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde. Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u. a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine

6 Mit freundlicher Genehmigung der Autorin aus http://www.klick.link-m.de/hilfe/glossar entnommen, überarbeitet und ergänzt.

Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adressinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Im folgenden werden einige Termini und Dienste des Internet sowie weitere Begriffe der Datenfernübertragung (DFÜ) erklärt.

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

Archie Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf ⇨ FTP-Servern. Der Zugriff erfolgt über ⇨ Telnet, ⇨ E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

Attachment Heute kann man an ⇨ E-Mails Dateien (z. B. ein Winword-Dokument) anhängen und gemeinsam verschicken. Diese Anlagen werden Attachments genannt.

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

Browser Ein Browser ist das Programm, mit dem man durch das ⇨ WWW surfen kann. Ein Browser ist notwendig, um WWW-Seiten überhaupt anschauen zu können (siehe auch ⇨ HTML).

Cookies Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers

auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Vor allem Firmen benützen Cookies, um Kundenprofile zu erstellen oder ein persönliches Angebot zusammenstellen zu können. Man kann einstellen, ob der Browser Cookies akzeptieren darf: InternetExplorer 4.0: Menü Ansicht/Optionen/ Erweitert, Netscape 4.0: Menü Bearbeiten/Einstellungen/Erweitert.

DFÜ DFÜ (Abk. für Datenfernübertragung) ist der Sammelbegriff für alles, was elektronische Kommunikation beinhaltet, besonders verbreitet im Mailboxbereich.

Domain Eine Domain ist eine weltweit erreichbare Adresse, die von Computern im Internet gebraucht wird, um Nachrichten automatisch zustellen zu können. Rhein-main.de, spiegel.de oder aol.com sind z. B. eine Domain, siehe auch ⇨ Username.

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

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

Emoticons auch Smileys genannt, mit ihnen werden Stimmungen in Texten (z. B. in mail und news) ausgedrückt (z. B.: **:-)** lächeln; **;-)** verschmitzt lächeln; **:-(** traurig)

FAQ FAQs (Abk. für Frequently Asked Questions) sind sehr hilfreiche Texte, die für Neueinsteigerinnen und Neueinsteiger empfehlenswert sind und verhindern sollen, dass immer dieselben Fragen gestellt werden.

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

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

Gate(way) Ein Gateway ist ein Computer, der den Übergang von einem Netz zu dem anderen (z. B. von dem Internet zu einem Mailboxnetz) darstellt. Gateways sind notwendig, da die verschiedenen Netze mit unterschiedlichen technischen Sprachen (⇨ Protokollen) arbeiten.

Gopher Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (⇨ FTP, ⇨ Telnet, ⇨ WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im ⇨ WWW integriert.

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

HTML HTML (Abk. für Hypertext Markup Language) ist die Sprache, in der Webseiten geschrieben werden. Erst der ⇨ Browser ermöglicht eine grafische Umsetzung der HTML Befehle. Das Besondere von HTML sind die universelle Einsetzbarkeit für alle Arten von Computern und die Verweise, sog. ⇨ Links.

HTTP HTTP (Abk. für Hypertext Transport Protokol) ist quasi die technische Grundlage für das WWW. Dem Computer wird mitgeteilt, dass die Daten aus HTML-Code bestehen, deswegen beginnen WWW Adressen mit http:// Bei neueren Browsern funktioniert das Ansehen von Webseiten allerdings auch, wenn man http:// weglässt.

Hypertext Hypertext wird ein Text genannt, der interaktive Verweise (⇨ Links) beinhaltet.

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

ISDN ISDN ist eine Telefon(leitungs)-Technik. Herkömmliche Telefonleitungen funktionieren analog, d. h. übertragen Töne. ISDN hingegen funktioniert – wie der Computer – digital und überträgt also 0 und 1. ISDN bedeutet vor allem auch dadurch eine Geschwindigkeitsverbesserung. Ein ISDN-Anschluss beinhaltet 3 bis 10 Rufnummern und 2 Leitungen, was den Nebeneffekt hat, dass man während des Surfens auch telefonieren kann.

IP-Adresse, IP-Nummer IP-Adressen sind Zahlenkombinationen, z. B. 195.35.6.214. Diese Zahlenkombinationen sind die Adresse des Computers. Jeder Computer hat sowohl eine Adresse aus Wörtern (siehe

Domain) als auch eine IP-Adresse. Die IP-Adresse wird von den Computern benutzt, die Namen sind für die Menschen leichter zu merken.

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

Mailbox

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

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

Metasearch Metasearch nennt man eine Suche, die in mehreren Katalogen und Datenbanken unterschiedlicher Suchmaschinen gleichzeitig erfolgt, bzw. eine Suchmaschine, die anbietet, auf einfache Art und Weise dieselbe Suche auf beliebigen Suchmaschinen durchzuführen.

Netcall Netcall nennt man sowohl den Datenaustausch von ⇨ Mailboxen untereinander, als auch das Anrufen und Nachrichtenabgleichen eines ⇨ Points bei der ⇨ Mailbox.

Netikette Die Netikette ist die Menge der Umgangsregeln für das Internet und die anderen Netze.

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

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

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

PGP Pretty Good Privacy, ein Verschlüsselungsprogramm für ⇨ E-Mails. Das Programm kann sowohl elektronische Unterschriften leisten als auch E-Mails sicher verschlüsseln.

Point Ein Point ist ein Programm, dass sich in die ⇨ Mailbox (2.) einwählt und automatisch die neuen Nachrichten empfängt und versendet, so dass man die Nachrichten in Ruhe daheim schreiben kann, ohne bestehende Telefonverbindung (⇨ offline).

PoP PoP (Abk. für Point of Presence), gleichbedeutend mit Provider bzw. Einwahlknoten.

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

PPP (Point to Point Protocol) PPP ist notwendig, um sich von Zuhause über Modem und Telefonleitung ins Internet einzuwählen. Die meisten Betriebssysteme und Provider unterstützen dieses Protokoll.

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

Provider Ein Provider ist ein Internetanbieter. Er ermöglicht Privatpersonen/Firmen Zugang zum Internet.

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

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

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

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

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

Usenet-News Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (⇨ Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zurzeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Username Name, der jeder Benutzerin und jedem Benutzer zugewiesen wird, z. B. nora.b, danach kommt immer ein @und der Name der Mailbox oder des Heimatrechners (also des Providers z. B.) und danach die Domain (die Internetadresse des Rechners). Im Gesamten also nora.b@ipn-b.de[7] Der Teil der Adresse nach dem @kann unterschiedlich lang sein und hängt von dem Heimatrechner bzw. Provider ab.

Wais WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit ⇨ Telnet, ⇨ E-Mail, einem eigenen WAIS-Client oder über ⇨ WWW durchgeführt werden.

---

7 Dies ist die E-Mail-Adresse der Autorin des Original-Glossars.

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

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

Weitere Glossare:
`http://www.geocities.com/CollegePark/Quad/6450/menu.htm`

Teil 2

Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“

erstellt vom Arbeitskreis "Technik” der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder

Stand: August 2000

In der Arbeitsgruppe haben mitgewirkt:
Ursula Meyer zu Natrup (Berliner Datenschutzbeauftragter),
Walter Ernestus (Bundesbeauftragter für den Datenschutz)

1. Einleitung

In den letzten Jahren hat sich die Informationstechnologie sehr schnell weiterentwickelt. Dies gilt insbesondere im Bereich der Vernetzung und der offenen Kommunikationssysteme. Die verstärkte Nutzung neuer Kommunikationsformen, beispielsweise E-Mail, erfordert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisse eingesetzt. Da auf die Informationen in diesen Verzeichnissen von verschiedenen Stellen aus direkt zugegriffen werden kann und insbesondere beliebige Informationen gespeichert werden können, geht die Funktionalität weit über die bisherigen Möglichkeiten eines in Papierform vorliegenden Adress- und Telefonverzeichnisses hinaus. Hieraus ergibt sich die Notwendigkeit, dass von der datenverarbeitenden Stelle festgelegt werden muss, welche Daten im Verzeichnis gespeichert werden.

Zum Einsatz kommen sowohl ISO-konforme (X.500) Systeme als auch Industriestandards (z. B. Network Directory System, NDS). Da in einem Verzeichnisdienst auch personenbezogene Daten gespeichert werden können, ist die Betrachtung datenschutzrechtlicher Aspekte notwendig. Im Verzeichnisdienst existieren verschiedene datenschutzrechtliche Probleme. Diese betreffen zum einen technische Aspekte, wie die sichere Übertragung personenbezogener Daten, zum anderen rechtliche Aspekte, wie Inhalt, Form und Zugriff auf Einträge. Im Vordergrund steht dabei, dass schutzwürdige Belange der verzeichneten Personen nicht beeinträchtigt werden.

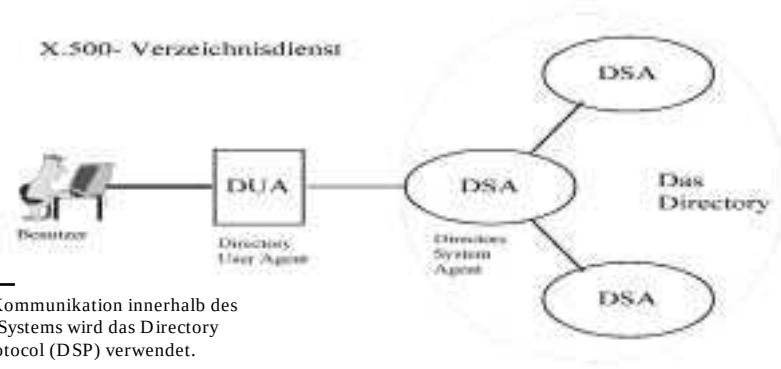
Diese Empfehlung befasst sich mit den Möglichkeiten des datenschutzgerechten Einsatzes von Verzeichnisdiensten. Sie basiert auf dem Betrieb eines Verzeichnisdienstes in einer definierten **Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung**. Die intranetübergreifende Verbindung mehrerer Verzeichnisse, z. B. über das Internet, wird nicht betrachtet. Des Weiteren wird die generelle Problematik der Systemverwaltung der beteiligten Rechnersysteme auch nicht mit einbezogen, da diese unabhängig von Verzeichnisdiensten sind.

2. Verzeichnisdienste

2.1 Verzeichnisdienst X.500

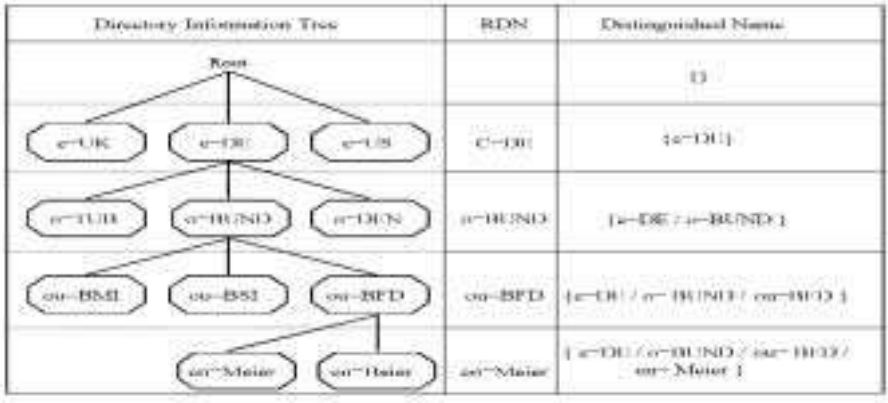
X.500 (ISO-9594) ist ein von der Comité Consultatif International Télégraphique et Téléphonique (CCITT) und der International Standardization Organization (ISO) erarbeiteter Standard, der einen global verteilten Verzeichnisdienst **– den Verzeichnisdienst –** beschreibt. Er kann als ein in vielen Aspekten erweitertes elektronisches Telefonbuch, das neben Telefonnummern auch andere Kommunikationsadressen, z. B. E-Mail-Adressen, enthält, betrachtet werden. Darüber hinaus können relativ beliebige Informationen über Organisationen, deren Mitarbeiter, Rechner, Peripheriegeräte und verfügbare Dienste, also das gesamte Spektrum aller im Kontext von vernetzten Computer- und Kommunikationssystemen vorkommenden Elementen, enthalten sein.

Die Benutzer des Directory-Systems können sowohl menschliche Benutzer als auch Anwendungsprogramme sein. Bei der Interaktion mit dem Directory greift der Benutzer über einen *Directory User Agent* (DUA) auf die Directory-Informationen zu. Dabei sieht die Verzeichnisnorm das *Directory Access Protocol* (DAP) als Zugangsprotokoll vor. Aufgrund der Komplexität hat sich dieses allerdings am Markt nicht durchgesetzt, sondern wurde teilweise (insbesondere in den Endgeräten) durch das **Lightweight Directory Access Protocol** (LDAP) als stark vereinfachtes Zugriffsprotokoll ersetzt. Das Directory besteht aus mehreren kooperierenden *Directory System Agents* (DSA), die auf verschiedenen Rechnern realisiert sein können[1].



1 Für die Kommunikation innerhalb des Directory-Systems wird das Directory System Protocol (DSP) verwendet.

Die Informationen, die das Verzeichnis bereitstellt, sind physikalisch über die DSAs verteilt, erscheinen jedoch für den Benutzer als eine logische Datenbasis. Die Gesamtheit aller Informationen über Objekte, die im Verzeichnis bekannt sind, wird als *Directory Information Base* (DIB) bezeichnet. Jedes Objekt wird darin durch einen Verzeichnis-Eintrag repräsentiert, der die für das Objekt relevanten Daten enthält. Die Einträge der Datenbasis sind hierarchisch angeordnet. Die logische Sicht auf die Datenbasis erscheint als Baumstruktur[2]. Diese Baumstruktur bildet die Grundlage einer eindeutigen Namensgebung innerhalb des Verzeichnisses. Die Namen der Einträge werden gemäß einer mehrstufigen hierarchischen Namenskonvention gebildet. Ein Directory-Name (Distinguished Name - DN) setzt sich aus einer geordneten Folge einzelner Komponenten (Relative Distinguished Name - RDN) zusammen.



Die Namen von Einträgen der DIB sind eindeutig, d. h., jeder Name bezeichnet genau ein Objekt. Dieses wird dadurch erreicht, dass jede Namensgeberautorität (naming authority) innerhalb einer Hierarchiestufe unterschiedliche RDNs verwendet. Jeder Eintrag im Directory besteht aus mehreren Informationen (Attributen). Ein Attribut wird durch einen Attributtyp und einen bzw. mehrere Attributwerte definiert. Ein Beispiel hierfür ist ein Personeneintrag, der folgendes Aussehen haben könnte:

2 Die Directory Information Base stellt sich somit als Directory Information Tree (DIT) dar.

Name des Eintrags (DN): {c=DE / o=Berliner Datenschutzbeauftragter / ou=Bereich Informatik und Organisation / cn=Meyer}

Attributtyp	Attributwert(e)
Name	Mustermann
Nachname	Mustermann
Postanschrift	Musterstr, 1000 Musterstadt
Telefonnummer	+49 30 12345678 +49 30 11223344
Faxnummer	+49 30 9999999
Email	mzn@muster.de
favourite drink	Sekt extra dry

Die im Verzeichnis gespeicherten Daten müssen gegen unautorisierten Zugriff geschützt werden. Hierzu wurde in der Norm X.509 die Sicherung der im Verzeichnis durchgeführten Kommunikation beschrieben. Die dargestellten Verfahren unterscheiden zwischen schwacher und starker Authentifizierung. Die schwache Authentifizierungsprozedur basiert auf dem eindeutigen Namen (DN) und einem Passwort. Die starke Authentifizierung arbeitet mit einem asymmetrischen Kryptosystem (z. B. dem RSA-Algorithmus).

Für die Zugriffskontrolle existiert ein generelles Zugriffskontroll-Modell, das die Anwendung einer bestimmten Sicherheitspolitik (security policy), die jedoch nicht durch das Verzeichnis vorgeschrieben wird, erlaubt. Als Basis wird ein Zugriffskontroll-Schema definiert, das auf Zugriffskontroll-Listen (Access Control Lists, ACL) basiert. Über die Zugriffskontroll-Listen wird festgelegt, wer auf welche Daten in einem Eintrag in welcher Weise (beispielsweise lesend, schreibend) zugreifen kann. Die Normung des Zugriffskontrollmechanismus erfolgte im X.500-Standard erst 1993.

2.2 Network Directory System (NDS)

Das Network Directory System (NDS) ist ein von Novell entwickelter Verzeichnisdienst. Es wurde als verteilte Datenbank konzipiert und ist für die Verwaltung von Netzwerken geeignet. NDS verwaltet Informationen über alle Komponenten im Netzwerk, z. B. Benutzer, Benutzergruppen und Drucker. Ein NDS-Objekt besteht aus einer Vielzahl von Informationen – Properties genannt – und den dazugehörenden Daten, die diese Properties haben können. Es existieren Objekte, mit deren Hilfe eine Baumstruktur ähnlich wie bei X.500 aufgebaut werden kann. Für jedes Objekt können Zugriffsberechtigungen vergeben werden. Dieses wird über Access Control Lists realisiert. Die Funktionalität von

NDS umfasst weniger die Bereitstellung der Telefonbuch-Funktionalität, sondern eher die Verwaltung von allen Objekten in großen Netzwerken.

2.3 Domain Name System (DNS)

Der Verzeichnisdienst wird im Internet zur Auflösung von logischen Rechnernamen auf IP-Adressen verwendet. Für die weiteren datenschutzrechtlichen Betrachtungen spielt DNS keine Rolle, wenn keine Personennamen, Standorte etc. in Zusatzfeldern (txt, ggf. HINFO) des DNS verwaltet werden. Ist dies der Fall, sind die typischen Probleme der anderen genannten Verzeichnisdienste nicht zu erwarten; deshalb wird DNS im Weiteren nicht besonders betrachtet. Gleichwohl ist die Sicherheit dieses Dienstes für eine korrekte Funktion von IP-Infrastrukturen bedeutsam. Die Korrektheit kommt allerdings auch ohne Personenbezug aus.

3. Komponenten und Beteiligte

Ein Verzeichnisdienst stellt in der Regel nur eine Unterstützungsfunktion innerhalb eines anderen Verfahrens oder Dienstes bereit, beispielsweise liefert er Kommunikationsadressen, Telefonnummern und öffentliche Schlüssel bei der Telekommunikation. Allerdings sind auch Lösungen vorstellbar, in denen die Verzeichnisdienste die Verwaltung und Organisation von anderen Datenbeständen übernehmen. In der Regel werden heute Verzeichnisdienste zur Verwaltung der Objekte in großen Netzwerken (Intranet) eingesetzt (Administration). In beiden Fällen werden für den Betrieb des Dienstes gewisse Grundkomponenten – ein Übertragungsnetz, Knotenrechner, eine verteilte Datenbank etc. – benötigt. Auch treten in allen Fällen die gleichen Beteiligten auf, die entweder den Betrieb des Verzeichnisses sicherstellen oder als Betroffener mitwirken.

4. Datenschutzaspekte von Verzeichnisdiensten

In Verzeichnisdiensten wird der eindeutige Teilnehmername (Distinguished Name, DN) definiert. Dieser Name dient als Adresse im Verzeichnis, mit der Personen gefunden werden können. Um das Verzeichnis in einer benutzerfreundlichen Weise zu organisieren, wird zur Identifizierung eine Kette von Namen und Namensteilen verlangt. Dies führt dazu, dass eine Person eindeutig identifiziert werden kann. In Verbindung mit der Möglichkeit, beliebige Informationen zu einer Person zu speichern, erwachsen hieraus besondere datenschutzrechtliche Gefahren. Hierbei ist insbesondere die einfache Zusammenführung bisher getrennt gespeicherter Daten zu sehen. Die Verbindung von verteilt vorliegenden Informationen und eventuell existierender Kopien (Repliken) kann zu Problemen hinsichtlich der Aktualität der Daten führen[3]. Dies stellt insbesondere für die datenschutzrechtlichen Anforderungen bei der Berichtigung und Löschung ein Problem dar. Darüber hinaus bieten sich zudem noch Verknüpfungsmöglichkeiten mit anderen elektronisch vorliegenden Daten, z. B. Telefonbuch auf CD-ROM, Adressbuch auf CD-ROM etc. Dieses ermöglicht die Erstellung von sehr detaillierten Profilen, deren Umfang nicht absehbar ist.

Üblicherweise wird der Verzeichnisdienst als Unterstützungsfunktion in bestehende Verfahren integriert. Damit muss sichergestellt sein, dass der Zugriff auf Informationen in Einträgen nur auf das für die Aufgabenerledigung Notwendige beschränkt wird.

Gefahren für das informationelle Selbstbestimmungsrecht erwachsen auch aus dem komplexen Zusammenspiel der verschiedenen Komponenten, die für den Betrieb des Verzeichnisdienstes benötigt werden. Jede Komponente für sich ist dabei einer Vielzahl von Bedrohungen ausgesetzt. Für jede einzelne Komponente kann dabei von den üblichen Bedrohungspotentialen ausgegangen werden, z. B. Manipulation der Einträge auf den Telekommunikationsleitungen, Zugriffe Unberechtigter (Mithören), Zerstörung der Infrastruktur, Einspielen alter Versionen des Dienstes, Virenbefall etc. Neben diesen allgemeinen Bedrohungen gibt es allerdings auch verzeichnisspezifische.

Das Bedrohungspotential ist abhängig vom Verbreitungsgrad und den Zugriffsmöglichkeiten auf die Inhalte. Ein Beispiel ist die Einführung eines Verzeich-

3 Die Möglichkeit der Replikationen ist wesentlicher Bestandteil der Funktionalität eines Verzeichnisdienstes

nisdienstes in einem Intranet, in dem nur die Adressdaten der Mitarbeiter aufgenommen wurden und das ausschließlich zur Verbesserung der internen Kommunikation dienen soll. Die Verbreitung der Adressen über das eigene Netz hinaus ist nicht vorgesehen. Damit ist das Verzeichnis als eine Art "hausinternes elektronisches Telefonbuch" zu bewerten. Die Bedrohung ist als sehr gering zu bewerten.

Verzeichnisdienste können durch Nutzung von systemimmanenten Replikationsmechanismen oder durch automatisiertes Abfragen zur Bildung von zeitabhängigen Profilen missbraucht werden. Dies sollte vor allem bedacht werden, wenn Verzeichnisdienste bereitgestellt werden, da die Auswerteverfahren und –werkzeuge dann nicht kontrollierbar sind.

4.1 Rechtliche Einordnung von Verzeichnisdiensten

Soweit Verzeichnisdienste nur im Intranet einer datenverarbeitenden Stelle angeboten werden, handelt es sich weder um einen Tele- noch einen Mediendienst. Es liegt somit kein „Angebot" i. S. d. §§ 2 Abs. 2 TDG bzw. MDSTV vor. Die Zulässigkeit derartiger Verzeichnisdienste richtet sich daher allein nach den allgemeinen datenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse.

Wird der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder gar ausgebaut, ist der Personalrat (und im Bereich der Privatwirtschaft der Betriebsrat) aufgefordert, durch Nutzung seiner Mitbestimmungsrechte und Abschluss von Dienst- und Betriebsvereinbarungen die Zusammenführung von Daten zu unterbinden bzw. zu kontrollieren.

4.2 Veröffentlichung von Klarnamen

Grundsätzlich sollte allen Bediensteten, die keine herausgehobene Funktion innehaben, ein Wahlrecht dahingehend eingeräumt werden, ob sie mit ihrem Klarnamen oder mit einem selbstgewählten Pseudonym in ein über das Intranet abrufbares Verzeichnis eingestellt werden wollen. Dieses Modell könnte auch genutzt werden, um die Zusammenführung von verschiedenen Verzeichnissen zu unterbinden, wenn der Betroffene verschiedene rollenspezifi-

sche Pseudonyme wählt. Auf diese Weise könnten auch die Risiken einer unkontrollierten Sammlung personenbezogener Informationen durch Suchmaschinen begrenzt werden.

4.3 Beschäftigtendaten in Verzeichnisdiensten

Die Verarbeitung von Personaldaten ist im Bund und in den Ländern unterschiedlich geregelt. Zum Teil enthalten die allgemeinen Datenschutzgesetze einschlägige Bestimmungen, zum Teil wird die Verarbeitung in den Beamtengesetzen angesprochen, wobei einige Landesbeamtengesetze diese Regelungen im Tarifbereich für entsprechend anwendbar erklären. Das Bundesbeamtengesetz (BBG) enthält keine umfassenden Vorschriften über die Verarbeitung von Personaldaten, sondern lediglich Regelungen über die Datenerhebung und den Umgang mit Personalaktendaten. Inhaltlich stimmen alle Regelungen darin überein, dass Beschäftigtendaten verarbeitet werden dürfen, wenn dies u. a. zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Soweit auf den Verzeichnisdienst nur Mitarbeiterinnen/Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiterinnen/Mitarbeiter zur Verfügung gestellt werden. Erstreckt sich die Zugriffsmöglichkeit auch auf andere Stellen im jeweiligen Bundesland, dürfen Familienname, dienstliche Telefonnummer und Hinweise auf den Aufgabenbereich von solchen Personen in den Verzeichnisdienst aufgenommen werden, die den Anschluss aus dienstlichen Gründen nutzen müssen und bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört. Unterschiedlich ist die Frage zu beurteilen, ob über diese Angaben hinaus die Amtsbezeichnung oder der Vorname in den Verzeichnisdienst eingestellt werden darf. Hier greifen unterschiedliche Regelungen in den einzelnen Bundesländern, so dass eine generelle Aussage hierzu unmöglich ist.

Für Bedienstete, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben (z. B. Angehörige interner Dienste, wie des Schreib- oder Botendienstes), ist die Bekanntgabe ihrer Daten nicht erforderlich. Deren Aufnahme in den Verzeichnisdienst wäre nur mit Einwilligung zulässig.

Soweit die Auffassung vertreten wird, dass Name, Dienst-, Funktionsbezeichnung und Organisationseinheit von Bediensteten wegen ihres engen Bezuges zur amtlichen Tätigkeit nicht deren grundsätzlicher Verfügungsbefugnis und damit ihrem Recht auf informationelle Selbstbestimmung unterfallen (Amtswaltertheorie), ergeben sich keine anderen Ergebnisse. Das Erfordernis, die genannten Daten für dienstliche Zwecke einzusetzen, dürfte sich regelmäßig auf das jeweilige Bundesland beschränken. Bei einer über den Landesbereich hinausgehenden Bereitstellung von Daten, beispielsweise bei einer Verbindung zweier öffentlicher Netze, empfiehlt sich – wie allgemein in Zweifelsfällen – der Abschluss einer Dienstvereinbarung.

5. Maßnahmen

Aus datenschutzrechtlicher Sicht sind beim Betrieb eines Verzeichnisdienstes technische und organisatorische Maßnahmen vorzunehmen, die geeignet sind, den aufgeführten Gefahren und Bedrohungen entgegenzuwirken. Für die Komponenten, auf die der Verzeichnisdienst aufsetzt, sind hinreichende und angemessene technische und organisatorische Datenschutzmaßnahmen zu realisieren. Allgemeine Empfehlungen finden sich in entsprechenden Orientierungshilfen (z. B. Unix-Systeme, PCs, Mail-Systeme oder Datenträger) oder auch im BSI-Grundschutzhandbuch, im UNIX-Leitfaden des Hamburger Datenschutzbeauftragten und in Checklisten des Landesbeauftragten für den Datenschutz in Niedersachsen.

Über die grundlegenden Maßnahmen hinaus ist beim Einsatz von Verzeichnisdiensten Folgendes zu beachten:

- Der Verzeichniseintrag ist auf die notwendigen Angaben zu beschränken, beispielsweise E-Mail-Adresse, Telefonnummer, Faxnummer, öffentliche Schlüssel etc. Andere Informationen, wie Hinweise auf Zuständigkeiten, Aufgabenbereiche, Tätigkeitsfelder, Arbeitszeiten, Örtlichkeiten etc., sollten, soweit nicht für die Aufgabenerledigung notwendig, nicht in das Verzeichnis aufgenommen werden.

- Die Zugriffsregelungen sind so eng wie möglich zu fassen. Die Verantwortung hierzu muss eindeutig und durch eine hierfür verantwortliche Stelle vorgenommen werden. Grundsätzlich sollten starke Authentifizierungsme-

chanismen (Digitale Signatur, biometrische Verfahren) zum Einsatz kommen (siehe Kapitel 2.1). Produkte, die lediglich dem X.500-Standard entsprechen, sind nicht einzusetzen.

- Die Organisation des Verzeichnisdienstes muss so gestaltet werden, dass sichergestellt ist, dass die Einträge des Verzeichnisdienstes immer in möglichst zeitnaher Aktualität vorliegen. Dies schließt auch Kopien des Verzeichnisses (Repliken) ein.

- Die Neueinrichtung, Änderung und Löschung von Verzeichniseinträgen sowie die Erstellung und Verbreitung von Repliken sind zu Zwecken der Revision und Datenschutzkontrolle zu protokollieren. Sofern die Protokollierung kein Bestandteil des Produkts ist, muss eine ausreichende Protokollierung durch andere Komponenten, beispielsweise das Betriebssystem, sichergestellt werden.

- Es ist zu prüfen, zu welchen Personen Angaben im Verzeichnisdienst zur Verfügung gestellt werden dürfen.

- Der Verzeichniseintrag ist auf die Angaben zu beschränken, die in der ausgeübten Funktion für die Nutzer des Verzeichnisses relevant sind. Mögliche Angaben sind E-Mail-Adresse, Telefonnummer, Faxnummer, öffentliche Schlüssel, Hinweise auf die Zuständigkeit, Aufgabenbereiche.

- Vor "Veröffentlichung" des Eintrags im Verzeichnis müssen dem Betroffenen die Daten des Eintrags zur Einsichtnahme und/oder Korrektur vorgelegt werden. Anhand von Attributen ist eine Filterung der Verzeichniseinträge nach dem Gesichtspunkt der internen/externen Bereitstellung zu ermöglichen oder die Möglichkeit zu schaffen, dass die Betroffenen selbst eine Sperrung oder Freischaltung bestimmter Attribute vornehmen können.

- Zur Sicherung der Integrität sind bei der Übertragung grundsätzlich kryptographische Verfahren einzusetzen. Ist die Vertraulichkeit von Verzeichnisdaten zu gewährleisten, z. B. bei Abfragen oder Replikation über unsichere Leitungen, so sind auch hierfür geeignete kryptographische Methoden zu benutzen. Dazu stehen auch Werkzeuge außerhalb des Verzeichnisdienstes (etwa zur Verbindungsverschlüsselung) zur Verfügung.

Teil 3

Internetnutzung durch öffentliche Stellen

Auszug aus dem Arbeitspapier "Vom Bürgerbüro zum Internet" der Arbeitsgruppe "Serviceorientierte Verwaltung" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: November 2000

1. Informationsangebote öffentlicher Stellen im Internet

1.1 Inhaltsebene und Tele-/Mediendienste

Bei der Bereitstellung von Informationsangeboten öffentlicher Stellen im Internet und deren Nutzung werden auf vielfältige Weise personenbezogene Daten verarbeitet. Je nach Art bzw. Zweck der Verarbeitung sind unterschiedliche Regelungen zu beachten. Man unterscheidet:

- Dienstedaten
  - Bestandsdaten
  - Nutzungsdaten
  - Abrechnungsdaten
- Inhaltsdaten

Die Datenarten werden in der nachstehenden Tabelle näher erläutert. Bei Bestands-, Nutzungs- und Abrechnungsdaten handelt es sich überwiegend um Daten der Nutzerinnen und Nutzer, die von der öffentlichen Stelle oder einem von ihr beauftragten Mediendienste- oder Teledienstean bieter verarbeitet werden, um ein entsprechendes Internet-Angebot zu realisieren. Bei der Bereitstellung von reinen Informationsangeboten fallen neben den Inhaltsdaten insbesondere Nutzungsdaten an. Auf die datenschutzrechtlichen Regelungen zur Verarbeitung dieser Daten wird in Kap. 1.3 eingegangen.

Datenart		Beschreibung	Beispiele	Rechts-grundlage
Dienste-daten	Bestands-daten	Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind.	Name, Anschrift der Nutzer, statische IP-Nummer, Kontonummer Kreditkarten-Nummer	TDDSG, MDStV
	Nutzungs-daten	Nutzerdaten, die für die Inanspruchnahme von Diensten erforderlich sind.	Name oder IP-Adresse des anfragenden Clients, Username, Anfrage und deren Status	TDDSG, MDStV
	Abrech-nungs-daten	Nutzerdaten für die Abrechnung von Diensten	Zeitpunkt und Dauer von Verbindungen, Datenvolumen	TDG, TDDSG, MDStV
Inhalts-Daten		In den Internet-Angeboten zum Abruf bereitgestellte Informationen	Zeichen, Bilder, Töne	Landes-datenschutz-gesetze, BDSG, Fachgesetze

Inhaltsdaten sind die eigentlichen Informationen, die von der öffentlichen Stelle zum Abruf bereitgestellt werden. Die Zulässigkeit der Verarbeitung von Inhaltsdaten wird in Kap. 1.2 behandelt.

1.2 Inhaltsdaten: Was darf ins Internet?

Die Bereitstellung von personenbezogenen (Inhalts-)Daten im Internet hat sich in vielen Fällen nach bereichsspezifischen Regelungen zu richten (z. B. Sozialgesetzbuch, Meldegesetze). Fehlen solche Regelungen, so sind die jeweiligen Landesdatenschutzgesetze und bei Stellen des Bundes das Bundesdatenschutzgesetz einschlägig. Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene Benutzergruppe durch z. B. ein Passwortverfahren gebildet wird, besteht weltweit die Möglichkeit zu einem Abruf. Da es Staaten gibt, in denen keine oder sehr schwach ausgeprägte Datenschutzbestimmungen existieren, können die schutzwürdigen Belange von

Betroffenen durch die Einstellung ins Netz in besonderem Umfang beeinträchtigt sein. Ein Bereithalten personenbezogener Daten im Internet ist daher nur zulässig, wenn die betroffenen Personen

- dies aufgrund einer Rechtsvorschrift hinzunehmen
- oder eingewilligt haben.

Einwilligung

Die Merkmale einer wirksamen Einwilligung sind:

- **Freiwilligkeit**
  Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig erteilt worden ist.

- **Informiertheit**
  Voraussetzung jeder Einwilligung ist, dass die Betroffenen umfassend über die Verarbeitung (Verwendungszweck, Beteiligte/Empfänger, Form der Verarbeitung, Anonymisierung) unterrichtet werden. Die Betroffenen sind darüber zu unterrichten, dass aus der Verweigerung einer Einwilligung keine Nachteile entstehen.

- **Schriftlichkeit**
  Von der Schriftform kann nur abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die neuen Datenschutzgesetze sehen auch eine elektronische Form der Einwilligung vor.

- **Widerrufbarkeit**
  Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung verweigern oder in Zukunft widerrufen können.

Auch bei einer Verarbeitung mit Einwilligung sind die sonstigen Datenschutzvorkehrungen zu beachten.

Unabhängig hiervon ist der Grundsatz der Datenvermeidung zu beachten. Auch wenn die Verarbeitung von personenbezogenen Daten im Internet zulässig ist, sind alternative anonyme oder pseudonyme Verfahren zu wählen, wenn der Zweck der Verarbeitung so in gleicher Weise erreicht werden kann.

Diese allgemeinen Aussagen zur Zulässigkeit der Bereitstellung werden im Folgenden in einzelnen Teilbereichen verifiziert.

1.2.1 Bedienstetendaten

In Bund und Ländern ist die Verarbeitung von Bedienstetendaten der öffentlichen Stellen bereichsspezifisch geregelt (Sondervorschriften in den Datenschutzgesetzen, Beamtengesetze der Länder). Danach ist eine Übermittlung der Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Dienstverkehr es erfordert oder die Betroffenen eingewilligt haben. Eine Veröffentlichung von Bedienstetendaten im Internet ist demnach zulässig, wenn der Dienstverkehr eine solche Veröffentlichung erfordert.

Diese Voraussetzungen sind in der Regel erfüllt für die Bekanntgabe des Namens, der dienstlichen Telefon- und Faxnummer, der E-Mail-Adresse und eines Hinweises auf den Aufgabenbereich von Bediensteten, die aufgrund ihres Aufgabenbereichs mit privaten oder anderen Dritten regelmäßig in Kontakt stehen, oder von herausgehobenen Funktionsträgern. Für Bedienstete, die in der Regel keinen unmittelbaren dienstlichen Kontakt mit Bürgerinnen und Bürgern haben (z. B. Angehörige interner Dienste wie des Schreib- oder Botendienstes), gilt dies nicht. Ob in diesem Zusammenhang eine Übermittlung von Vornamen und Amtsbezeichnung erforderlich ist, wird unterschiedlich beurteilt. In Zweifelsfällen sollte eine Einwilligung eingeholt oder auf eine Veröffentlichung ganz verzichtet werden. In Betracht kommt auch eine Regelung durch Abschluss einer Dienstvereinbarung. Auf jeden Fall müssen die Bediensteten in geeigneter Form vor der Bereitstellung der Daten im Internet informiert werden. Zusätzlich sollte ihnen ein Widerspruchsrecht eingeräumt werden.

Weitere Daten über Beschäftigte mit Außenkontakten, wie private Telefonnummer, Fotos usw., dürfen nur mit Einwilligung der Betroffenen in Internet-Angeboten bereitgehalten werden. Die Bereitstellung von vollständigen

Geschäftsverteilungsplänen oder Telefonverzeichnissen ist in aller Regel nicht erforderlich und damit ohne Einwilligung oder Dienstvereinbarung unzulässig. Sachsen-Anhalt und Thüringen halten die Veröffentlichung von Bedienstetendaten generell nur mit Einwilligung für zulässig.

1.2.2 Bürgerdaten

Grundsätzlich rechtlich zulässig ist die Bereitstellung von Informationen, die ohnehin rechtmäßig veröffentlicht sind oder werden dürfen. Hierzu gehören u. a.

- Publikationen der Presse,
- Tagesordnungen, Referenten, u. U. Gremienmitglieder öffentlicher Veranstaltungen,
- amtliche Bekanntmachungen.

Dabei ist allerdings zu beachten, dass auf diese Weise ein weltweiter Zugriff möglich ist und die bereitgestellten Daten automatisiert recherchierbar sind. Vor der Entscheidung einer Veröffentlichung im Internet sollten daher mögliche negative Konsequenzen für die Betroffenen untersucht und berücksichtigt werden. Zusätzlich sollte ihnen ein Widerspruchsrecht eingeräumt werden. Bereits bestehende Widerspruchsrechte sind zu beachten. Außerdem sollten die Möglichkeiten zur Reduzierung der Recherchierbarkeit in geeigneter Weise genutzt werden (siehe Kasten).

Fehlt eine Rechtsgrundlage, können Daten von Bürgerinnen und Bürgern nur mit ihrer Einwilligung veröffentlicht werden. Dabei sollten pseudonyme Verfahren gewählt werden, wenn dies möglich und sinnvoll ist. Auch beim Vorliegen einer Einwilligung sollten die Möglichkeiten zur Einschränkung der Recherchierbarkeit in geeigneter Weise genutzt werden.

Einschränkung der Recherchierbarkeit von Webseiten

Der automatisierten Recherchierbarkeit von Webseiten kann begegnet werden, wenn die Daten nur über Downloads oder geeignete Datenbankabfragen übermittelt werden. Eingeschränkt gilt dies auch für Webseiten, die beim Zugriff aus Datenbankinhalten automatisch erstellt werden ("dynamisch generierte Webseiten"). Sie können zwar prinzipiell von Suchmaschinen indiziert werden; die meisten Anbieter von Suchmaschinen verzichten aber hierauf, weil so zu viele Fehleintragungen entstehen würden. Es besteht auch die Möglichkeit, durch die Aufnahme von geeigneten Metainformationen in das Internet-Angebot die automatische Recherche durch Suchmaschinen einzuschränken. So werden z. B. durch den html-Befehl

<META NAME="robots" CONTENT="noindex">

Suchmaschinen angewiesen, den Seiteninhalt nicht zu indizieren. Allerdings hängt es von der Gestaltung der jeweiligen Suchmaschine ab, ob diese Befehle unterstützt werden oder nicht.

1.2.3 Webcams

Es wird immer häufiger üblich, Kameras in öffentlichen und privaten Bereichen aufzustellen und deren Bilder im Internet abrufbar zu speichern. Öffentliche Stellen dürfen dies allenfalls dann tun, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter, Autokennzeichen oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder Bildbearbeitung seitens des Empfängers erkennbar gemacht werden können. In Frage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen. Dabei spielen Rahmenbedingungen wie Bildausschnitt, Bildschärfe oder Bildfrequenz eine wichtige Rolle.

Es sollte auch beachtet werden, dass die erwarteten Informationen oft auf andere, datensparsamere Weise übermittelt werden können. Z. B. können Informationen über die Verkehrslage in Schriftform ("Stau im Bereich...") oder über markierte Stadtpläne oft wirkungsvoller, schneller und völlig ohne personenbezogene Daten über das Internet weitergegeben werden.

1.3 Nutzungsdaten: Was darf wie verarbeitet werden?

Internet-Angebote öffentlicher Stellen sind entweder Teledienste, die im Teledienstegesetz (TDG) und im Teledienstedatenschutzgesetz (TDDSG) geregelt sind, oder Mediendienste, für die der Mediendienste-Staatsvertrag (MDStV) gilt. Teledienste sind alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. § 2 Abs. 2 TDG nennt einige Beispiele, wie Telebanking, Datenaustausch, Datendienste (z. B. über Verkehrs- oder Wetterdaten), Angebote zur Nutzung des Internet oder weiterer Netze, Angebote zur Nutzung von Telespielen und Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. Zu den Mediendiensten gehören die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste wie Fernseheinkauf, Verbreitung von Messergebnissen in Text und Bild, Fernsehtext und vergleichbare Textdienste.

Da die Datenschutzregelungen für Tele- und Mediendienste in TDG/TDDSG und MDStV weitgehend identisch sind, kann die schwierige Unterscheidung zwischen Telediensten und Mediendiensten bei Internetangeboten öffentlicher Stellen in der Regel dahingestellt bleiben. Öffentliche Stellen haben folgende Anforderungen zu erfüllen:

- Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen (soweit es sich nicht um Abrechnungsdaten handelt; § 6 Abs. 2 TDDSG bzw. § 15 Abs. 2 MDStV).

- Der Anbieter darf die Erbringung von Diensten nicht von einer Einwilligung der Nutzerinnen und Nutzer in eine Verarbeitung und Nutzung ihrer Daten für andere Zwecke abhängig machen (§ 3 Abs. 3 TDDSG bzw. § 12 Abs. 4 MDStV).

- Die Prinzipien der Datenvermeidung und der Datensparsamkeit sind zu beachten (§ 3 Abs. 4 TDDSG bzw. § 12 Abs. 5 MDStV).

- Der Anbieter hat den Nutzerinnen und Nutzern die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Nutzerinnen und Nutzer sind über diese Möglichkeit zu informieren (§ 4 Abs. 1 TDDSG bzw. § 13 Abs. 1 MDStV).

- Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 TDDSG bzw. § 13 Abs. 4 MDStV).

1.3.1 Speicherung von Nutzungsdaten

Selbst wenn eine Nutzerin oder ein Nutzer im Internet keine Daten über ihre bzw. seine Identität von sich aus offenbart (Ausfüllen von Formularen, E-Mail-Adressen usw.), fallen beim Anbieter Daten über die Nutzerin bzw. den Nutzer an. Dazu gehören die IP-Adressen, über die der Datenaustausch vollzogen wird.

IP-Adresse

Die IP-Adresse (IP = Internet-Protokoll) ist die eindeutige Adresse eines Rechners im weltweiten Internet. Man schreibt sie meist als vier durch Punkte voneinander getrennte Zahlen zwischen 0 und 255. Da Bezeichnungen leichter zu merken sind als Zahlen, sind den IP-Adressen sog. Domain-Namen zugeordnet. Die Zuordnung wird im Domain Name System (DNS) über bestimmte DNS-Server aufgelöst.

Während die Internet-Server feste IP-Adressen haben, gilt dies für die Rechner der meisten Nutzerinnen und Nutzer nicht. Vielmehr erhalten sie von ihrem Access-Provider für die jeweilige Internet-Session eine IP-Adresse dynamisch zugeteilt. Es besteht die Gefahr, dass dynamische IP-Adressen außer vom Access-Provider auch von Außenstehenden (mit großem Aufwand) einer bestimmten Nutzerin oder einem bestimmten Nutzer zugeordnet werden.

Es gibt außerdem Rechner, die über fest vergebene IP-Adressen verfügen. Dies können Rechner von Universitäten oder Firmen sein, die einen großen Bereich von IP-Adressen erworben haben, oder auch private Nutzer, die sehr früh im Internet präsent waren. In diesen Fällen lässt sich die IP-Adresse häufig auch ohne weitere Hilfsmittel einer bestimmten Nutzerin bzw. einem bestimmten Nutzer zuordnen; sie ist deshalb als ein personenbezogenes Datum anzusehen. Allerdings ist nicht erkennbar, ob eine IP-Adresse statisch oder dynamisch ist. Öffentliche Stellen müssen deshalb darauf achten, dass vollständige IP-Nummern bei der Nutzung ihrer

Informationsangebote nicht dauerhaft protokolliert werden. Dies kann zum einen durch einen vollständigen Verzicht auf Protokollierungen erfolgen. Eine andere Möglichkeit besteht darin, nur die ersten drei Nummern der IP-Adresse zu speichern. Auch ist es denkbar, schon während der Verbindung den Besuch des Internetangebots durch Zuordnung zu einer größeren Nutzergruppe zu erfassen, um so eine gewünschte, anonyme Statistik zu erhalten.

1.3.2 Cookies

Die Verwendung von Cookies stellt einen Eingriff in die Datenverarbeitung auf dem persönlichen Rechner des Nutzers dar. Für die Nutzerinnen und Nutzer ist in den meisten Fällen allenfalls die Tatsache einer Speicherung, nicht aber unmittelbar dessen Inhalt und Bedeutung erkennbar.

Cookies

Cookies sind kleine Dateneinheiten, die von Internet-Servern auf den Rechnern der Nutzer gespeichert werden. In den Cookies können Aktivitäten der Nutzerin bzw. des Nutzers festgehalten werden. Cookies können zur Verbindungssteuerung während einer Sitzung ("Session Cookies") verwendet werden. In diesem Fall werden sie bei Beendigung der Sitzung wieder gelöscht. Häufig werden Cookies aber über viele Jahre gespeichert, um dem Anbieter beim nächsten Zugriff eine "bedarfsgerechte" Angebotsauswahl oder die Führung von Statistiken über das Nutzerverhalten zu ermöglichen bzw. Nutzerprofile zu bilden.

Die Verwendung von Cookies unterliegt dem TDDSG oder dem MDStV, wenn die Cookies bestimmten Personen zugeordnet werden können. Eine Zuordnung ist dann möglich, wenn – wie oben beschrieben – Nutzerinnen und Nutzer statische IP-Adressen verwenden oder ihren Namen in Transaktionen preisgeben. In diesen Fällen ist die Verwendung von Cookies nur mit Einwilligung der Nutzerin bzw. des Nutzers zulässig, wenn sie über das Sitzungsende hinaus gespeichert werden sollen. Dabei ist zu beachten, dass bei einer Preisgabe des Namens auch früher gesetzte Cookies zugeordnet werden können.

Wegen der damit verbundenen Risiken sollten öffentliche Stellen in ihren Informationsangeboten auf das Setzen von Cookies möglichst vollständig verzichten, soweit diese nicht zur Gestaltung des Angebots als so genannte Session Cookies eingesetzt werden.

1.3.3 Active-X, Java, JavaScript, Plug-Ins

Active-X-Controls, Java-Applets und JavaScripts sind Programme, die beim Aufrufen von Angeboten auf den Rechner des Nutzers heruntergeladen und dort zur Ausführung gebracht werden. Eine Gefahr geht insbesondere von Programmeinheiten aus, die unter Ausnutzung von Sicherheitslücken Funktionen mit schädlichen Eigenschaften beinhalten. Diesen Gefahren kann der Nutzer durch Deaktivierung der Ausführbarkeit der Programme begegnen. Anbieter sollten daher damit rechnen, dass Nutzer beispielsweise Active-X-Controls, Java-Applets oder Plug-Ins (im Nutzerbrowser installierte Zusatztools) nicht ausführen können. Dies gilt insbesondere für Active-X-Programme, von denen im Allgemeinen die weitreichendsten Gefährdungen für Internet-Nutzer ausgehen. Die Informationsangebote sollten dementsprechend ohne solche Programme gestaltet werden.

1.4 Gestaltung des Angebots

1.4.1 Datenschutzhinweise

§ 12 Abs. 6 MDStV und § 3 Abs. 5 TDDSG legen fest, dass der Nutzer vor einer Erhebung personenbezogener Daten über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten zu unterrichten ist. Diese Regelung lässt sich in vielen Fällen umsetzen, wenn im Informationsangebot der öffentlichen Stellen Datenschutzhinweise gegeben werden. Sie sollten immer dann veröffentlicht werden, wenn personenbezogene Daten online über die Web-Site gesammelt werden. Dies ist dann der Fall, wenn z. B. eine Online-Registrierung verlangt bzw. ermöglicht wird, wenn sonstige Formulare online ausgefüllt werden können oder wenn mittels E-Mail mit der öffentlichen Stelle kommuniziert werden kann. Auch wenn dies nicht der Fall ist, sollten entsprechende Datenschutzhinweise gegeben werden.

Die Datenschutzhinweise von Informationsangeboten sollten eine Erklärung zu Grundsätzen und Verfahrensweisen bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten enthalten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Informationsangebotes im Internet auftreten.

Beispiel für Datenschutzhinweise

Mit Ihrem Zugriff auf diese Web-Site werden Ihre um die letzte Zahl verkürzte IP-Adresse und weitere Angaben (Datum, Uhrzeit, betrachtete Seite) auf unserem Server für Zwecke der Datensicherheit für zwei Monate gespeichert. Die Daten werden außerdem für statistische Zwecke ausgewertet. Durch die Verkürzung der IP-Adresse ist ein Bezug der gespeicherten Daten auf Ihre Person ausgeschlossen.

Wir verwenden keine Cookies, Java-Applets oder Active-X-Controls.

Sollten Sie noch Fragen zum Datenschutz haben, so wenden Sie sich bitte an:
Name: ... E-Mail-Adresse: ... Telefon: ...

Darüber hinaus steht Ihnen auch der Landes-/Bundesbeauftragte für den Datenschutz als Ansprechpartner zur Verfügung.

Web-Site: ... E-Mail-Adresse: ... Telefon: ...

Wenn Sie eine E-Mail mit schutzwürdigem Inhalt an uns senden wollen, so empfehlen wir dringend, diese zu verschlüsseln, um eine unbefugte Kenntnisnahme und Verfälschung auf dem Übertragungsweg zu verhindern. Unseren öffentlichen Schlüssel finden Sie unter ... unseres Informationsangebots.

Die Hinweise sollten an zentraler Stelle erfolgen, z. B. direkt auf der Begrüßungsseite oder durch einen Link über eine aussagekräftige Schaltfläche. Hier sollte erläutert werden, ob und inwiefern IP-Adressen für statistische Zwecke verarbeitet werden. Auch sollte darauf hingewiesen werden, ob Cookies verwendet werden. Soweit dies zutrifft, sollte dies begründet und über die Auswirkungen

informiert werden. Wenn dies nicht der Fall ist, sollte hierauf hingewiesen werden, weil damit eventuell vorhandene Bedenken und Befürchtungen der Besucher zerstreut werden können.

1.4.2 Anbieterkennzeichnung, Impressum

Sowohl das Teledienstegesetz als auch der Mediendienstestaatsvertrag sehen eine Anbieterkennzeichnung vor (§ 6 TDG, § 6 MDStV). Diese muss Name und Anschrift, bei Personenvereinigungen und -gruppen auch Name und Anschrift des Vertretungsberechtigten enthalten. Die Anbieterkennzeichnung schafft auch aus Datenschutzsicht Transparenz und sollte dementsprechend zentral und vollständig in das Internet-Angebot eingestellt werden. Das Impressum sollte von jeder Webseite aus erreichbar sein.

Dienstanbieter sollten auch deutlich herausstellen, wenn ein Link des Angebots zu einer Seite führt, die nicht mehr im eigenen Verantwortungsbereich liegt (§ 4 Abs. 3 TDDSG, § 13 Abs. 3 MDStV).

Vorschlag für ein Impressum

Stadt <Name>
Verantwortlich: <Name>
<Straße>
<PLZ/Ort>
Telefon: <Telefonnummer>
Telefax: <Telefaxnummer>
E-Mail: <E-Mail-Adresse>

Hinweis zu externen Links
Die Stadt <Name> ist als Inhalteanbieter (Content provider) nach § 5 Abs.1 des Teledienstegesetzes (TDG) bzw. § 5 Mediendienstestaatsvertrag (MDStV) für die "eigenen Inhalte", die sie zur Nutzung bereithält, verantwortlich. Von diesen eigenen Inhalten sind Querverweise ("Links") auf die von anderen Anbietern bereitgehaltenen Inhalte zu unterscheiden. Durch Querverweise hält die Stadt <Name> "fremde Inhalte" zur Nutzung bereit, die durch den Hinweis ▼

[LINK]
gekennzeichnet sind. Die Stadt <Name> hat bei der erstmaligen Verknüpfung die fremden Inhalte gesichtet. Bei Links handelt es sich allerdings stets um "lebende" (dynamische) Verweisungen; die fremden Inhalte können deshalb geändert worden sein, ohne dass die Stadt <Name> hiervon Kenntnis hat.

1.5 Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren und zerstören. Dies ist besonders gravierend, weil angesichts von ca. 200 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Dieses Risiko ist bei den Informationsangeboten öffentlicher Stellen zu berücksichtigen. Die meisten Gefahren können durch eine geeignete Platzierung des Web-Servers beseitigt werden. Web-Server sollten sich auf jeden Fall außerhalb der lokalen Netze der öffentlichen Stelle befinden. Dies kann durch eine Insellösung realisiert werden, bei der die Daten über das Internet oder durch direkte Eingabe gepflegt werden. Um einen Zugriff aus den lokalen Netzen in das Internet sowie eine Online-Pflege des Web-Servers zu ermöglichen und dennoch die lokalen Netze zu schützen, ist der Einsatz einer Firewall zwischen

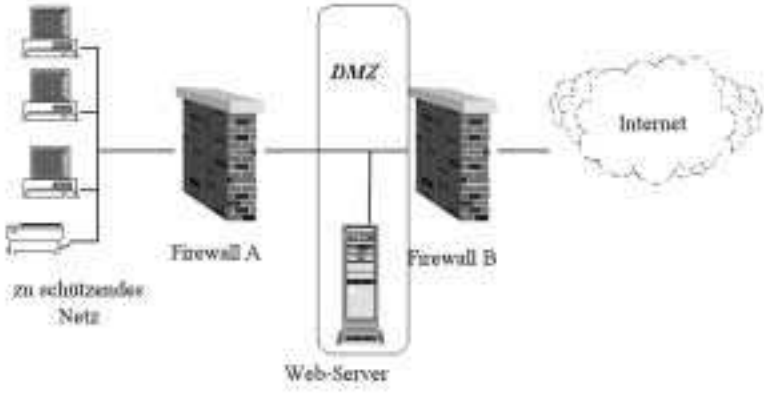
lokalen Netzen und Web-Server erforderlich. Zusätzlich muss der Web-Server selbst gegen Manipulationen aus dem Internet geschützt werden. Er sollte so konfiguriert werden, dass nur die unbedingt erforderlichen Dienste und Protokolle aktiviert sind, die Schreibrechte auf das unabdingbare Maß beschränkt sind und eine Anzeige der Verzeichnisstruktur nicht möglich ist. Weitere Sicherheitsvorgaben lassen sich durch den Aufbau einer doppelten Firewall erreichen, wobei der Web-Server zwischen diesen in der so genannten demilitarisierten Zone steht (siehe Abbildung).

Dabei sollte auf Folgendes geachtet werden:

- Die Anschaffung eines Firewallsystems allein schafft noch keine ausreichende Sicherheit. Die Firewall muss in geeigneter Weise konfiguriert werden. Außerdem müssen die Verantwortlichen für die System- und Netztechnik die Internet-Systeme regelmäßig überprüfen. Auch ist organisatorisch sicherzustellen, dass auf neue Risiken und bekannt werdende Sicherheitslücken sofort mit den geeigneten Maßnahmen reagiert wird.

- Der direkte Zugriff auf Datenbanken der öffentlichen Stelle im LAN sollte nicht zugelassen werden. Soweit ein Datenbankzugriff erforderlich ist, sollten Kopien in Rechnern der entmilitarisierten Zone verwendet werden.

- Das Internet-Angebot ist durch geeignete Maßnahmen gegen unbefugte Manipulationen zu sichern. Hierzu gehören eine sichere Konfiguration der



Rechteverwaltung und eine geeignete Protokollierung unerlaubter Zugriffe auf dem Web-Server sowie eine geeignete Einstellung der äußeren Firewall.

- Besonderes Augenmerk ist auf die personenbezogenen Daten zu richten, die durch die Nutzung entstehen. Sie müssen gegen den Zugriff über das Internet geschützt werden und sollten nur kurzfristig im Web-Server gespeichert sein.

Unabhängig hiervon muss den Risiken begegnet werden, denen eigene Mitarbeiter bei der Nutzung des Internet ausgesetzt sind. Zusätzlich zur Firewall müssen z. B. Maßnahmen gegen Computerviren, schädliche Active-X- und Java-Programme oder Plug-Ins, fehlerhafte Bedienung usw. getroffen werden.

Weitere Informationen zum Thema Datenschutz und Internet können z. B. den Orientierungshilfen der Datenschutzbeauftragten des Bundes und der Länder entnommen werden (Orientierungshilfe Internet des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter www.datenschutz.de, Orientierungshilfen und Selbstschutz unter www.lfd.niedersachsen.de u. a.).

2. Interaktive Verwaltung

Im Zusammenhang mit den Informationsangeboten öffentlicher Stellen im Internet (unter 1.) wurden bereits grundlegende Vorgaben für die Gestaltung des Internetauftrittes angesprochen. Wollen die Verwaltungen auch eine interaktive Kommunikation mit den Bürgerinnen und Bürgern im Internet anbieten, sind darüber hinaus weitere Gesichtspunkte bei der Gestaltung des Angebotes zu berücksichtigen:

- Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

- Wie ist die internetbasierte Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?

- Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

- Ist der Einsatz von Signierverfahren erforderlich?

- Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

2.1 Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

Die Service-Orientierung der Verwaltung bedingt ein hohes Maß an Organisationsfreiheit der Verwaltung in der Ausgestaltung der Kommunikation mit den Bürgerinnen und Bürgern. Gerade auch Kommunen haben seit jeher auf ihre Organisationshoheit verwiesen, deren Grenzen lediglich in den bestehenden gesetzlichen Bestimmungen liegen dürften. Das bedeutet, dass öffentliche Stellen – wenn nicht etwas anderes ausdrücklich festgelegt ist – ein Verwaltungsverfahren so durchführen können, wie sie es für zweckmäßig halten. Das schließt auch die Wahl des Kommunikationsmediums ein. Wie internetbasierte Kommunikation mit der Verwaltung künftig aussehen könnte, zeigen folgende Beispiele:

Die elektronische Bestellung zur Sperrmüllabholung

Frau A möchte, dass ihr Sperrmüll abgeholt wird. Sie setzt sich an ihren Rechner, wählt die WWW-Adresse ihrer Gemeinde aus und ruft das entsprechende Formular auf der Homepage auf. Bevor sie das Dokument absenden kann, wird mit SSL (Secure Socket Layer) ein "sicherer Kanal" aufgebaut, der von dem PC der Frau A bis zum Server der Kommune reicht. Der Aufbau erfolgt ohne weiteres Zutun von Frau A. Sie erhält lediglich den Browser-Hinweis, dass sie im Begriff ist, Daten über eine sichere Verbindung zu versenden, und dass Dritte Informationen, die mit dieser Seite ausgetauscht werden, nicht sehen können. Sie weiß damit, dass ihre Daten geschützt übertragen werden, füllt das Formular mit den entsprechenden Angaben (Name und Anschrift) aus und sendet es ab. Auf dem gleichen Weg erhält sie auch die Mitteilung über den Abholtag.

Die elektronische Anmeldung zum Volkshochschulkurs

Frau A möchte einen Volkshochschulkurs besuchen. Sie informiert sich auf der Homepage der Volkshochschule über die Angebote und entscheidet sich dort für den Kurs: "Aggressivität und aggressive Kinder – ein Wochenende für Betroffene". Auf der Homepage befindet sich der Hinweis, dass sie die Anmeldung auch online durchführen kann, wenn sie die erforderlichen Angaben per E-Mail übersendet. Da die Kommune ausdrücklich darauf hinweist, dass unver-

schlüsselte E-Mails auf ihrem Weg durch das Internet viele Stationen durchlaufen und unbemerkt gelesen oder verändert werden können, will sie das Angebot wahrnehmen, die E-Mail verschlüsselt zu übersenden. Hierzu installiert sie die erforderliche Software auf ihrem PC, lädt den öffentlichen Schlüssel der Kommune von der Homepage und überprüft ihn mit dem veröffentlichten "Fingerprint". Anschließend verschlüsselt sie ihre Angaben mit dem heruntergeladenen Schlüssel und sendet sie an die Kommune. Diese kann die E-Mail entschlüsseln und die Anmeldung entsprechend weiterleiten.

Da gesetzliche Vorgaben, die die Wahl des Kommunikationsmediums einschränken, weder für die elektronische Bestellung der Sperrgutabfuhr noch für die Anmeldung zu einem Volkshochschulkurs bestehen, wäre in diesen Beispielsfällen eine internetbasierte Kommunikation zulässig.

Dagegen lässt sich eine ebenso eindeutige Aussage für einen anderen Beispielsfall – die Wohnsitzanmeldung – nicht treffen.

Die elektronische Wohnsitzanmeldung

Frau A ist umgezogen und möchte auf elektronischem Weg ihren Wohnsitz ummelden. Zu diesem Zweck ruft sie das elektronische Formular der entsprechenden Internetseite ihrer Kommune auf und gibt ihre Daten ein. Sie signiert das Meldeformular mit ihrem Signaturschlüssel und verschlüsselt das Dokument. Das Formular wird von den zuständigen Mitarbeiterinnen und Mitarbeitern geöffnet und mit einem elektronischen Eingangsstempel versehen. Eine Bestätigung ihrer Anmeldung wird ihr übersandt.

Das Melderechtsrahmengesetz enthält keine Aussage dazu, wie die Meldepflicht konkret zu erfüllen ist. Regeln finden sich aber in den Meldegesetzen der Länder, die vorschreiben, dass die Meldepflichtigen einen Meldeschein auszufüllen, zu unterschreiben und bei der Meldebehörde abzugeben haben. Darüber hinaus sind – in der Regel durch Rechtsverordnung – Form und Inhalt des Meldescheins detailliert festgelegt. Zwar kann in den meisten Bundesländern vom Ausfüllen des Meldescheins abgesehen werden, falls das Melderegister automatisiert geführt wird. Dies gilt aber überwiegend nur dann, wenn die meldepflichtige Person bei der Behörde erscheint, um die erforderlichen

Angaben zu machen. In einigen Ländern wird zusätzlich verlangt, dass die oder der Meldepflichtige die Richtigkeit und Vollständigkeit der Daten durch Unterschrift bestätigt. Ob dort, wo das Gesetz lediglich die eigenhändige Unterschrift vorsieht, internetbasierte Kommunikationsformen der Bürgerinnen und Bürger mit der Verwaltung rechtlich zulässig sind, lässt sich bislang nicht eindeutig beantworten. Schriftliches Handeln setzt auch im Verwaltungs- bzw. Verwaltungsprozessrecht grundsätzlich eine eigenhändige Unterschrift auf einem Papierdokument voraus (vgl. m. w. N. BVerwGE 81, 32 (33)). Bezüglich der von der Verwaltung einzuhaltenden Formvorschriften gibt es gesetzliche Ausnahmen. So kann etwa beim Erlass eines schriftlichen Verwaltungsaktes, der mit Hilfe automatischer Einrichtungen erlassen wird, die Unterschrift fehlen, § 37 Abs. 4 Satz 1 VwVfG (daneben wird die Übermittlung eines Verwaltungsaktes durch E-Mail allerdings mit dem Problem des Nachweises der Bekanntgabe bzw. des Zugangs zu kämpfen haben, wovon wiederum die Wirksamkeit desselben abhängt).

Im Bereich der Kommunikation der Bürgerinnen und Bürger mit ihrer Verwaltung wäre es denkbar, unter Berufung auf die Rechtsprechung des Bundesverwaltungsgerichts im Zusammenhang mit dem Schriftformerfordernis (vgl. etwa BVerwGE 30, 274 ff.; 81, 32 ff.) weitere Ausnahmen zuzulassen.

Das Bundesverwaltungsgericht hat schon in der Vergangenheit zugunsten der Bürgerinnen und Bürger Ausnahmen vom eigenhändig unterschriebenen Dokument etwa bei der Klageerhebung (vgl. BVerwGE 81, 32 (38 ff.)) oder der Erhebung des Widerspruchs (vgl. BVerwGE 30, 274 (277 ff.)) zugelassen, wenn sich aus anderen Anhaltspunkten eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen feststellen ließ. Fortentwickelt wird diese Auffassung, die maßgeblich auf die Rechtssicherheit und Verlässlichkeit als alleinige Zwecke der Schriftform abstellt, auch durch einen Beschluss des gemeinsamen Senates der obersten Gerichtshöfe des Bundes (Az.: GmS-OGB 1/98, NJW 2000, 2340 f.) vom 05.04.2000. Darin wird der technischen Entwicklung Rechnung getragen und ein Computerfax mit eingescannter Unterschrift als ausreichend angesehen. Es dürfte nicht mehr lange dauern, bis auch die E-Mail akzeptiert wird. Eine entsprechende Entschließung, verbunden mit der Aufforderung an die Bundesregierung, die elektronische Abwicklung von Verwaltungsdienstleistungen auch im Bereich der durch Bundesrecht vorgeschriebenen Formerfordernisse zuzulassen, hat der Bundesrat

in seiner Sitzung am 09.06.2000 bereits angenommen (BR-Drs. 231/00; Beschluss). Zeitdruck wird außerdem durch das Europarecht erzeugt, da die Richtlinie 1999/93 EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Abl. EG L 13 vom 19.01.2000, Seite 12 ff.) bis zum 19.07.2001 in nationales Recht umzusetzen ist. Sie sieht in Art. 5 Abs. 1 a vor, dass die dort näher umschriebene digitale Signatur der eigenhändigen Unterschrift gleichzustellen ist. Gleichwohl sollte in den Bereichen, in denen eine eigenhändige Unterschrift für erforderlich gehalten wird, auf eine kostenintensive Projektierung internetbasierter Kommunikationsformen vorerst verzichtet werden.

Bis zur Klärung der rechtlichen Situation empfiehlt sich folgende Vorgehensweise:

Wird die eigenhändige Unterschrift für erforderlich gehalten, so ist sie nachträglich einzuholen. Ergibt sich auf andere Weise eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen, ist im Einzelfall zu entscheiden, ob ausnahmsweise auf die Unterschrift verzichtet werden kann.

2.2 Wie ist die internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?

Internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung lässt sich datenschutzrechtlich auf zwei Ebenen unterscheiden:

- Auf der Inhaltsebene sind die Vorgaben für die einzelnen Gegenstandsbereiche zu beachten, die spezialgesetzlich normiert oder den allgemeinen Datenschutzgesetzen zu entnehmen sind.

- Auf der Diensteebene gibt es Vorgaben für das Angebot von Informations- und Kommunikationsdiensten, die Pflichten speziell für die Diensteanbieterinnen enthalten.

Mit der Bestellung über das Internet hat Frau A in dem Beispielsfall 1 ihren Namen und ihre Adresse in das Formular eingegeben. Diese Angaben sind erforderlich, damit das Sperrgut abtransportiert werden kann. Die eingegebe-

nen Daten unterliegen nicht der Diensteebene, weil sie unabhängig von der Art der Kommunikation sind. Sie gehören zur Inhaltsebene. So könnte Frau A die Sperrmüllabfuhr mit denselben Angaben schriftlich, durch einen Gang aufs Amt oder telefonisch anfordern. Genauso verhält es sich mit der Anmeldung zum Volkshochschulkurs. Auch hier sind die in der E-Mail versandten Daten (Name, Adresse, Kursart etc.) der Inhaltsebene zuzuordnen. Für die Zulässigkeit der Erhebung der personenbezogenen Inhaltsdaten gilt nichts anderes als auf dem Medium Papier. Fehlt es z. B. schon an der Erforderlichkeit der Angaben, dürfen sie nicht verarbeitet werden.

Die für die Diensteebene maßgebenden rechtlichen Regelungen, nämlich der Mediendienstestaatsvertrag (MStV) und das Teledienstedatenschutzgesetz (TDDSG), enthalten Anforderungen, die erfüllt werden müssen, wenn die Kommunikation auf elektronischem Wege über das Internet geführt werden soll. Für die bei der Individualkommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung unabhängig von der Inhaltsebene anfallenden personenbezogenen Daten ist das Teledienstedatenschutzgesetz einschlägig. Nach § 6 Abs. 1 Nr. 1 TDDSG darf die Diensteanbieterin personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um den Nutzerinnen und Nutzern die Inanspruchnahme von Telediensten zu ermöglichen. Die IP-Nummer, die Aufschluss darüber geben kann, welche Rechner miteinander kommunizieren, stellt ein solches Nutzungsdatum im Sinne des Teledienstedatenschutzgesetzes dar, weil es sich hierbei um ein für den Verbindungsaufbau benötigtes Datum handelt. Die zunächst zulässig gespeicherten Nutzungsdaten sind aber frühestmöglich, spätestens nach dem Ende der jeweiligen Nutzung, zu löschen (§ 6 Abs. 2 Nr. 1 TDDSG).

Bei der E-Mail-Kommunikation ist grundsätzlich zwischen dem Transport im Internet über die E-Mail-Server und dem Empfang bzw. Versand über die Endgeräte zu unterscheiden. Im Folgenden soll lediglich auf die rechtlichen Vorgaben eingegangen werden, die die Verwaltungen beim Empfang bzw. Absenden einer E-Mail-Nachricht zu beachten haben. In diesem Fall sind die Verwaltungen nicht Adressatinnen der Befugnisse und Pflichten aus dem Teledienstedatenschutzgesetz. Das in § 3 Abs. 1 TDDSG niedergelegte Verbot mit Erlaubnisvorbehalt, personenbezogene Daten zu verarbeiten, richtet sich an die Diensteanbieterinnen ("vom Diensteanbieter"). Die Empfängerinnen und

Empfänger einer E-Mail sind nicht Anbieterinnen und Anbieter des Informations- und Kommunikationsdienstes E-Mail im Sinne des § 2 Nr. 1 TDDSG, da sie den Teledienst nicht zur Nutzung bereithalten, sondern selber Nutzerinnen und Nutzer des Dienstes sind. Als Diensteanbieterin kommt hier allenfalls die Betreiberin einer Mailbox in Betracht. Das kann im Einzellfall auch eine Kommune sein. Die Zulässigkeit der Speicherung der im Zusammenhang mit der E-Mail-Kommunikation entstandenen Datensätze richtet sich daher auch für die über den Inhalt einer E-Mail-Nachricht hinausgehenden Informationen nach den datenschutzrechtlichen Vorgaben auf der Inhaltsebene. Das bedeutet, dass personenbezogene Daten, wie etwa die Absenderadresse, das Sendedatum oder weitere Sendeinformationen zu löschen sind, wenn ihre Speicherung zur Erfüllung der jeweiligen Aufgabe nicht oder nicht mehr erforderlich ist.

Nutzungsdaten – wie etwa die IP-Nummer – sind spätestens nach dem Ende der jeweiligen Nutzung zu löschen. Auch andere Daten – wie etwa Routinginformationen – müssen gelöscht werden, wenn diese Daten nicht oder nicht mehr zur Erfüllung der jeweiligen Aufgabe der öffentlichen Stelle erforderlich sind.

2.3 Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

Anders als bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Informations- und Kommunikationsdienst E-Mail sind die Verwaltungen aber Diensteanbieterinnen, wenn sie die Bürgerinnen und Bürger zu einer internetbasierten Kommunikation etwa im Rahmen einer Homepage einladen. Nach § 4 Abs. 2 Nr. 3 TDDSG hat die Diensteanbieterin durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Für die Nutzerinnen und Nutzer muss also die Möglichkeit – nicht die Verpflichtung – bestehen, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung zu schützen (Schaar / Schulz in: Roßnagel, Recht der Multimediadienste, Stand: Januar 2000, Rdnr. 91 ff. zu § 4 TDDSG).

Die abstrakte Verpflichtung nach § 4 Abs. 2 Nr. 3 TDDSG regelt allerdings nicht, welcher Art die Anforderungen an die Verfahren zur Gewährleistung vertraulicher Kommunikation zu sein haben. Praktisch bedeutet das jedoch, dass die Verwaltungen Verschlüsselungsverfahren anzubieten haben. Das gilt unabhängig vom Inhalt für alle drei Beispielsfälle. Ein Warnhinweis kann zwar der nach § 3 Abs. 5 TDDSG erforderlichen Unterrichtung Rechnung tragen, einen wirksamen Schutz, wie er als technische oder organisatorische Maßnahme von den Diensteanbieterinnen nach dem Teledienstedatenschutzgesetz gefordert ist, stellt der Warnhinweis aber nicht dar, weil er keine vor der Kenntnisnahme Dritter geschützte Kommunikation sicherstellen kann.

Die Auswahl des konkreten Verschlüsselungsverfahrens richtet sich nach den allgemeinen Datenschutzgrundsätzen. Danach hat die Verwaltung diejenigen Verschlüsselungsverfahren anzubieten oder zu verwenden, die erforderlich sind, um die Vertraulichkeit zu gewährleisten. Vorschläge hierzu enthält die Tabelle unter Kap. 2.5.

Es gilt der Grundsatz, dass die Nutzerinnen und Nutzer Informations- und Kommunikationsdienste vor der Kenntnisnahme Dritter geschützt, z. B. durch angemessen sichere Verschlüsselung, in Anspruch nehmen können müssen. Ein bloßer Warnhinweis auf die Risiken unverschlüsselter Kommunikation im Netz reicht nicht aus.

2.4 Ist der Einsatz von Signierverfahren erforderlich?

Zum Schutz von Authentizität und Integrität ist der Einsatz von Signierverfahren zu empfehlen. Nach § 10 Abs. 2 Nr. 2 und 4 Datenschutzgesetz Nordrhein-Westfalen sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell (Integrität) bleiben und jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Eine technische Maßnahme zur Umsetzung dieser Verpflichtung kann der Einsatz von Signierverfahren sein. Ob sich die Erforderlichkeit eines Einsatzes von Signierverfahren auch aus einer Zusammenschau verschiedener Gebote technischer und organisatorischer Maßnah-

men, etwa der Zugriffs-, Übermittlungs-, Benutzer- oder der Transportkontrolle ergeben könnte, wird unterschiedlich beurteilt. Vorschläge für eine technische Umsetzung enthält die Tabelle unter 2.5.

Manchmal erweist sich die Verwendung von Signierverfahren auch aus anderen Erwägungen als sinnvoll. Die Signatur eines Dokumentes als obligatorische Voraussetzung für eine elektronische Bestellung der Sperrgutabfuhr kann notwendig sein, um die Identität der Betroffenen zweifelsfrei sicherzustellen und einer Verbreitung unrichtiger Daten über die Betroffenen, wie etwa bei scherzhaften Massenbestellungen unter einem falschen Namen, vorzubeugen. Zwar ist dies auch derzeit per Telefon möglich. Die unsichere Identifizierung der anrufenden Person ist jedoch auch der angerufenen Person bekannt. Demgegenüber lässt sich im Internet der tausendfache Versand einer E-Mail unter einer Schein-Identität mit wenigen Mausclicks initiieren!

2.5 Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

Die nachfolgende Tabelle soll einer ersten Orientierung über den Umfang der erforderlichen technischen und organisatorischen Maßnahmen dienen. Sie weist auf den Zusammenhang hin, der je nach der konkreten Datenverarbeitungssituation im aktuellen Verwendungszusammenhang entsprechend der unterschiedlichen Sensitivität der Daten unterschiedliche technische und organisatorische Maßnahmen fordert.

Die Anwendung der Tabelle darf nicht schematisch erfolgen. Die Einordnung der einzelnen Daten hängt entscheidend von dem Sachzusammenhang ab, in dem diese Daten verarbeitet werden. Wegen der Kontextabhängigkeit der Sensitivität von Daten müssen besondere Risiken individuell berücksichtigt werden. Sind die Daten eines Datensatzes unterschiedlichen Stufen zuzuordnen, so sind jeweils für den genannten Datensatz die Anforderungen der höchsten Stufe für das einzelne Datum zu wählen. Ebenso wenig darf die Tabelle genutzt werden, um sich der Verpflichtung zu entziehen, ein ausreichendes Sicherheitskonzept zu erstellen.

Die öffentlichen Stellen haben zu gewährleisten, dass – verglichen mit konventionellen Formen des Austausches von Informationen – durch die neuen Kommunikationswege nicht zusätzliche Beeinträchtigungen des Grundrechts

Kategorien personenbezogener Daten	**Technische und organisatorische Maßnahmen**	**Technische Umsetzung**
Kategorie 1: Personenbezogene Daten oder Verwendungszusammenhänge, die wegen ihrer Sensitivität in dem konkreten Datenverarbeitungszusammenhang einen besonderen Datenschutz erfahren müssen. Dieses Schutzniveau ist i. d. R. insbesondere bei Berufs- und Amtsgeheimnissen (z. B. Sozialdaten) und bei personenbezogenen Daten, die nach Art. 8 der EG-Datenschutzrichtlinie als besondere Kategorie eingestuft worden sind (z. B. Daten über die Gesundheit) zu fordern. Ferner personenbezogene Daten oder Verwendungszusammenhänge, deren Missbrauch zu einer Beeinträchtigung von weiteren Grundrechten oder in der Folge zu sonstigen besonders schwerwiegenden Nachteilen führen kann.	Es ist sicherzustellen, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Wahrung der Vertraulichkeit). Erforderlich sind außerdem Maßnahmen, die geeignet sind, dass personenbezogene Daten während der Verarbeitung unversehrt und vollständig bleiben (Integrität) sowie jederzeit ihrem Ursprung zugeordnet werden können (Authentizität).	Die Kommunikationspartnerinnen und Kommunikationspartner müssen eine hinreichende Verschlüsselung der Daten vornehmen und eine digitale Signatur einsetzen, die auf dem Signaturgesetz i. V. m. der Signaturverordnung basiert. An die Ausgestaltung der Sicherungsinfrastruktur und an die Verwendung der technischen Komponenten sind die hier beschriebenen besonderen Anforderungen zu stellen.

Kategorie 2: Personenbezogene Daten, deren Missbrauch in ihrem Verwendungszusammenhang geeignet ist, die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen nicht besonders gewichtig zu beeinträchtigen.	Es sind grundsätzlich die gleichen Maßnahmen wie in Kategorie 1 erforderlich. Allerdings sind an die Ausgestaltung der Sicherungsinfrastruktur keine besonderen (über einen geregelten RZ-Betrieb hinausgehenden) Anforderungen zu stellen. Betroffene und öffentliche Stellen können Zertifikate oder vergleichbare Authentifizierungsmaßnahmen nach eigenen festgesetzten Regeln verwenden.	Eine Umsetzungsmöglichkeit besteht darin, allgemein verbreitete Verschlüsselungs- und Signatursoftware einzusetzen. Notwendige Voraussetzung für einen vertrauenswürdigen Umgang mit einem derartigen Produkt ist die Einrichtung von Zertifizierungsstellen, bei denen die Bürgerinnen und Bürger ihren öffentlichen Schlüssel hinterlegen und digital bestätigen, also zertifizieren lassen können.
Kategorie 3: Personenbezogene Daten, die den Kategorien 1 und 2 nicht zugeordnet werden können.	Es sind Schutzmaßnahmen zu treffen, die einen sicheren Übertragungskanal zwischen den beteiligten Endsystemen mit ausreichender Verschlüsselung ermöglichen. Zusätzliche Maßnahmen sind dann erforderlich, wenn der Verwendungszusammenhang dies erfordert.	Eine Möglichkeit der Kommunikation öffentlicher Stellen mit Bürgerinnen und Bürgern über einen “sicheren Kanal” besteht darin, Secure Socket Layer einzusetzen. Secure Socket Layer (SSL) legt, wie der Name andeutet, eine zusätzliche Schicht zwischen die Transport-Ebene TCP/IP und die Anwendungsebene (HTTP, Telnet, FTP,...) einer Datenübertragung. Von "oben” gesehen ist sie transparent, d. h., die Anwendungsprogramme können ohne große Modifikation auf eine sichere Übertragung zugreifen.

24. September 2007

Arbeitskreis Medien[1]

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Viele Beschäftigte im öffentlichen Dienst haben heute die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener (beispielsweise Dritter, deren Namen in einer E-Mail genannt werden) bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a. Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber[2] so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b. Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c. Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Be-

[1] Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nicht-öffentlichen Bereich übertragen werden.

[2] Zur Vereinfachung bezeichnet „Arbeitgeber“ sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherren

quemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

d. Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

e. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Welche Maßnahmen dafür grundsätzlich in Betracht kommen, kann etwa der Anti-Spam-Studie des BSI[3] entnommen werden. Die auf dieser Grundlage denkbaren Lösungen unterscheiden sich sowohl hinsichtlich ihrer Eignung als auch hinsichtlich des Ausmaßes, in dem sie in die Persönlichkeitsrechte der Kommunikationspartner oder Dritter eingreifen. Daher sollte jede Stelle, bevor sie Maßnahmen zur Spam-Abwehr ergreift, eine schriftliche Konzeption hierfür erstellen, der zu entnehmen ist, dass unter den in Betracht kommenden Varianten die datenschutzfreundlichste gewählt wurde.

   Die Konzeption sollte dabei folgenden Grundsätzen Rechnung tragen:

   - Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.
   - Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
   - Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie über den Umgang mit den an sie gerichteten E-Mails selbst entscheiden können.

II. Dienstliche Nutzung

a. Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Telemedienrechts (vgl. § 11 Abs. 1 Nr. 1 Telemediengesetz, TMG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den jeweils einschlägigen, am Erforderlichkeitsmaßstab orientierten Vorschriften des Beamtenrechts sowie des BDSG bzw. der Landesdatenschutzgesetze.

b. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung

[3] www.bsi.de/literat/studien/antispam/antispam.pdf

und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c. Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verkehrsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d. Der Arbeitgeber darf die Nutzungs- und Verkehrsdaten der Personalvertretung, der Schwerbehindertenvertretung sowie der Frauen- bzw. Gleichstellungsbeauftragten u.ä. nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen – was überwiegend der Fall sein wird –, ist eine Auswertung dieser Daten unzulässig.

e. Eine Betriebs- oder Dienstvereinbarung kann nur dann als besondere Rechtsvorschrift angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung ausreichend und präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und sie das gesetzliche Schutzniveau nicht unterschreitet.

f. Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

g. Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren übrigem dienstlichen Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm seine Mitarbeiter jede ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten.

i. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen kann.

III. Private Nutzung

1. Allgemeines

a. Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Telemediendienste-Anbieter.

b. Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Telemediendienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c. Der Arbeitgeber ist gegenüber den Beschäftigten und den Absendern zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d. Es gelten die Regelungen der Telekommunikationsgesetzes, des Telemediengesetzes bzw. des Rundfunkstaatsvertrages.

e. Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Beschränkungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – unter Beteiligung des Personalrats eindeutig geregelt werden.

g. Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a. Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b. Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Fernmeldegeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines Web-Mail-Dienstes verweisen.

c. Wie bei der dienstlichen Nutzung (s. II.i.) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken führen kann.

Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d. Eine zentrale Spam-Filterung, bei der automatisch auf den Header oder Inhalte zugegriffen wird, darf nur mit Einwilligung des Empfängers erfolgen, da die Reichweite des Fernmeldegeheimnisses erst endet, wenn die E-Mail in seine vollständige Verfügungsgewalt gelangt ist. Auch dies ist als einschränkende Voraussetzung für die Erlaubnis zur privaten Nutzung (s. o., III.1.e) anzusehen und damit Bestandteil der Einwilligung. Die Einwilligung kann pauschal vorab erfolgen. Die Beschäftigten sind über die Art und Weise der Spam-Filterung, insbesondere über die dabei stattfindende Verarbeitung personenbezogener Daten, zu informieren.

e. Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.

Dipl.-Volkswirt Oliver Bauer, Dipl.-Kauffrau (FH) Beate Tenz

Informations- und Kommunikationstechnologie in Unternehmen

Ergebnisse für das Jahr 2007

Die weite Verbreitung und Nutzung von Informations- und Kommunikationstechnologie (IKT) in Unternehmen ist zu einem wesentlichen Faktor für Innovations- und Wettbewerbsfähigkeit geworden. Entsprechend ist die Durchdringung mit IKT ein wichtiger Impulsgeber für gesamtwirtschaftliches Wachstum und Beschäftigung, gerade in ressourcenarmen Ländern oder Wirtschaftsräumen wie der Europäischen Union (EU).

Die Erhebung zur Nutzung von IKT in Unternehmen liefert einen Überblick über die Ausstattung von deutschen Unternehmen mit modernen Informations- und Kommunikationstechnologien. Neben Informationen über die Verbreitung von Computern, Internet und Netzwerken bilden die verschiedenen Nutzungsaspekte moderner Informationstechnologien, wie etwa E-Government oder E-Commerce, einen zentralen Bestandteil der Studie.

In allen Mitgliedstaaten der Europäischen Union erfolgt eine methodisch harmonisierte Erhebung. So sind für Kernaussagen Zeitvergleiche und Vergleiche zwischen den einzelnen Ländern möglich.

Vorbemerkung

Der Europäische Rat von Lissabon hat im März 2000 beschlossen, Europa bis zum Jahr 2010 zum wettbewerbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum der Welt, mit mehr Arbeitsplätzen und besserem sozialen Zusammenhalt, auszubauen. Dazu wurde im Juni 2000 im portugiesischen Feira der Aktionsplan eEurope 2002 als ein integrierter Bestandteil der Lissabonner Strategie vereinbart. Im Juni 2002 verabschiedete der Europäische Rat auf dem Gipfel in Sevilla eEurope 2005 als Nachfolger dieses Aktionsplans. Die Bestrebungen der Europäischen Kommission, den Einsatz moderner Informations- und Kommunikationstechnologien zu fördern und damit wichtige Impulse für Wachstum und Beschäftigung in Europa zu geben, werden im Rahmen der Initiative „i2010: Informationsgesellschaft 2010“ fortgeführt, welche im Juni 2005 beschlossen wurde.

Zur Evaluierung der Aktionspläne und zur Durchführung eines gemeinsamen Benchmarking wurden zwischen 2002 und 2005 in fast allen Mitgliedstaaten der EU harmonisierte Piloterhebungen zur Nutzung von Informations- und Kommunikationstechnologie (IKT) in Unternehmen und privaten Haushalten durchgeführt.

Durch die Verordnung Nr. (EG) 808/2004 des Europäischen Parlaments und des Rates vom 21. April 2004 (Amtsbl. der EU Nr. L 143, S. 49) sind nun alle Mitgliedstaaten der Europäischen Union verpflichtet, jährlich ab 2006 für zunächst fünf Jahre statistische Ergebnisse für die Erstellung von Gemeinschaftsstatistiken über die Nutzung von IKT durch Unternehmen, Haushalte und Einzelpersonen zu liefern. Da die EG-Verordnung den nach dem Bundesstatistikgesetz geforderten Regelungsinhalt nicht vollständig abbildet, wurde mit dem Gesetz über die Statistik zur Informationsgesellschaft (InfoGesStatG) vom 22. Dezember 2005 (BGBl. I S. 3685) eine nationale Rechtsgrundlage geschaffen, auf deren Basis die Erhebungen „IKT in Unternehmen“ und „IKT in privaten Haushalten“ ab dem Jahr 2006 als reguläre Erhebungen in Zusammenarbeit mit den Statistischen Ämtern der Länder und mit Unterstützung des Statistischen Amtes der Europäischen Gemeinschaften (Eurostat) durchgeführt werden. Somit ist zumindest bis 2010 die Kontinuität der jährlichen Erhebungen gesichert.

Im Folgenden werden ausgewählte Ergebnisse der Erhebung für Deutschland aus dem aktuellen Berichtsjahr 2007 vorgestellt. Die Ergebnisse beziehen sich, wenn nicht anders erwähnt, auf den Monat Januar des Berichtsjahres. Mit Ausnahme des Landwirtschafts- und des Bergbausektors sind Unternehmen nahezu aller Wirtschaftszweige befragt worden. Der Finanzdienstleistungssektor wurde wegen seiner strukturellen Unterschiede zu den anderen Wirtschaftsbereichen in einer separaten Untersuchung mit reduziertem Fragеprogramm erfasst. Aus diesem Grund ist der Finanzdienstleistungssektor nicht in die Betrachtungen zum E-Commerce eingeschlossen.

1 Methodisches Konzept der Erhebung

Erhebungseinheiten und Stichprobenziehung

Die Erhebung zur Nutzung von IKT in Unternehmen 2007 wurde gemäß § 2 InfoGesStatG bei 20 000 Unternehmen und Einrichtungen zur Ausübung einer freiberuflichen Tätigkeit durchgeführt.

Erhebungseinheiten waren die Unternehmen und die Einrichtungen zur Ausübung einer freiberuflichen Tätigkeit aus den folgenden ausgewählten Wirtschaftsbereichen der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 1.1) gemäß der Verordnung (EWG) Nr. 3037/90 des Rates vom 9. Oktober 1990 (Amtsbl. der EG Nr. L 293, S. 1) in der zum Erhebungszeitpunkt gültigen Fassung:

- Abschnitt D: Verarbeitendes Gewerbe
- Abschnitt E: Energie- und Wasserversorgung
- Abschnitt F: Baugewerbe
- Abschnitt G: Handel, Instandhaltung und Reparatur von Kraftfahrzeugen und Gebrauchsgütern
- Abschnitt H: Gastgewerbe
- Abschnitt I: Verkehr und Nachrichtenübermittlung
- Abschnitt J: Kredit- und Versicherungsgewerbe
- Abschnitt K: Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen, Erbringung von unternehmensbezogenen Dienstleistungen
- Abteilung 92: Kultur, Sport und Unterhaltung
- Abteilung 93: Erbringung von sonstigen Dienstleistungen

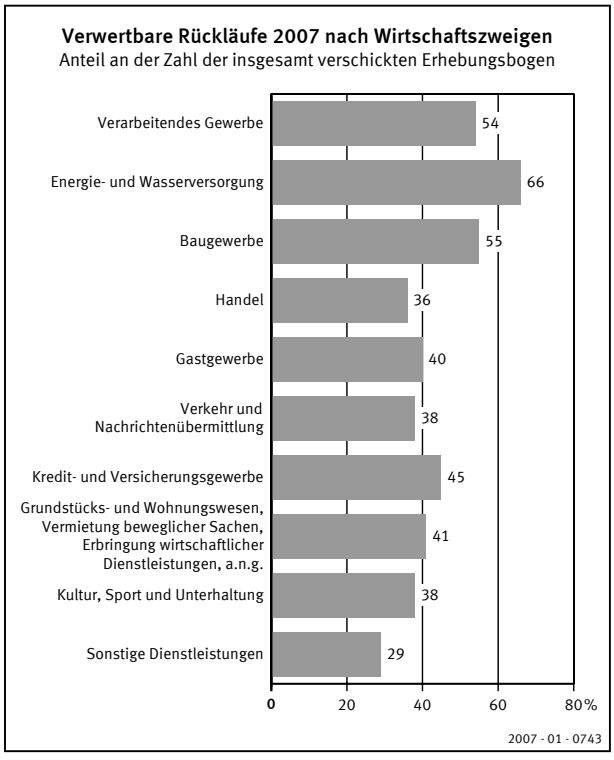
Zur Festlegung der Auswahlgesamtheit aller Erhebungseinheiten diente das bei den Statistischen Ämtern des Bundes und der Länder geführte Unternehmensregister. Aus der Grundgesamtheit des Unternehmensregisters mit Stand Dezember 2006 wurden die zu befragenden Erhebungseinheiten nach einem Auswahlplan mittels einer nach Bundesländern, Wirtschaftszweigen und Beschäftigtengrößenklassen geschichteten Zufallsstichprobe gezogen. Auswahleinheit war das einzelne Unternehmen. Es war zugleich Erhebungs- und Darstellungseinheit.

Insgesamt wurde eine Schichtung nach 21 Wirtschaftsbereichen, fünf Beschäftigtengrößenklassen und 12 Regionen zugrunde gelegt, was zu 1 260 Schichten führte. In jeder Schicht wurde eine separate Zufallsstichprobe gezogen. Die Schichten der Unternehmen mit 250 und mehr tätigen Personen sowie diejenigen Schichten, die auf Bundesebene nur sehr schwach besetzt waren, wurden als Totalschichten berücksichtigt. Das bedeutet, dass jedes darin befindliche Unternehmen angeschrieben wurde. Schichten, die im Verhältnis dazu sehr stark besetzt waren, sind in dem Umfang bei der Stichprobenziehung erfasst worden, wie es für eine gesicherte Ergebnisdarstellung in der angestrebten Tiefengliederung nötig erschien.

Die Befragung wurde in zwei aufeinanderfolgenden Wellen durchgeführt. Der Erstversand der Erhebungsunterlagen erfolgte im März 2007. Im Mai 2007 wurden alle Unternehmen, die bis dahin noch nicht geantwortet hatten, erneut angeschrieben und um die Teilnahme an dieser freiwilligen Erhebung gebeten.

Bis zum Beginn der Ergebnisaufbereitung sind an die Statistischen Landesämter und an das Statistische Bundesamt insgesamt 8 853 Erhebungsbogen mit verwertbaren Angaben zurückgesandt worden. Dies entspricht einer an der Zahl der verschickten Erhebungsbogen gemessenen Rücklaufquote von 44,3 %.

Schaubild 1



Die mit Abstand höchste Rücklaufquote (66 %) wies der Bereich Energie- und Wasserversorgung auf, gefolgt vom Baugewerbe (55 %) und Verarbeitenden Gewerbe (54 %, siehe Schaubild 1). Erheblich schlechter war das Antwortverhalten im Dienstleistungsbereich. Das Kredit- und Versicherungsgewerbe, für welches innerhalb des Dienstleistungssektors der stärkste Rücklauf verzeichnet werden konnte, kam lediglich auf eine Quote von 45 %. Am schlechtesten schnitt der Wirtschaftszweig der sonstigen Dienstleistungen ab: Hier antworteten nur rund drei von zehn angeschriebenen Unternehmen mit verwertbaren Angaben.

Ergebnisaufbereitung

Die Ergebnisaufbereitung aller plausibilisierten Daten fand im Statistischen Bundesamt statt. Es wurde das Verfahren der sogenannten gebundenen Hochrechnung eingesetzt. Unter Berücksichtigung des Wirtschaftszweiges und der Beschäftigtengrößenklasse der einzelnen Unternehmen wurden die Daten anhand der Ergebnisse folgender Quellen hochgerechnet:

- Kostenstrukturerhebung der Unternehmen des Verarbeitenden Gewerbes für den Abschnitt D der Wirtschaftszweigklassifikation NACE Rev. 1.1
- Kostenstruktur- und Investitionserhebung der Unternehmen in der Energie- und Wasserversorgung für den Abschnitt E
- Jahreserhebung im Baugewerbe für den Abschnitt F
- Jahreserhebung im Handel und Gastgewerbe für die Abschnitte G und H
- Unternehmensregister (Stand: Dezember 2006) für den Abschnitt J
- Strukturerhebung im Dienstleistungsbereich (Dienstleistungsstatistik) für die Abschnitte I und K der Wirtschaftszweigklassifikation
- Umsatzsteuerstatistik für die Abteilungen 92 und 93.

2 Ergebnisse für das Berichtsjahr 2007

Bevor auf die verschiedenen Nutzungsaspekte moderner Informations- und Kommunikationstechnologie und deren Nutzungsintensität durch Unternehmen näher eingegangen wird, soll einleitend zunächst die generelle Ausstattung von Unternehmen mit wesentlichen IKT-Gütern beleuchtet werden.

Rund vier von fünf Unternehmen in Deutschland setzten 2007 Computer in ihrem Geschäftsablauf ein. Bestimmend für die Nutzung von Computern ist dabei weniger die Branche, in der das jeweilige Unternehmen tätig ist, sondern vielmehr die Größe des Unternehmens. Da die Struktur der Unternehmen in den einzelnen hier betrachteten Branchen recht unterschiedlich war, wirkte sich dieser Bestimmungsfaktor auf die Ergebnisse nach Wirtschaftszweigen aus. Der auf den ersten Blick relativ niedrig erscheinende Anteil Computer nutzender Unternehmen von 82 % resultiert aus der zahlenmäßigen Dominanz der kleinen Unternehmen in Deutschland. So hatten zum Ende des Jahres 2006 etwa 91 % aller Unternehmen weniger als zehn Beschäftigte. Gerade in dieser Größenklasse ist die Ausstattung der Unternehmen mit PC mit einem Anteilswert von 78 % aber vergleichsweise gering, was sich erheblich auf das Gesamtergebnis niederschlägt. Demgegenüber ist bei 95 % der Unternehmen mit zehn und mehr Beschäftigten die Computernutzung Standard.

Der Anteil der Unternehmen mit PC-Nutzung lag 2007 auf dem Niveau der letzten Jahre. Dies lässt vermuten, dass bei der Ausstattung von Unternehmen mittlerweile ein gewisser Sättigungsgrad erreicht wurde. Unter dem Gesichtspunkt der Wettbewerbsfähigkeit haben vor allem die Unternehmen in den letzten Jahren den technologischen Nachholbedarf ausgeglichen, bei denen die Integration von Computern in den Geschäftsablauf betriebswirtschaftlich notwendig erschien. Andere Aspekte, wie etwa zu hohe Anschaffungs- und Wartungskosten, fehlende EDV-Kenntnisse oder einfach fehlender Bedarf mögen der Grund dafür sein, dass weiterhin insbesondere kleine Unternehmen auf den Einsatz von IKT verzichten.

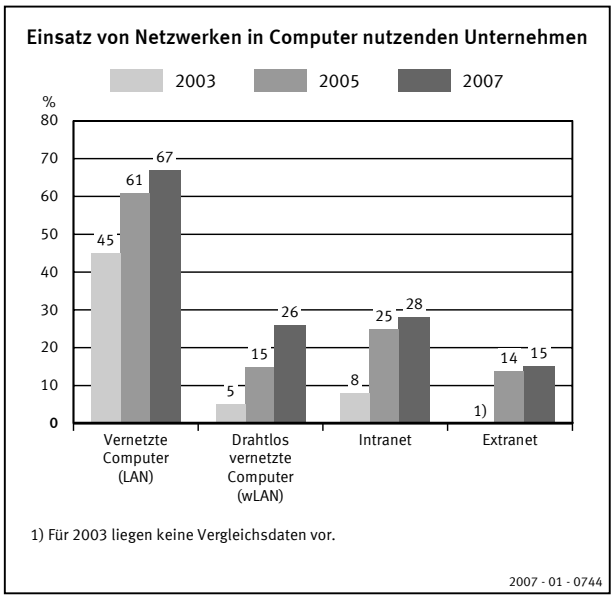
Die Analyse der Ergebnisse konzentriert sich daher mittlerweile nicht mehr rein auf den Ausstattungsgrad der Unternehmen mit IKT, vielmehr rückt die Frage nach der Adaption von IKT in den Mittelpunkt.

75 % der Unternehmen verbesserten Informationsfluss durch Einsatz von Netzwerken

Der einzelne, unvernetzte PC wird kaum noch im Geschäftsablauf eingesetzt. Netzwerke ermöglichen die gemeinsame Nutzung von wichtigen Ressourcen und den schnellen und unkomplizierten Zugriff auf notwendige Daten und Informationen. Die Informationsversorgung kann so verbessert werden und Prozesse können schneller und effizienter ablaufen. Im Jahr 2007 verfügten bereits 75 % aller Computer nutzenden Unternehmen über derartige Netzwerke (2006: 67 %, 2005: 61 %, 2004: 54 %, 2003: 45 %). Die einfachste Form von Netzwerken, sogenannte LANs (Local Area Networks), nutzten 67 % der Unternehmen mit Computereinsatz (siehe Schaubild 2). Hierbei werden Rechner auf kurze Entfernungen, zum Beispiel innerhalb eines Gebäudes, miteinander vernetzt. Bei 26 % der Unternehmen erfolgte die Datenübertragung kabellos per Funk, hier kam ein wLAN (wireless LAN) zum Einsatz.

Weiter entwickelte Arten von Netzwerken sind das Intranet und das Extranet, die auf den gleichen Techniken wie das Internet basieren. Während das Intranet als unternehmensinterne Informationsplattform nur Nutzern innerhalb dieser Organisation zugänglich ist, können auf das Extranet auch registrierte externe Benutzer zugreifen, wie etwa Geschäftspartner oder Großkunden. Im Jahr 2007 war in 28 % der Computer nutzenden Unternehmen ein Intranet vorhanden und immerhin 15 % der Unternehmen ermöglichten exter-

Schaubild 2



nen Nutzern den Zugriff auf unternehmensinterne Daten über ein Extranet.

Auch bei den Netzwerken zeigt sich insgesamt, dass mit zunehmender Größe der Unternehmen die Nutzungsintensität steigt. So setzten 90 % der Unternehmen mit 20 bis 49 Beschäftigten 2007 ein Netzwerk ein, bei den Unternehmen mit 50 bis 249 Beschäftigten waren es 94 % und bei den Großunternehmen mit 250 und mehr Beschäftigten 99 %. In der Größenklasse 1 bis 19 Beschäftigte waren immerhin bei 62 % der Unternehmen die Computer vernetzt.

Unternehmen nutzten Netzwerke zur Automatisierung von internen Prozessen

Die Verfügbarkeit von Netzwerken ermöglicht es den Unternehmen zunehmend, spezielle EDV-Anwendungen einzusetzen, die die Automatisierung der Bearbeitung von Bestellungen und Rechnungen sowie die Durchführung von Einkäufen erleichtern. Im Jahr 2007 setzten 41 % aller Unternehmen, die Computer nutzten, ein IT-System für die Auftragsbearbeitung ein (2004: 31 %). Solch ein EDV-Verfahren ist häufig mit anderen unternehmensinternen Programmsystemen verbunden. Es handelt sich dabei überwiegend um Abrechnungs- und Zahlungssysteme (bei 70 %) sowie um IT-Systeme zur Steuerung von Produktion, Logistik und Dienstleistungen (bei 46 %). Eine Verknüpfung mit betriebsinternen Systemen für die Nachbestellung von Ersatzteilen fand dagegen nur bei 19 % der Unternehmen statt.

Des Weiteren bilden Netzwerke die Grundlage für den Einsatz komplexer Softwaresysteme, welche die Unternehmen einerseits bei der effizienten Ressourcenplanung unterstützen können und andererseits auch eine strukturierte und gegebenenfalls automatisierte Erfassung sämtlicher Kundenkontakte sowie die Analyse der Daten (z. B. für Kundenbewertungen, Marktsegmentierungen) ermöglichen. So setzten im Jahr 2007 gut 12 % der Computer nutzenden Unternehmen eine firmeninterne ERP(Enterprise Resource Planning)-Software ein, um Informationen über Einkäufe und Verkäufe zwischen einzelnen Abteilungen, zum Beispiel Finanz-, Planungs- und Marketingabteilung, auszutauschen. 38 % der Unternehmen nutzten im Jahr 2007 eine CRM(Customer Relationship Management)-Software, um Kundendaten zu erfassen, zu speichern und anderen Unternehmensbereichen zur Verfügung zu stellen. 19 % der Unternehmen nutzten diese Software, um Kundendaten zu Marketingzwecken zu analysieren.

Acht von zehn Unternehmen in Deutschland haben Zugang zum Internet

Das Internet hat die Kommunikationsprozesse bei geschäftlichen Beziehungen nachhaltig verändert und ist zur grundlegenden Infrastruktur der Telekommunikation geworden. Einen Zugang zum Internet besaßen im Jahr 2007 etwa 77 % der in Deutschland ansässigen Unternehmen (2006: 79 %, 2005 und 2004: 78 %, 2003: 74 %, 2002: 62 %). Die Entwicklung zeigt, dass sich die Unternehmen in den vergangenen Jahren den technologischen Entwicklungen und den veränderten globalen Rahmenbedingungen angepasst und ihr Unternehmen mit dem World Wide Web vernetzt haben, um die vielfältigen Potenziale des Internets zu nutzen.

Nach wie vor gilt, dass mit zunehmender Größe der Unternehmen die Nutzung des Internets stärker verbreitet ist. Im Jahr 2007 hatten 75 % der Unternehmen mit weniger als 20 Beschäftigten einen Internetanschluss. In der Größenklasse von 20 bis 49 Beschäftigten lag der Anteil bei 93 %, in Unternehmen mit 50 und mehr Beschäftigten schon bei 99 %.

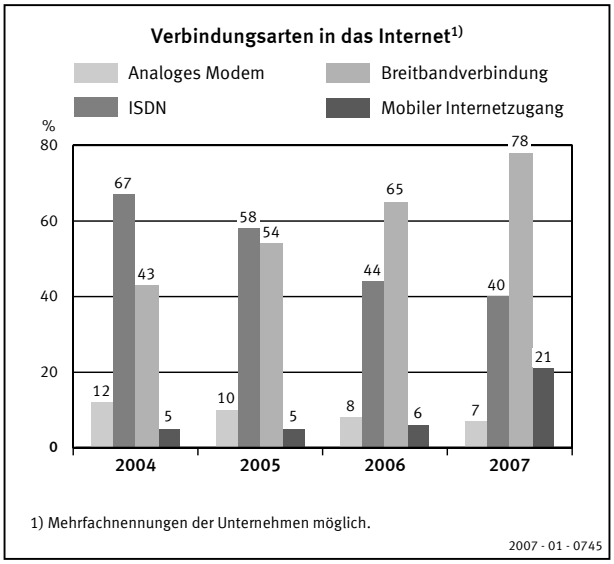
78 % nutzten Breitbandverbindung

Während die Zahl der Unternehmen, die einen Zugang zum Internet besitzen, seit dem Jahr 2004 bei einem Anteil von knapp unter 80 % stagniert, entwickeln sich Breitbandzugänge zur vorherrschenden Zugangsart zum Internet. Viele Internetanwendungen lassen sich nur mit einem Breitbandanschluss nutzen. Hatten im Jahr 2004 nur 43 % der Unternehmen einen Breitbandzugang, so nutzten im Jahr 2007 bereits vier von fünf Unternehmen (78 %) eine DSL- oder andere Breitbandverbindung (siehe Schaubild 3). Damit hat die Verwendung breitbandiger Anschlusstechnologien in Unternehmen von 2004 bis 2007 um 35 Prozentpunkte zugenommen. Demgegenüber ist die Nutzung von ISDN-Verbindungen im Vergleich zu 2004 um 27 Prozentpunkte zurückgegangen. Jedoch lässt sich auch erkennen, dass ISDN-Verbindungen noch nicht vollständig durch Breitbandverbindungen substituiert worden sind, sondern dass vielmehr in vielen Unternehmen noch beide Verbindungsarten existieren. Auch das analoge Modem ist noch nicht komplett vom Markt verschwunden. Immerhin gingen 2007 noch 7 % der Unternehmen teilweise über ein analoges Modem in das Internet. Die immer noch relativ hohe Zahl an ISDN- und Modem-Nutzern kann als Indiz dafür gewertet werden, dass die Verfügbarkeit von Breitbandanschlüssen noch nicht restlos in allen Regionen Deutschlands gewährleistet ist.

Immer mehr Unternehmen verfügen zusätzlich über einen mobilen Internetzugang, beispielsweise mittels GPRS oder

UMTS. Der Anteil der Unternehmen mit mobilem Anschluss ist gegenüber dem Vorjahr um über 15 Prozentpunkte auf 21 % bei der Erhebung 2007 gestiegen. Ein mobiler Internetzugang ermöglicht den Unternehmen ein noch flexibleres Arbeiten und einen effektiven Ressourceneinsatz. Die Nutzung des Internets ist nicht mehr lokalisiert, vielmehr kann von jedem Ort der Welt auf alle benötigten Daten im Unternehmen zugegriffen werden. Schaffte der Einsatz von IKT anfangs neue Beschäftigungsmodelle wie Telearbeit – im Jahr 2006 gewährleisteten 18 % der Computer nutzenden Unternehmen ihren Beschäftigten den externen Zugriff auf unternehmensinterne IT-Systeme – ist durch den mobilen Internetzugang mittlerweile auch ein Zugriff „von unterwegs", beispielsweise auf Geschäftsreisen, möglich.

Schaubild 3

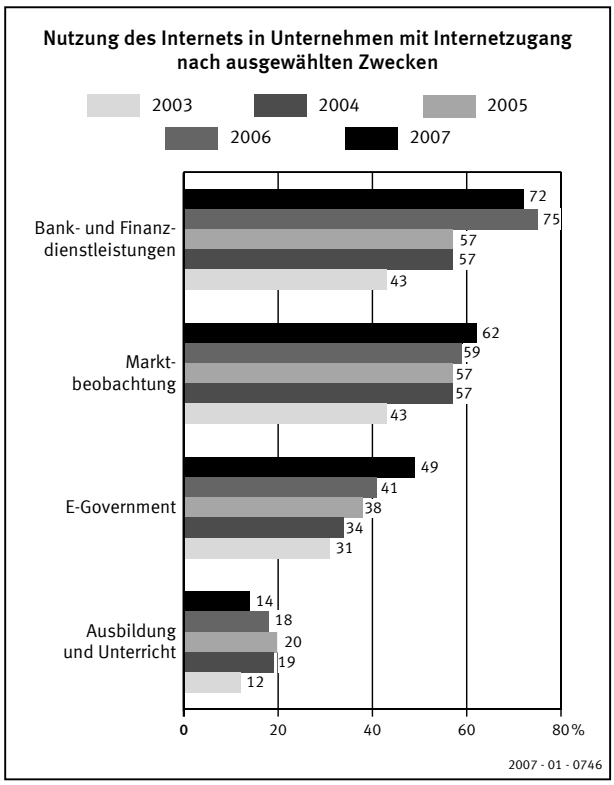


Unternehmen nutzten das Internet vorrangig zum Online-Banking

Das Internet mit seinen verschiedenen Möglichkeiten wird in Unternehmen in unterschiedlicher Art und Weise sowie auch in unterschiedlicher Intensität genutzt (siehe Schaubild 4). Vorrangig wurde es im Jahr 2007 weiterhin für die Inanspruchnahme von Bank- und Finanzdienstleistungen eingesetzt. 72 % der Unternehmen mit Internetzugang nutzten diese Möglichkeit, insbesondere auch kleinere Unternehmen mit weniger als 50 Beschäftigten. Unternehmen aus dem Kreditgewerbe (92 %) und aus dem Bereich Datenverarbeitung und Datenbanken (87 %) tätigten am häufigsten ihre Bank- und Finanzgeschäfte online.

Das Internet zählt darüber hinaus zu einer wichtigen Informationsquelle für die Marktbeobachtung. 62 % der Unternehmen nutzten 2007 das Internet, um Kenntnisse und Informationen zu Preisen, Produkten und Angeboten von Wettbewerbern zu gewinnen. Im Kreditgewerbe waren es sogar 85 % der Unternehmen. Bei großen Unternehmen war die Marktbeobachtung sogar der Hauptzweck der Internetnutzung. 81 % der Unternehmen mit 250 und mehr Beschäftigten bezogen im Jahr 2007 marktrelevante Informationen

Schaubild 4



über das Internet, während nur 66 % dieser Unternehmen das Internet für Bank- und Finanzdienstleistungen nutzten.

Fast jedes zweite Unternehmen nutzte Online-Angebote der öffentlichen Hand

Elektronische Behördendienste leisten einen wesentlichen Beitrag zur Verwaltungsmodernisierung und stellen einen Standort- und Wirtschaftsfaktor für einzelne Länder, Kommunen und für Deutschland insgesamt dar. Durch die Vereinfachung und Standardisierung von Vorgängen werden Bürgerinnen und Bürger und die Wirtschaft von bürokratischem Aufwand entlastet und Übermittlungsfehler reduziert. Gleichzeitig entstehen auf beiden Seiten Kosten- und Zeitersparnisse. Die Dienstleistungen der öffentlichen Hand sind zudem durch das Internet 24 Stunden am Tag von vielen Orten aus zugänglich.

Der Bund arbeitet seit dem Jahr 2000 daran, internetfähige Dienstleistungen der Bundesverwaltung online zu stellen. Im Rahmen der Initiative „BundOnline 2005" wurden bis zum April 2006 insgesamt 444 Anwendungen im Internet verfügbar gemacht. Die Bemühungen des Bundes, Verwaltungsleistungen online bereitzustellen, werden im Rahmen des Programms „E-Government 2.0" bis 2010 fortgeführt. Bundesländer und Kommunen bauen zudem mit eigenen Plänen ihr Online-Angebot aus. So verfügt mittlerweile eine Vielzahl an Landesbehörden und Kommunen über einen eigenen Internetauftritt und verschiedene Online-Services.

Im Juni 2003 beschlossen Bund und Länder darüber hinaus die E-Government-Strategie „Deutschland Online" mit

dem Ziel, zentrale ebenenübergreifende E-Government-Vorhaben von Bund, Ländern und Kommunen zu bündeln. Auf europäischer Ebene wurde im Jahr 2006 gleichfalls ein E-Government-Aktionsplan verabschiedet, welcher Bestandteil der „i2010: Informationsgesellschaft 2010"-Initiative für Wachstum und Beschäftigung in der Informationsgesellschaft der Europäischen Gemeinschaft ist.

Die Nutzung von E-Government wie auch das Angebot entsprechender Dienstleistungen der Verwaltung ist in den letzten Jahren stetig gestiegen. Immer mehr Unternehmen in Deutschland nutzen die Möglichkeit, ihre Behördenangelegenheiten online zu erledigen. Im Jahr 2007 griffen rund 49 % der Unternehmen mit Internetzugang auf Online-Dienstleistungen der öffentlichen Hand zurück. Damit ist der Anteil der E-Government-Nutzer bei den Unternehmen mit Internetzugang im Vergleich zu 2003 um 18 Prozentpunkte gestiegen. Betrachtet man alle Unternehmen in Deutschland, so beträgt der Anteil der E-Government-Nutzer 38 %.

Am häufigsten kommunizierten die Unternehmen mit der öffentlichen Verwaltung über das Internet, um Formulare herunterzuladen (81 %) und um Informationen einzuholen (73 %). 71 % der Unternehmen sandten zudem die ausgefüllten Formulare direkt über das Internet an die zuständige Behörde zurück und 16 % gaben bei einer elektronischen Ausschreibung online ein Angebot ab.

82 % der Unternehmen nutzten ihre Website zur Vermarktung der eigenen Produkte

Unternehmen können durch die Nutzung des Internets nicht nur Geschäftsprozesse automatisieren und optimieren, sondern sich auch regional oder weltweit über eine eigene Website präsentieren und Kunden akquirieren.

Immer mehr Unternehmen in Deutschland nutzen die Chance, ihr Unternehmen mit seinen Produkten und Dienstleistungen weltweit darzustellen. 62 % der Unternehmen mit Internetzugang verfügten im Jahr 2007 über eine eigene Internetpräsenz (2006: 58 %, 2005 und 2004: 59 %, 2003: 40 %, 2002: 33 %). Damit ist der Anteil der Unternehmen mit eigener Website im Vergleich zu 2002 deutlich – um 29 Prozentpunkte – gestiegen. Über die Hälfte der kleineren Unternehmen (58 %) mit weniger als 20 Beschäftigten und Internetzugang hatte im Jahr 2007 eine Website. Bei den Unternehmen mit 20 bis 49 Beschäftigten lag dieser Anteil bei 81 %, bei den Unternehmen mit 50 bis 249 Beschäftigten waren es sogar 87 %. Von den Großunternehmen mit 250 und mehr Beschäftigten verfügten 86 % über eine eigene Internetpräsenz.

Am meisten verbreitet waren Websites in den Branchen Hotellerie (92 %), Datenverarbeitung und Datenbanken (89 %), Fahrzeugbau (85 %) sowie im Bereich Kultur, Sport und Unterhaltung (89 %).

Die Website diente den Unternehmen in erster Linie zur Vermarktung der eigenen Produkte. 82 % der Unternehmen mit eigener Website nutzten diese im Jahr 2007 für Marketingzwecke. 78 % der Unternehmen stellten auf ihrer Website Kundenserviceleistungen bereit und 32 % verfolgten damit das Ziel, den Kunden einen leichteren Zugang zu Produktkatalogen und Preislisten zu ermöglichen.

Knapp die Hälfte aller Unternehmen in Deutschland beteiligte sich am elektronischen Handel über das Internet

Vor dem Hintergrund dieser günstigen infrastrukturellen Voraussetzungen tätigten im Jahr 2006 rund 44 % aller in Deutschland ansässigen Unternehmen Einkäufe oder Verkäufe über das Internet. Damit ist dieser Anteil gegenüber 2003 weiter gestiegen (+4 Prozentpunkte). Allerdings hat die Größe des Unternehmens einen erheblichen Einfluss auf die Nutzung des weltweiten Netzes als Beschaffungs- oder Vertriebskanal. So beteiligten sich 2006 nur rund 42 % der Unternehmen mit weniger als 20 Beschäftigten aktiv am E-Commerce über das Internet. In der Größenklasse von 20 bis 49 Beschäftigten lag dieser Anteil bei 60 % und in der Größenklasse von 50 bis 249 Beschäftigten bei 63 %. Von den Unternehmen mit 250 und mehr Mitarbeitern kauften oder verkauften 2006 bereits sieben von zehn Unternehmen (69 %) Waren oder Dienstleistungen über das Internet.

Werden als Basis nur diejenigen Unternehmen zugrunde gelegt, die über einen Internetzugang verfügten, so lag der Anteil der Unternehmen, die sich am E-Commerce beteiligten, bei 58 % (2003: 52 %). Dieser Wert variiert jedoch stark, wenn zusätzlich die Art der eingesetzten Internetverbindung berücksichtigt wird. Von allen Internet nutzenden Unternehmen, die über eine Breitbandverbindung online gingen, partizipierten 64 % am elektronischen Handel. Demgegenüber betrug der entsprechende Anteil bei den Unternehmen, die ausschließlich über Modem oder ISDN auf das Internet zugriffen, lediglich 37 %.

Anteil der Unternehmen mit Online-Einkäufen von 2003 bis 2006 um 5 Prozentpunkte gestiegen

42 % aller Unternehmen machten im Jahr 2006 von der Möglichkeit Gebrauch, Waren oder Dienstleistungen im Internet zu bestellen (2003: 37 %); bei Unternehmen mit Internetzugang waren es 55 % (2003: 48 %) (siehe Schaubild 5). Auch hierbei zeigt sich deutlich, dass mit zunehmender Beschäftigtenzahl der Unternehmen das Internet häufiger als Beschaffungskanal genutzt wird: So orderten 2006 rund 65 % (2003: 53 %) der Unternehmen mit 250 und mehr Beschäftigten und Internetzugang Waren oder Dienstleistungen online, bei Unternehmen mit weniger als 20 Mitarbeitern lag der Anteil bei 54 % (2003: 47 %).

Wertmäßig machten 2006 die Online-Einkäufe von Unternehmen mit Internetzugang rund 8 % ihrer Gesamtaufwendungen aus. Bei dieser Betrachtungsweise hat die Unternehmensgröße allerdings den umgekehrten Einfluss: So betrug der Anteil der auf Online-Bestellungen zurückgehenden Aufwendungen an den Gesamtaufwendungen bei den Internet nutzenden Unternehmen mit weniger als 20 Beschäftigten etwa 13 %. In der Größenklasse von 20 bis 49 Mitarbeitern

Schaubild 5

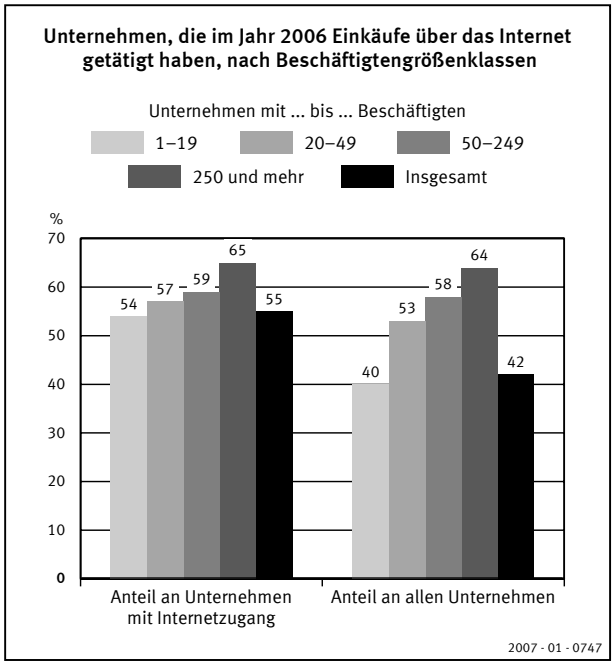
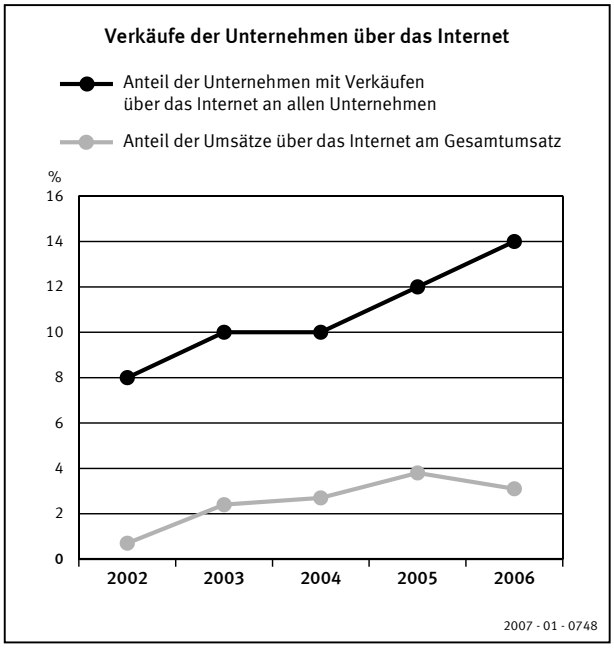


Schaubild 6



lag dieser Wert sogar bei 15 %. In den Größenklassen von 50 bis 249 sowie 250 und mehr Beschäftigten gingen dagegen mit 9 bzw. 6 % deutlich weniger der getätigten Aufwendungen auf Online-Einkäufe zurück.

Vertriebsweg Internet für Hotellerie und Beherbergungsgewerbe besonders attraktiv

Wird die Betrachtung auf die Unternehmen fokussiert, die Waren oder Dienstleistungen über das weltweite Netz verkaufen, so ist der Anteil von Unternehmen mit Online-Verkäufen im Zeitraum von 2002 bis 2006 um 6 Prozentpunkte gestiegen. Damit veräußerten im Jahr 2006 etwa 14 % aller Unternehmen in Deutschland ihre Produkte auch online (siehe Schaubild 6). Werden hierbei nur die Unternehmen mit Internetzugang berücksichtigt, so lag der Anteil der Unternehmen mit Online-Verkäufen bei 18 %.

Die Nutzung des Internets für den Verkauf von Waren und Dienstleistungen variiert stark mit der Größe der Unternehmen und dem Wirtschaftszweig: 31 % der Unternehmen mit 250 und mehr Beschäftigten und Internetzugang nutzten 2006 das World Wide Web als Vertriebskanal. In den Größenklassen mit 20 bis 49 Beschäftigten und mit 50 bis 249 Beschäftigten waren es 29 bzw. 27 % der Unternehmen. Demgegenüber verkauften nur 17 % der Internet nutzenden Unternehmen mit weniger als 20 Beschäftigten ihre Waren oder Dienstleistungen online.

Tabelle 1: Unternehmen mit Verkäufen über das Internet 2006 nach Wirtschaftszweigen
Prozent

Wirtschaftszweig	Anteil der Unternehmen mit Internetverkäufen an		Anteil des Umsatzes über Internet am Gesamtumsatz	
	allen Unternehmen	Unternehmen mit Internetzugang	aller Unternehmen	der Unternehmen mit Internetverkäufen
Untersuchte Wirtschaftsbereiche insgesamt	14	18	3	10
Verarbeitendes Gewerbe	18	21	2	7
Energie- und Wasserversorgung	6	6	2	11
Baugewerbe	9	11	1	6
Kraftfahrzeughandel; Instandhaltung und Reparatur von Kraftfahrzeugen; Tankstellen	16	19	3	10
Handelsvermittlung und Großhandel	22	26	4	11
Einzelhandel	18	26	4	10
Hotellerie und Beherbergungsgewerbe	49	63	13	17
Gastronomie, Kantinen und Caterer	6	18	1	9
Verkehr	12	16	6	16
Nachrichtenübermittlung	9	12	4	6
Grundstücks- und Wohnungswesen	6	9	1	13
Vermietung beweglicher Sachen ohne Bedienungspersonal	–	–	–	–
Datenverarbeitung und Datenbanken	27	28	6	22
Forschung und Entwicklung	2	4	1	26
Erbringung von wirtschaftlichen Dienstleistungen, a. n. g.	8	9	2	12
Kultur, Sport und Unterhaltung	32	35	15	32
Erbringung von sonstigen Dienstleistungen	11	18	3	19

Mit Blick auf die einzelnen Wirtschaftszweige tätigten 2006 Unternehmen aus der Hotellerie und dem Beherbergungsgewerbe am häufigsten Verkäufe über das Internet. In diesem Bereich setzten 63 % der Unternehmen mit Internetzugang ihre Leistungen auch online ab (siehe Tabelle 1). In den Bereichen Kultur, Sport und Unterhaltung sowie Datenverarbeitung und Datenbanken hatte der Absatzkanal Internet ebenfalls eine überdurchschnittlich hohe Bedeutung: 35 bzw. 28 % der Internet nutzenden Unternehmen dieser Branchen verzeichneten für 2006 Online-Verkäufe. Im Groß- und Einzelhandel nutzte 2006 immerhin rund jedes vierte Unternehmen das Internet, um Güter zu vertreiben.

Wenn auch der Online-Vertrieb für einzelne Unternehmen durchaus eine wesentliche oder sogar unerlässliche Säule im Absatzgefüge darstellt, haben Online-Verkäufe – trotz der steigenden Zahl von Unternehmen, die das Internet für den Verkauf von Waren oder Dienstleistungen nutzten – auf Wirtschaftszweigebene nur einen geringen Anteil am Gesamtumsatz. Insgesamt entfielen 2006 nur rund 3,1 % des Gesamtumsatzes aller Unternehmen in Deutschland auf den Vertriebskanal Internet (2005: 3,8 %, 2004: 2,7 %, 2003: 2,4 %). Lediglich im Wirtschaftszweig Kultur, Sport und Unterhaltung sowie in der Hotellerie und im Beherbergungsgewerbe war das wertmäßige Volumen der Internetverkäufe mit Anteilen von 15 bzw. 13 % am gesamten Umsatz aller in diesen Branchen tätigen Unternehmen überdurchschnittlich hoch (siehe Tabelle 1).

Nur rund jedes vierte Unternehmen gewährleistete Online-Kunden eine verschlüsselte Datenübertragung

Ein wichtiges Thema beim elektronischen Handel ist Sicherheit und Datenschutz. Grundsätzlich werden alle Daten im Internet im Klartext übertragen, das heißt auf ihrem Weg von einem Rechner zum anderen können diese Daten von Dritten verhältnismäßig einfach mitgelesen, geändert und sogar gelöscht werden. Gerade aber im Online-Bestellprozess, bei dem sensible Kundeninformationen wie Kreditkarten-Daten übermittelt werden, sollten die online transportierten Angaben vor unerlaubtem Mitlesen, Kopieren oder Fälschen geschützt werden. Mit Hilfe von Verschlüsselungsprotokollen wie SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) können Datenübertragungen im Internet gesichert werden.

Im Januar 2007 gewährleisteten lediglich 28 % der Unternehmen mit Online-Verkäufen ihren Kunden eine verschlüsselte Datenübertragung und damit einen gesicherten Bestellprozess. Der Einsatz von Verschlüsselungsprotokollen für über das Internet eingehende Bestellungen nimmt aber mit zunehmender Größe der Unternehmen zu. Von den Unternehmen mit weniger als 20 Beschäftigten sicherten 26 % die Internetbestellungen ihrer Kunden mittels Datenverschlüsselung. In der Größenklasse von 20 bis 49 Beschäftigten lag dieser Anteil bei 29 %, in der Größenklasse von 50 bis 249 Beschäftigten bei 41 %. Immerhin jedes zweite Unternehmen mit 250 und mehr Mitarbeitern nutzte im Januar 2007 Verschlüsselungsprotokolle für eingehende Online-Bestellungen, um einen Missbrauch der übermittelten Kundendaten zu verhindern.

Elektronischer Handel über EDI in Deutschland wenig verbreitet

Neben dem Internet können Unternehmen auch über andere elektronische Netzwerke E-Commerce betreiben. Dabei handelt es sich beispielsweise um Festverbindungen. Diese Netzwerke haben einen wesentlich geringeren Verbreitungsgrad als das Internet und haben sich vorwiegend in festen Kunden-Lieferanten-Beziehungen zwischen Unternehmen etabliert.

Im Jahr 2006 nutzten rund 3,6 % aller Unternehmen in Deutschland EDI (Electronic Data Interchange) oder andere direkte Verbindungen zum Kauf oder Verkauf von Waren und Dienstleistungen (2005: 3,5 %, 2004: 2,4 %). Dabei spielen diese Direktverbindungen noch eher als Beschaffungskanal eine Rolle: Während 3 % aller Unternehmen Waren oder Dienstleistungen über EDI einkauften, nutzten nur rund 1 % aller Unternehmen diese Verbindung für Verkäufe. Allerdings wickelten diese Unternehmen vom Umsatzvolumen her einen bedeutenden Anteil über EDI ab: Rund 32 % des Gesamtumsatzes dieser Unternehmen resultierte aus Verkäufen über EDI oder andere computergestützte Netzwerke.

Mehr als jeder zweite Beschäftigte nutzte regelmäßig einen PC während der Arbeitszeit

Die zunehmende Implementierung von IKT in die Geschäftsprozesse von Unternehmen führt dazu, dass auch die Zahl der Beschäftigten, die mit diesen neuen Technologien arbeiten, steigt. Um die positiven Effekte und Potenziale von IKT in Unternehmen realisieren zu können, müssen daher nicht nur die entsprechenden Technologien vorhanden sein, sondern es ist auch entsprechend ausgebildetes Personal und Know-How erforderlich.

Bereits jetzt kommt mehr als jeder zweite Arbeitnehmer im täglichen Arbeitsleben nicht mehr ohne den Einsatz von Computern aus. So arbeiteten im Jahr 2007 etwa 57 % der Beschäftigten in Deutschland bei ihrer beruflichen Tätigkeit mit Computern (siehe Schaubild 7). Damit ist der Anteil der Mitarbeiter, die einen PC nutzen, im Vergleich zu 2002 (46 %) um elf Prozentpunkte gestiegen.

Die Nutzung von Computern durch Beschäftigte variiert jedoch innerhalb der einzelnen Branchen deutlich. In dem stark technologiebasierten Wirtschaftszweig Datenverarbeitung und Datenbanken (98 %), aber auch im Kredit- und Versicherungsgewerbe (93 %) arbeiteten 2007 nahezu alle Mitarbeiterinnen und Mitarbeiter mit Computertechnik. Ebenfalls stark überdurchschnittlich wurden PC von Beschäftigten im Papier-, Verlags- und Druckgewerbe (75 %), bei Unternehmen der Energie- und Wasserversorgung (72 %) und bei Großhandelsunternehmen (71 %) genutzt. Im Gegensatz dazu arbeiteten im Gastgewerbe nur rund 18 % der tätigen Personen regelmäßig beruflich mit Computertechnik.

Schaubild 7

48 % aller Beschäftigten in Deutschland waren 2007 zudem an ihrer Arbeitsstätte mit einem Zugang zum Internet ausgestattet, das waren 19 Prozentpunkte mehr als im Jahr 2003. Da das Internet den Unternehmen immer vielfältigere Möglichkeiten bietet, Geschäftsprozesse zu beschleunigen und zu optimieren, ist auch die Ausstattung der einzelnen Mitarbeiter mit einem Zugang zum weltweiten Netz von immer größerer Bedeutung.

13 % aller Computer nutzenden Unternehmen beschäftigten IT-Fachkräfte

IT-Fachkräfte sind in Unternehmen verantwortlich für die Planung, Einrichtung, Wartung und Administration von Systemen und Netzwerken. Sie sind darüber hinaus zuständig für die Anwendungs-, Datenbank- und Softwareentwicklung sowie die Beschaffung, Installation und Anpassung von Hard- und Software. Im Jahr 2007 beschäftigten 13 % der Unternehmen mit Computernutzung eigene IT-Fachkräfte (siehe Tabelle 2). Da in größeren Unternehmen der Durchdringungsgrad mit IKT höher ist und in der Regel komplexere IT-Systeme zum Einsatz kommen als in kleineren Unternehmen, steigt mit zunehmender Beschäftigtenzahl auch die Zahl der Unternehmen, die über eigene IT-Fachkräfte, oft sogar ganze IT-Abteilungen, verfügen. Diese Tendenz zeigt sich über alle Wirtschaftsbereiche hinweg. So waren im Jahr 2007 in rund 79 % der Computer nutzenden Unternehmen mit 250 und mehr Beschäftigten IT-Fachkräfte angestellt. In der Größenklasse mit weniger als 20 Beschäftigten lag dieser Anteil hingegen nur bei 9 %.

Im Jahr 2006 stellten insgesamt 5 % aller Computer nutzenden Unternehmen in Deutschland IT-Fachkräfte ein oder strebten zumindest die Einstellung von IT-Fachkräften an. Von diesen Unternehmen gab rund die Hälfte (52 %) an, Schwierigkeiten bei der Gewinnung von Personal mit den zur Aufgabenerfüllung erforderlichen IT-Fachkenntnissen gehabt zu haben. 75 % dieser Unternehmen nannten die fehlenden Fachkenntnisse der Bewerber als Hürde für die Personalgewinnung. Für 64 % bereitete die fehlende Berufserfahrung der Bewerber Schwierigkeiten. Darüber hinaus äußerten 54 % der Unternehmen, dass die Bewerber zu hohe Gehaltsforderungen vorgebracht hätten, und ebenfalls 54 % gaben als Grund die mangelnde Zahl an Bewerbern für die ausgeschriebene Stelle an.

46 % der PC nutzenden Unternehmen greifen auf IT-Personal externer Anbieter zurück

Aus den im vorigen Absatz genannten Gründen sind daher für viele Unternehmen externe Anbieter eine gute Alternative zur Beschäftigung eigener IT-Fachkräfte. Gerade wenn die IT-Systeme nur sporadisch betreut werden müssen, ist die Beauftragung zum Beispiel einer Hard- oder Softwareberatung meist kostengünstiger. Im Jahr 2006 griffen 46 % der Unternehmen mit Computernutzung auf IT-Fachpersonal externer Anbieter zurück. Dieser Anteil steigt mit zunehmender Unternehmensgröße, auch wenn größere Unternehmen in der Regel häufiger selbst IT-Fachkräfte beschäftigten. So lag der Anteil der Unternehmen, die auf IT-Personal externer Anbieter zurückgriffen, bei Unternehmen mit weniger als 20 Beschäftigten bei 42 %, in der Größenklasse von 20 bis

Tabelle 2: Unternehmen mit Computernutzung und Beschäftigung von IT-Fachkräften 2007 nach Beschäftigtengrößenklassen und Wirtschaftszweigen

Prozent

Wirtschaftszweig	Insgesamt	Mit . . . bis . . . Beschäftigten			
		1 – 19	20 – 49	50 – 249	250 und mehr
Untersuchte Wirtschaftsbereiche insgesamt	13	9	24	44	79
Verarbeitendes Gewerbe	14	6	20	55	92
Energie- und Wasserversorgung	29	7	46	73	85
Baugewerbe	4	3	11	32	82
Handel	10	7	28	56	82
Gastgewerbe	5	4	10	23	77
Verkehr	6	3	13	40	80
Nachrichtenübermittlung	26	22	39	53	57
Kredit- und Versicherungsgewerbe	11	4	61	91	91
Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen, Erbringung von wirtschaftlichen Dienstleistungen, a. n. g.	17	15	46	70	73
Kultur, Sport und Unterhaltung	29	13	31	49	78
Erbringung von sonstigen Dienstleistungen	19	4	14	28	75

49 Beschäftigten bereits bei 70 % und in der Größenklasse von 50 bis 249 Beschäftigten bei 78 %. Von den Unternehmen mit 250 und mehr Beschäftigten griffen rund neun von zehn Unternehmen auf die IT-Expertise externer Anbieter zurück, obwohl in dieser Größenklasse auch 79 % der Unternehmen über eigenes IT-Fachpersonal verfügten.

Auszug aus Wirtschaft und Statistik

Herausgeber: Statistisches Bundesamt, Wiesbaden

Schriftleitung: Walter Radermacher
Präsident des Statistischen Bundesamtes
Verantwortlich für den Inhalt:
Brigitte Reimann,
65180 Wiesbaden
- Telefon: +49 (0) 6 11/75 20 86
- E-Mail: wirtschaft-und-statistik@destatis.de

Vertriebspartner: SFG Servicecenter Fachverlage
Part of the Elsevier Group
Postfach 43 43
72774 Reutlingen
Telefon: +49 (0) 70 71/93 53 50
Telefax: +49 (0) 70 71/93 53 35
E-Mail: destatis@s-f-g.com

Erscheinungsfolge: monatlich

Allgemeine Informationen über das Statistische Bundesamt und sein Datenangebot erhalten Sie:
- im Internet: www.destatis.de

oder bei unserem Informationsservice
65180 Wiesbaden

- Telefon: +49 (0) 6 11/75 24 05
- Telefax: +49 (0) 6 11/75 33 30
- www.destatis.de/kontakt

Rechtsanwalt Thomas Feil
www.recht-freundlich.de

IT-Recht · Fachanwalt für Arbeitsrecht

Private eMail- und Internetnutzung am Arbeitsplatz: Viele Fragen, wenig Antworten

Das Thema „Private eMail- und Internetnutzung am Arbeitsplatz“ wird in vielen Unternehmen eifrig diskutiert. Dennoch bestehen nach wie vor in Detailfragen Unsicherheiten in der rechtlichen Bewertung. Der nachfolgende Beitrag soll einen Überblick über den aktuellen Stand der Diskussion und über die aktuelle Rechtsprechung geben.

Das Machtwort der Bundesarbeitsrichter

Die Diskussion um die private Internet-Nutzung hat durch das Urteil des Bundesarbeitsgerichts vom 7. Juli 2005 (Az.: 2 AZR 581/04) eine neue Qualität bekommen. Die Bundesarbeitsrichter haben klargestellt, dass eine private Nutzung des Internets eine fristlose Kündigung rechtfertigen kann. Diese Auffassung war bis dato nicht von allen Arbeitsgerichten geteilt worden. In der Pressemitteilung des Bundesarbeitsgerichts lesen sich die wichtigsten Erkenntnisse der Entscheidung so:

> *Auch wenn der Arbeitgeber die Privatnutzung nicht ausdrücklich verboten hat, verletzt der Arbeitnehmer mit einer intensiven zeitlichen Nutzung des Internets während der Arbeitszeit zu privaten Zwecken seine arbeitsvertraglichen Pflichten. Das gilt insbesondere dann, wenn der Arbeitnehmer auf Internetseiten mit pornographischem Inhalt zugreift. Diese Pflichtverletzung kann ein wichtiger Grund zur fristlosen Kündigung des Arbeitsverhältnisses sein. Ob die Kündigung in einem solchen Fall im Ergebnis wirksam ist, ist auf Grund einer Gesamtabwägung der Umstände des Einzelfalls festzustellen.*

Das es auch anders gehen kann, musste ein Arbeitgeber vor dem Landesarbeitsgericht (LAG) Köln erfahren. Das Urteil der Kölner Richter vom 15.12.2003 (Az.: 2 Sa 816/03) zeigt das Dilemma um die private PC-Nutzung in Unternehmen überdeutlich.

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

Eine Chefsekretärin hatte mehrfach private eMails an Dritte gesandt und sogar ihren Arbeitgeber als dumm und unfähig bezeichnet. Aber kündigen konnte der Arbeitgeber dennoch nicht. Das LAG Köln fordert zunächst eine Abmahnung. Der Fehler des Arbeitgebers: Es gab im Unternehmen keine betriebliche Regelung über den Umfang der Privatnutzung des PC´s am Arbeitsplatz.

Der rechtliche Hintergrund

Immer wieder scheiterten bisher Arbeitgeber mit Kündigungen, weil die private PC-Nutzung in den Betrieb nicht oder nur unzureichend geregelt ist. Es empfiehlt sich also dringend, diesen Bereich mit den Mitarbeitern klar zu vereinbaren. Daran ändert auch die Eingangs vorgestellte Entscheidung des Bundesarbeitsgerichts nichts. Wie formulieren die Richter so schön: Ob die Kündigung wirksam ist, ist im jeweiligen Einzelfall zu prüfen. Es kommt also darauf an, wie Juristen immer wieder gern erklären.

Ein spezielles Gesetz zum Arbeitnehmerdatenschutz oder zur Nutzung von Internet und eMail am Arbeitsplatz existiert nicht. Die Zulässigkeit der privaten PC-Nutzung richtet sich vornehmlich nach dem Bundesdatenschutzgesetz (BDSG), den Normen des Individualarbeitsrechts und den Regelungen des Betriebsverfassungsgesetzes (BetrVG)zu der Einrichtung von technischen Überwachungssystemen. Die Betriebe, in denen Betriebsräte bestehen, müssen die im BetrVG festgeschriebenen Mitspracherechte und Mitbestimmungsrechte beachten.

Für Arbeitgeber ungewöhnliche Vorschriften ergeben sich aus dem Telekommunikationsgesetz sowie den weiteren telekommunikationsrechtlichen Regelungen. Internet und Email beruhen auf der Nutzung von Telekommunikationseinrichtungen. Weil bei der Nutzung der neuen Medien gleichzeitig auch Telekommunikationsdienste genutzt werden, kommen die Datenschutzregelungen der Telekommunikationsgesetze zur Anwendung kommen. Ob die Bereitstellung eines separaten PC´s für die private Nut-

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

zung die Lösung ist, um telekommunikationsrechtlichen Anforderungen zu entgehen, kann bezweifelt werden.

Der Arbeitgeber wählt

Der Arbeitgeber muss sich zwischen zwei Wegen entscheiden:

1. Dem Arbeitnehmer ist nur die rein dienstliche Nutzung von Internet und eMail erlaubt.
2. Dem Arbeitnehmer ist auch die private eMail- und Internetnutzung gestattet oder nicht ausdrücklich verboten.

Verboten ist verboten

Die Variante 1 ist der rechtlich einfachere, für die Betriebspraxis zumeist schwierigere Weg. Wurde einmal die private Internet-Nutzung gestattet, wird jedes Verbot von den Mitarbeitern als Rückschritt empfunden. Hier werden sowohl von der IT-Abteilung als auch von der Unternehmensleitung kommunikative Höchstleistungen erwartet, um den Mitarbeitern deutlich zu machen, dass eine erlaubte private Internet-Nutzung zusätzliche erhebliche Kosten aufgrund der Telekommunikationsgesetze und strafrechtliche Gefahren mit sich bringen. Nur bei einer Untersagung der privaten Nutzung sind vom Arbeitgeber die telekommunikationsrechtliche Vorschriften nebst den besonderen datenschutzrechtlichen Regelungen nicht zu beachten.

Im Betrieb ist bei einer völligen Untersagung der privaten Nutzung darauf zu achten, das nicht der jeweilige Vorgesetzte seinen Mitarbeitern entgegen der Vereinbarung „unter der Hand“ wieder Freiräume zur Privatnutzung einräumt. Diese würde wie bei einem regelungslosen Zustand dazu führen, dass eine „betriebliche Übung“ geschaffen wird, die dann im Ergebnis zu einer erlaubten privaten Nutzung führt.

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

Praxistipp

Wenn eine „betriebliche Übung“ der privaten Nutzung besteht, kann diese nicht durch eine Betriebsvereinbarung aufgehoben werden. Die betriebliche Übung kann nur durch eine individual-arbeitsvertragliche Übung oder durch eine „negative“/entgegengesetzte betriebliche Übung beseitigt werden

Unabhängig davon wird in der juristischen Literatur teilweise diskutiert, ob die Einrichtung und der Einsatz von Spamfiltern bei einer erlaubten Privatnutzung zu einer Strafbarkeit des Arbeitgebers führen kann. Wenn Spamfilter private Mails des Mitarbeiters herausfiltern, so könnte dies eine Verletzung des Post- oder Fernmeldegeheimnisses sein. Diese Auffassung hat beispielsweise das Oberlandesgerichts Karlsruhe vertreten.

„Erlaubt“ ist nicht einfach

Die Variante 2 ist der für den Arbeitgeber komplizierte Weg. Der Arbeitgeber muss das Fernmeldegeheimnis wahren. Jegliche Überwachung der Inhalte sowie der Verbindungsdaten der Internet- und eMail-Nutzung ist unzulässig. Trennt der Arbeitgeber eine erlaubte private Kommunikation nicht von der dienstlichen Kommunikation, so erstreckt sich die Geheimhaltungspflicht auch auf dienstliche eMails.

Neben der Wahrung des Fernmeldegeheimnisses ist der Arbeitgeber als Erbringer geschäftsmäßiger Telekommunikationsdienste gem. § 87 I TKG zu angemessenen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses verpflichtet. Diese Maßnahmen werden im Regelfall einen erheblichen Mehraufwand darstellen. Die Verpflichtung bezieht sich nur auf solche Datenverarbeitungssysteme, die bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten eingesetzt werden, wie z.B. ein PC mit Internet-/eMailzugang. Als Maßnahmen zum Schutz des Fernmeldegeheimnisses kommen Zutritts- und Zugriffsbe-

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

schränkungen, Verschlüsselungen sowie der Schutz der Firewall-Auswertungsprotokolle vor unbefugter Einsichtnahme in Betracht.

Bereits diese rechtlichen Aspekte zeigen die Komplexität der zu beachtenden Vorschriften. Datenschutzrechtliche Vorgaben aus dem Bereich des Teledienstedatenschutzgesetzes und des Bundesdatenschutzgesetzes kommen hinzu.

Lösungen für die Praxis

Die einfachste und für alle Beteiligten transparenteste Lösung ist, Kontrollrechte des Arbeitgebers umfassend im Arbeitsvertrag oder in der Betriebsvereinbarung zu regeln.

Gestattet der Arbeitgeber die Nutzung von eMail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- bzw. Teledienstrechts. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. eMail-Versenden der Mitarbeiter dienstlicher Natur ist. Dies ist insbesondere bei dem Verdacht von Straftaten wichtig. Andernfalls kann sich ein Arbeitgeber schnell in der Situation sehen, dass Strafverfolgungsbehörden beispielsweise in Hinblick auf Kinderpornografie oder wegen Urheberrechtsverletzungen Rechner oder gar Server des Unternehmens beschlagnahmen.

Von ein- und ausgehenden dienstlichen eMails der Mitarbeiter darf der Arbeitgeber selbstverständlich Kenntnis nehmen. Dies gilt im gleichen Maße wie für den dienstlichen Schriftverkehr.

Bei der Spam-Filterung setzt sich in der Praxis immer mehr durch, den Mitarbeitern eine Nachricht über die gefilterten Mails zukommen zu lassen. So kann im Einzelfall der Mitarbeiter prüfen, ob versehentlich eine dienstliche Mail als Spam eingeordnet wurde.

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

Inhalt einer Vereinbarung zur eMail- und Internetnutzung im Betrieb

- Zielsetzung der Vereinbarung
- Umfang der eMail- und Internetnutzung
- Beschreibung der Kontrollmaßnahmen
- Einwilligung in Protokollierung und Kontrolle
- Vertretungsregelung bei Ausscheiden oder längerer Krankheit des Mitarbeiters, Zugriffsmöglichkeiten des Arbeitgebers auf eMails
- Datenschutz für eMail- und Internetnutzung
- Sanktionen

Ihr Ansprechpartner für rechtliche Beratungen:
RA Thomas Feil, Ostfeldstr. 46, 30559 Hannover, Telefon: 0511 / 54 48 87 31, eMail: feil@recht-freundlich.de

Dürfen Chefs jede E-mail lesen und Internet-Nutzung kontrollieren?

Redaktion und Zusatzrecherchen: Benjamin Gehlen

Bei der Frage, ob die Chefs alle E-mails lesen und die Internet-Nutzung ihrer Mitarbeiter kontrollieren dürfen, gibt die Rechtslage in den einzelnen EU-Staaten recht unterschiedliche Antworten. Eine Arbeitsgruppe der Generaldirektion Binnenmarkt der Europäischen Kommission, die sich aus Vertretern der Datenschutzbehörden der Mitgliedstaaten zusammensetzte, hat dazu vor einigen Wochen ein Arbeitsdokument vorgelegt, in dessen Anhang die Regelungen in den einzelnen Mitgliedstaaten in bezug auf die Überwachung der elektronischen Kommunikation von Beschäftigten erläutert wird.
Die in der nachfolgenden Übersicht angeführten Informationen zu den einzelstaatlichen Bestimmungen im Zusammenhang mit der Kontrolle der elektronischen Kommunikation am Arbeitsplatz stützen sich im Falle von Dänemark, Griechenland, Spanien, Irland, Italien, Luxemburg, den Niederlanden, Portugal, Finnland, Schweden und Großbritannien im wesentlichen auf Angaben aus diesem Text. Die Informationen zu Belgien, Deutschland, Frankreich und Österreich beinhalten zudem aktuelle Recherchen bzw. Ergänzungen durch Europa-Kontakt.

BELGIEN

In Belgien regelt ein am 13. Juli 2002 in Kraft getretener branchenübergreifender Tarifvertrag zwischen Arbeitnehmern und Arbeitgebern den Datenschutz am Arbeitsplatz. Grundsätzlich dürfen die Arbeitgeber nach diesem Tarifvertrag die E-mails ihrer Beschäftigten kontrollieren. Dabei müssen sie sich aber an genau umrissene Verfahrensregeln halten, in denen explizit festgelegt wird, welche Vorgehensweise erlaubt ist und welche nicht. Eine Beratung mit den Gewerkschaften über die Kontrollkriterien und über die mit der Kontrolle zu beauftragende Abteilung ist unabdingbar. Die Überwachung muß zunächst anonym, d.h. so erfolgen, daß aus den gesammelten Daten zur E-mail- und Internet-Nutzung nicht unmittelbar der Schreibtisch, von dem die Daten stammen, zu ermitteln ist. Erst wenn strafbare Handlungen, Gefahren für wirtschaftliche Interessen des Unternehmens oder die Funktionsweise des EDV-Systems auffallen, darf der einzelne Arbeitnehmer, auf dessen Verhalten diese Auffälligkeiten zurückzuführen sind, identifiziert werden. Liegt hingegen bloß ein Verstoß gegen die Hausregeln zum Internetgebrauch vor, so muß der Arbeitgeber ein dreistufiges Verfahren anwenden. Zunächst sind seine Beschäftigten über den Verstoß zu informieren. Stellt er danach weitere Mißbrauchshandlungen fest, kann er die Identität der gegen die Regeln verstoßenden Person ermitteln. In einem Gespräch, bei dem auch ein Gewerkschaftsvertreter anwesend sein kann, wird dem Arbeitnehmer die Möglichkeit geboten, sein Verhalten zu rechtfertigen.
Bei all diesen Verfahren gilt, daß der Arbeitgeber ab dem Zeitpunkt, zu dem der dienstliche Charakter der Kommunikation angezweifelt wird, nicht mehr ohne die explizite Zustimmung des Arbeitnehmers den Inhalt oder auch nur die Betreffzeile der Mitteilung lesen darf. Auf diese Weise soll deren (höchstwahrscheinlich) privater Inhalt geschützt werden. Unterschieden wird also zwischen dienstlichen E-mails, die der Vorgesetzte jederzeit überprüfen darf, und privaten E-mails, die nur mit Einverständnis des Arbeitnehmers und dessen Kommunikationspartners gelesen werden dürfen. Bei Verstößen gegen diese Regeln kann gegen den Arbeitgeber vorgegangen werden.
Das weiterhin geltende Telekommunikationsgesetz von 1991 macht hingegen keinen Unterschied zwischen privaten und dienstlichen E-mails. Jede an einen Empfänger gerichtete E-mail kann ungeachtet ihres Inhalts als private Mail betrachtet werden und darf nur mit Zustimmung des Versenders und Empfängers gelesen werden. Sie ist selbst dann kein zulässiges Beweismittel für die Entlassung eines Arbeitnehmers aus dringenden Gründen, wenn mit der E-mail geheime Betriebsinformationen an Dritte verschickt wurden.

DÄNEMARK

In Dänemark wird die Kontrolle und Überwachung am Arbeitsplatz vor allem durch Übereinkommen zwischen den Sozialpartnern, insbesondere durch das sog. „basic agreement“, geregelt. Die zentrale Aussage dieses Textes ist, daß der Arbeitgeber die am Arbeitsplatz verrichtete Arbeit kontrollieren darf. Die Gerichte haben jedoch anerkannt, daß dieses Recht die Pflicht des Arbeitgebers zum verantwortungsvollen Handeln und das Mißbrauchsverbot einschließt. Im Anhang dieses Übereinkommens zwischen dem dänischen Verband der Arbeitgeber und dem dänischen Bund der Gewerkschaften vom 24. April 2001 heißt es, daß der Arbeitgeber verpflichtet ist, seinen Arbeitnehmer zwei Wochen im voraus über jegliche geplante Kontrollaktivitäten zu unterrichten.
Das Abhören privater oder dienstlicher Telekommunikation ist in Dänemark strafbar. Ob auch die E-mail-Korrespondenz als Telekommunikation im Sinne dieses Gesetzes gilt, ist bislang nicht geklärt worden. Die dänische Datenschutzbehörde geht davon aus, daß ein Unternehmen Sicherheitskopien von Arbeitnehmer-E-mails anfertigen und diese anschließend untersuchen kann, wenn Mißbrauchsverdacht besteht und zudem die folgenden Voraussetzungen vorliegen:

1. Notwendigkeit der Maßnahme für den Schutz der rechtmäßigen Interessen des Arbeitgebers, die nicht geringer sein dürfen als die entgegenstehenden Interessen des betroffenen Arbeitnehmers.

2. Rechtmäßige Interessen können an der Funktionalität des Unternehmens (operation of the business), der Sicherheit, der Wiederherstellung der E-mail, der Dokumentation und an der Überwachung bestehen.
3. Bei der Überwachung der E-mail- und Internetnutzung ist der Arbeitgeber verpflichtet, die Daten in der üblichen Verfahrensweise zu verarbeiten.

DEUTSCHLAND

In Deutschland gelten für die rein dienstliche und die zumindest auch private Nutzung von E-mail und Internet am Arbeitsplatz unterschiedliche Regeln. Gestattet der Arbeitgeber ausschließlich die dienstliche Nutzung, so ist er nicht Anbieter im Sinne des Telekommunikations- bzw. Teledienstrechts. Grundsätzlich hat er das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-mail-Versenden dienstlichen Zwecken dient. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist aber ein schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten und kann daher nur bei konkretem Mißbrauchsverdacht im Einzelfall zulässig sein. Auf jeden Fall sind die Beschäftigten auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen hinzuweisen. Nach der Rechtsprechung des Bundesarbeitsgerichts ist die Kenntnisnahme des Inhalts und der Verbindungsdaten dienstlicher Telefonate von solchen Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden (z.B. Psychologen, Ärzte, Sozialarbeiter und -pädagogen) durch den Arbeitgeber ausgeschlossen, falls diese Daten einen Rückschluß auf die betroffenen Personen zulassen.
Von ein- und ausgehenden dienstlichen E-mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. So kann der Vorgesetzte beispielsweise verfügen, daß ihm jede ein- oder ausgehende dienstliche E-mail seiner Mitarbeiter vorzulegen ist. Zum Zwecke der Effizienz-Kontrolle seiner Beschäftigten darf der Arbeitgeber den dienstlichen E-mail-Verkehr aber nur dann beobachten, wenn der Betriebsrat damit einverstanden ist.
Erlaubt ein Arbeitgeber die private Nutzung von Internet oder E-mail, so ist er seinen Beschäftigten gegenüber Telekommunikations- bzw. Teledienste-Anbieter. Er ist dann wie beim privaten Telefonieren zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet und muß die privaten E-mails wie private schriftliche Post behandeln. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle über die Einhaltung dieser Bedingungen müssen unter Beteiligung des Betriebsrats eindeutig geregelt werden.
Die Datenschutzbeauftragten des Bundes und der Länder Bayern, Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Schleswig-Holstein und Thüringen forderten in einer gemeinsamen Erklärung vom 27. Februar 2002 angesichts stetig wachsender technischer Möglichkeiten eine klare Regelung darüber, welche Daten die Arbeitgeber über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie genutzt werden dürfen.

FINNLAND

Am 01.10.2001 haben die Finnen ein Gesetz zum Schutz der Privatsphäre während der Arbeitszeit erlassen. Es betrifft den öffentlichen wie den privatwirtschaftlichen Arbeitsmarkt und beinhaltet überdies Bestimmungen zu Bewerbern.
Abschnitt 9 behandelt die Überwachung der Arbeitnehmer. Ziel dieses Gesetzes ist aber nicht die Schaffung von Rechten und Pflichten bei der technischen Überwachung oder Nutzung von Informationsnetzwerken. Vielmehr will man dazu anregen, diesbezügliche Grundsätze zu etablieren. Vorgegeben ist aber, daß die aus der Überwachung gewonnenen Daten notwendig für das Arbeitsverhältnis sein müssen. Außerdem dürfen geplante E-mail-Kontrollen erst nach Absprache mit den Beschäftigten erfolgen. Dabei muß der Arbeitgeber Angaben zu der von ihm mit den Maßnahmen verfolgten Absicht, den angewandten Methoden und den Prinzipien der E-mail- und Internet-Nutzung machen.

FRANKREICH

Artikel 9 des französischen Code Civil garantiert jedem Menschen das Recht auf Schutz des Privatlebens auch während der Arbeitszeit und am Arbeitsplatz. Das Telekommunikationsgesetz von 1991 wird von der französischen Datenschutzbehörde so ausgelegt, daß zwar die Erfassung des Umfangs und der Größe der Nachrichten zusammen mit dem Format der anhängenden Dateien erlaubt ist, nicht aber das Lesen der E-mails. Sammelt der Arbeitgeber persönliche Informationen über den Arbeitnehmer, so muß er ihn nach dem französischen Arbeitsrecht darüber informieren.
Das Oberste Gericht hat im Oktober 2001 entschieden, daß der Arbeitgeber selbst dann die private E-mail nicht lesen darf, wenn sie einen Verstoß gegen das Verbot der privaten Nutzung der Internetverbindung darstellt. Nach einer öffentlichen Konsultation zum Thema Cyber-Überwachung hat die französische Datenschutzbehörde (CNIL) eine Lösung des Problems der Überwachung am Arbeitsplatz von den Sozialpartnern verlangt. Die CNIL schlug den Unternehmen vor, gemeinsam mit ihren Arbeitnehmervertretern einen Beauftragten für Datenschutz und die Nutzung neuer Technologien zu ernennen. Dieser Beauftragte soll bei Fragen zu Sicherheitsmaßnahmen, dem Recht auf Zugang zu Daten sowie dem Datenschutz am Arbeitsplatz in seinem Unternehmen von beiden Seiten konsultiert werden können.
Die griechische Verfassung enthält mehrere grundsätzliche Regeln, die das Recht auf Privatleben und das weitergehende Persönlichkeitsrecht abdecken. Das griechische Zivilrecht sieht außerdem vor, daß jede Rechtshandlung,

GRIECHENLAND

die gegen die guten Sitten verstößt oder die in der Verfassung gewährten Freiheits- und Menschenrechte verkürzt, nichtig ist. Diese Grundsätze könnten herangezogen werden, um die E-mail-Überwachung durch den Arbeitgeber für ungültig zu erklären, weil mit dieser Maßnahme in das von der Verfassung gewährte Privatleben des Arbeitnehmers eingegriffen wird. Ein weiteres Gesetz gibt den Betriebsräten das Recht, in bestimmten Bereichen, z.B. der Arbeitnehmerüberwachung, Absprachen mit dem Arbeitgeber zu treffen.

IRLAND

In Irland sollen die Persönlichkeitsrechte der Bürger laut Verfassung durch die Gesetze geschützt und in den Gesetzen respektiert werden. Im irischen Richterrecht werden sie ständig fortentwickelt. Das Recht auf Schutz der Privat- und Intimsphäre wurde bereits als Persönlichkeitsrecht der Bürger anerkannt.

ITALIEN

Im Geltungsbereich des italienischen Rechts bedarf es einer gerichtlichen Anordnung, um die E-mail eines Arbeitnehmers öffnen zu dürfen. Artikel 15 der Verfassung garantiert die Freiheit und das Geheimnis der Korrespondenz bzw. jeglicher Form der Kommunikation. Die Bedeutung dieser Vorschrift für den Bereich der E-mail-Überprüfung wurde von der italienischen Garante (entspricht Datenschutzbeauftragten) anerkannt. Danach unterliegen E-mails der selben Vertraulichkeit wie die traditionelle Briefpost. Um dies zu gewährleisten, wurden 1993 ein Gesetz zur Computer-Kriminalität und vier Jahre später eine Verordnung zum Umgang mit elektronischen Dokumenten erlassen.

LUXEMBURG

In Luxemburg existiert bisher noch keine einschlägige Gesetzgebung im Bereich der Kontrolle und Überwachung der elektronischen Kommunikation am Arbeitsplatz.

NIEDERLANDE

Artikel 10 der niederländischen Verfassung garantiert, daß jeder das Recht auf Achtung seines Privatlebens hat. Vorschriften aus dem Arbeitsrecht verpflichten den Arbeitgeber, seine Beschäftigten über bevorstehende Kontrollen zu informieren. Bei Kontrollen am Arbeitsplatz müssen die Personalvertretung und die Gewerkschaft zuvor informiert und angehört worden und mit den Maßnahmen einverstanden gewesen sein. 1999 hat die niederländische Datenschutzbehörde entschieden, daß kontinuierliche E-mail-Kontrollen nicht erlaubt sind, wenn damit kein bestimmter legitimer Zweck verfolgt wird.
In einem Urteil des Regionalgerichtshofs von Harlem von 1999 wurde auf den Begriff der Privatisierung des Arbeitsplatzes abgestellt, um zu verdeutlichen, daß die Grenzen zwischen Privatleben und Arbeit nicht mehr klar sind. Private Kontakte vom Arbeitsplatz aus dürften demnach in den Niederlanden erlaubt sein.

ÖSTERREICH

Der in Österreich direkt anwendbare Artikel 8 der Europäischen Menschenrechtskonvention gewährt das Recht auf Achtung des Privatlebens. Ebenso wie diesem Artikel kommt auch Artikel 1 des Datenschutzgesetzes, der allen Individuen das Recht auf Datenschutz verleiht, der Rang eines Grundrechts zu.
Im Datenschutzgesetz aus dem Jahr 2000 ist eine explizite Regelung für den Umgang mit sensiblen Daten am Arbeitsplatz enthalten. Wenn die Nutzung der persönlichen Daten durch den Arbeitgeber in Einklang mit dessen Rechten und Pflichten aus dem Arbeitsrecht steht und auch durch spezielle rechtliche Bestimmungen legitimiert ist, stellt sie keinen Verstoß gegen den Datenschutz dar.
Nach Paragraph 96 des Arbeitsverfassungsgesetzes darf der Arbeitgeber bestimmte Maßnahmen nur mit Zustimmung des Betriebsrats durchführen. Zu den zustimmungspflichtigen Maßnahmen gehören auch die Einführung von Kontrollen und technischer Einrichtungen, wenn sie die Menschenwürde der Arbeitnehmer berühren könnten. Selbst wenn der einzelne Beschäftigte in seinem Arbeitsvertrag sein Einverständnis zu solchen Maßnahmen gegeben hat, bleibt die Zustimmung des Betriebsrats unerläßlich.

PORTUGAL

Die portugiesische Verfassung beinhaltet neben dem Recht auf Schutz des Privatlebens, auf Wahrung der Menschenwürde und dem Kommunikationsgeheimnis einen eigenen Artikel, der die Beziehung von Datenschutz und elektronischer Datenverarbeitung regelt. Abgesehen von gesetzlich verfügten Ausnahmefällen aus dem Strafprozeßrecht dürfen öffentliche Stellen die Korrespondenz, Telekommunikation oder jegliche andere Kommunikation nicht stören. Entsprechend Artikel 18 soll dieses Verbot in öffentlich-rechtlichen und in privatrechtlichen Beschäftigungsverhältnissen seine Wirkung entfalten. Das Korrespondenzgeheimnis deckt laut einer Entscheidung von Portugals Datenschutzkommission nicht nur Inhalt, sondern auch die Art und Weise der Korrespondenz ab.

SCHWEDEN

Die schwedischen Bürger werden durch ihre Verfassung vor der Überprüfung ihrer Post und vertraulicher Kommunikation geschützt. Die Internetnutzung und die E-mails der Arbeitnehmer dürfen nur kontrolliert werden, wenn ihr Arbeitgeber damit bestimmte Zwecke verfolgt, über die die Beschäftigten zuvor informiert wurden. Gesetzlich festgelegt ist auch, daß jegliche Überwachung der Arbeitnehmer nur nach Absprache mit den Gewerkschaften erfolgen darf.

SPANIEN

In Spanien gewährt Artikel 18 der Verfassung den Schutz des postalischen, telegrafischen oder telefonischen Kommunikationsgeheimnisses, so es sich um private Kommunikation handelt. Das Arbeitsgesetz sieht ferner vor, daß Kontrollen des Arbeitnehmers, seines Schließfaches oder seiner anderen persönlichen Angelegenheiten nur dann am Arbeitsplatz und in der Arbeitszeit erfolgen dürfen, wenn es für den Schutz des Unternehmens und seiner Mitarbeiter notwendig ist. Würde und Privatleben des Arbeitnehmers sollen bei der Kontrolle respektiert werden. Ein rechtmäßig ernannter Vertreter des Personals bzw. in dessen Abwesenheit ein anderer Arbeitnehmer des Unternehmens soll, wenn möglich, bei diesen Maßnahmen anwesend sein. Der Arbeitgeber ist nach einem Gesetz aus dem Jahr 1995 verpflichtet, seine Arbeitnehmer im Vorfeld über Entscheidungen, die u.a. die Arbeitsplanung und -organisation des Unternehmens oder die Einführung neuer Technologien betreffen, sowie über deren Konsequenzen für die Sicherheit und Gesundheit des Arbeitnehmers zu informieren.
Nach spanischem Strafrecht macht sich strafbar, wer sich mit der Absicht, persönliche Geheimnisse oder Einzelheiten des Privatlebens zu enthüllen, Besitz an der privaten Korrespondenz eines anderen verschafft.

VEREINIGTES KÖNIGREICH

In Großbritannien dürfen ohne Einverständnis des Senders und des Empfängers keine E-mails vom Arbeitgeber abgefangen werden. So bestimmt es der „Regulation of Investigatory Powers Act“, der im Oktober 2000 Gesetz wurde. Von diesem Grundsatz kann aber abgewichen werden, wenn

1. für das Unternehmen wichtige Daten wiederhergestellt werden sollen;
2. das Einhalten von auferlegten oder freiwilligen Praktiken oder Verfahrensweisen festgestellt werden soll;
3. ermittelt werden soll, ob die Arbeitnehmer die an sie gestellten Anforderungen erfüllen;
4. dadurch Straftaten verhindert oder aufgedeckt werden;
5. Sicherheit und effektive Arbeitsweise des Systems gesichert werden sollen.

Die Ausnahmen zum Verbot unfreiwilliger Kontrollen sind sehr weit gefaßt. Die Systemnutzer müssen vom Arbeitgeber darüber informiert werden, daß die von ihnen gesendeten oder empfangenen Daten abgefangen werden können. Zusätzlich müssen bei den Kontrollen, sofern diese persönliche Daten verarbeiten, die Regelungen des Datenschutzgesetzes von 1998 eingehalten werden.

Ansprechpartner und Fundstellen:

- **Datenschutz auf EU-Ebene:**
  Europäische Kommission, Generaldirektion Binnenmarkt, Referat A/4 - Datenschutz, Philippe Renaudière, Avenue de Cortenbergh 107, 1040 Brüssel, Belgien, E-mail: Markt-A4@cec.eu.int, Tel.: 0032/2/2957377, Fax: 0032/2/2968010, Internet: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm
- **Datenschutz in Deutschland:**
  Der Bundesbeauftragte für den Datenschutz, Friedrich-Ebert-Straße 1, 53173 Bonn, E-mail: poststelle @bfd.bund.de, Tel.: 01888/77990, Fax: 01888/7799550, Internet: http://www.bfd.bund.de
- **Datenschutz in Österreich:**
  Bundeskanzleramt, Österreichische Datenschutzkommission, Ballhausplatz 1, 1014 Wien, E-mail: v3post@bka.gv.at, Tel.: 00431/531152525, Fax: 00431/531152690, Internet: http://www.bka.gv.at/datenschutz/
- **Datenschutz in den anderen EU-Staaten:**
  Liste mit allen Kontaktdaten der nationalen Datenschutzbeauftragten der EU-Staaten und weiterer Länder im Internet unter: http://europa.eu.int/comm /internal_market/de/dataprot/links.htm
- **Der komplette Text des in Englisch abgefaßten Anhangs zu dem Arbeitsdokument der Arbeitsgruppe der Generaldirektion Binnenmarkt: „Einzelstaatliche Rechtslage zur Überwachung und Kontrolle der elektronischen Kommunikation am Arbeitsplatz“ kann unter folgender Internetadresse abgerufen werden: http://europa.eu.int/comm/internal_market/de/dataprot/wpdocs/index.htm.**

Private Internetnutzung am Arbeitsplatz/I

JOERG HEIDRICH

Ob Unternehmen ihren Mitarbeitern privates Surfen im Web und Verschicken von Mails gestatten oder nicht-dienstliche Anwendungen völlig verbieten - in beiden Fällen lauern juristische Fallstricke.

Eigentlich hatte sich die Rezeptionistin einer internationalen Anwaltskanzlei gar nichts Böses gedacht, als sie den gerade von ihrer Tante erhaltenen Kettenbrief an ihre Kolleginnen und ein paar Freunde außerhalb der Kanzlei weiterleitete. Zwar hatte sie vor einiger Zeit mal ein internes Memo gelesen, nachdem private E-Mails nicht versandt werden sollten. Darin sah sie jedoch kein bindendes Verbot - schließlich hatte sie nicht den Betriebsablauf gestört oder gar Viren verbreitet. Jedenfalls hätte sie nie mit der fristlosen Kündigung gerechnet, die ihr die Kanzleioberen am nächsten Tag präsentierten. Diese sahen nämlich in der Weiterleitung der Mail eine potenzielle Bedrohung für den lebenswichtigen Datenbestand der Kanzlei und damit das Vertrauensverhältnis zu ihrer Angestellten erheblich gestört.

Das Beispiel zeigt die große Unsicherheit, die sowohl auf Seiten der Arbeitnehmer als auch der Arbeitgeber bei der Nutzung des Internets in Betrieben herrscht. Eine aktuelle Studie der Jobsuchmaschine monster.de zeigt, dass rund 43 % der befragten Arbeitnehmer täglich private E-Mails versenden, immerhin 22 % tun dies mehrmals in der Woche. Gleiches gilt für die Nutzung des Web. Nur wenige Arbeitnehmer, die während der Fußballweltmeisterschaft die Ergebnisticker abgefragt oder digitale Moorhühner heruntergeladen haben, dürften dies aus beruflicher Notwendigkeit getan haben. Und die Zugriffszahlen vieler Erotikseiten weisen ihre Spitzenwerte eher während der üblichen Arbeitszeiten als in den geruhsamen Feierabendstunden auf.

Für Unternehmen ist das Dilemma nur schwer zu lösen: Auf der einen Seite wünscht sich jeder Arbeitgeber einen gut informierten, die Möglichkeiten des Internets für seine Aufgaben nutzenden Angestellten. Auf der anderen Seite belasten die durch Traffic und Arbeitsausfall verursachten Kosten die schmalen Budgets, und jede privat erhaltene E-Mail oder angesurfte unsichere Internetseite bringt die EDV-Infrastruktur des Unternehmens in Gefahr.

PERSÖNLICHKEITSRECHT CONTRA ARBEITGEBERINTERESSE

Darüber hinaus bestehen im Rahmen der Nutzung elektronischer Datendienste in Büros eine ganze Reihe von rechtlichen Problemen. Deren Nutzung und Überwachung befindet sich in einem Spannungsfeld zwischen dem grundgesetzlich garantierten Schutz des Persönlichkeitsrechts des Arbeitnehmers, das ebenso am Arbeitsplatz gilt, und der Verpflichtung des Arbeitenden, seine Aufgaben ordnungsgemäß und vertrauensvoll im Interesse seines Arbeitgebers zu erfüllen - wofür auch eine gewisse Kontrolle durch diesen erforderlich sein kann.

Hinsichtlich der rein geschäftlichen Nutzung von E-Mail und Web wiegt das Interesse des Unternehmens an der Aufrechterhaltung der betrieblichen Organisation und der geschäftlichen Kontakte schwerer als das Persönlichkeitsrecht des Betroffenen. Daraus ergibt sich, dass eine Protokollierung der abgerufenen beruflichen Inhalte und Mails jederzeit

zulässig ist. Das eigentliche Problem entsteht jedoch dadurch, dass häufig private Inhalte oder Mails über denselben Zugang empfangen werden. Dass der Arbeitgeber bei der Überprüfung der privaten Korrespondenz den Rahmen des Erlaubten verlässt, liegt auf der Hand, da hier ein schutzwürdiges Interesse des Unternehmens fehlt. Sofern sich also private und geschäftliche Nutzung der Dienste vermischen, ist eine Überwachung des Arbeitnehmers weitgehend ausgeschlossen.

Grundsätzlich hat ein Arbeitnehmer keinen Anspruch auf eine private Nutzung beruflicher Kommunikationseinrichtungen. Eine nur scheinbar einfache Lösung des beschriebenen Problems liegt im generellen Verbot der privaten Nutzung des Internets am Arbeitsplatz. In diesem Fall bestimmt sich die Frage, inwieweit der Arbeitgeber von den Verbindungs- und Inhaltsdaten Kenntnis nehmen darf, nach den allgemeinen Regeln des Bundesdatenschutzgesetz (BDSG), das ebenfalls die beschriebene Abwägung zwischen Persönlichkeitsrecht und Interesse des Unternehmens vorsieht.

Ergebnis dieser Abwägung ist allerdings, dass auch bei einem Verbot privater Nutzung nur die äußeren Verbindungsdaten wie Zeit, IP- oder E-Mail-Adressen und allenfalls Mail-Header zur Kenntnis genommen werden dürfen. Denn auch wenn man davon ausgehen kann, dass nur dienstliche Inhalte abgerufen oder in Mails versendet werden, stellt die ohne Zustimmung des Betroffenen vorgenommene Überwachung des Datenverkehrs, ähnlich wie das unangekündigte Mithören eines dienstlichen Telefonats, einen durch nichts zu rechtfertigenden Eingriff in das Persönlichkeitsrecht dar. Allenfalls in Ausnahmefällen wie dem Verdacht auf eine Straftat überwiegt hier das Interesse des Arbeitgebers.

Letztlich ist damit ein generelles Verbot der Nutzung elektronischer Datendienste rechtlich kaum oder nur unter ganz erheblichem, kaum zu leistenden Aufwand zu kontrollieren. Zudem dürfte es vielfach zu einer erheblichen Verunsicherung der Mitarbeiter führen und den produktiven Umgang mit dem für viele immer noch neuen Medium stark beeinträchtigen. Schließlich ist für etliche Berufe die uneingeschränkte Nutzung des Internets eine wichtige Voraussetzung, sodass eine scharfe Abgrenzung hier ohnehin kaum möglich ist.

Doch auch die Erlaubnis zur privaten Nutzung des Internets unter bestimmten Voraussetzungen und in Grenzen - etwa im Rahmen von Arbeitspausen - ist rechtlich problematisch. Soweit der Arbeitgeber diese private Nutzung nämlich gestattet, bietet er Telekommunikationsdienste im Sinne des § 3 des Telekommunikationsgesetzes (TKG) an. In diesem Fall erbringt er ein ‘auf Dauer angelegtes Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte’ seinen Arbeitnehmern.

DATENSCHUTZ-KONFLIKT

Damit gelten aber in diesem Fall für einen Arbeitnehmer die gleichen Regeln hinsichtlich des Datenschutzes wie für jeden Kunden eines Telefon- oder Internetunternehmens. Insbesondere gilt das strenge Fernmeldegeheimnis des § 85 TKG für sämtliche Nutzerdaten, da dienstliche und private Nutzung aus technischen Gründen kaum unterschiedlich behandelt werden können. Daraus folgt, dass der Arbeitgeber grundsätzlich überhaupt keine E-Mails lesen und Verbindungsdaten speichern darf. In der Praxis resultieren aus diesen starken Einschränkungen erhebliche Probleme: So ist es beispielsweise für die Systemadministratoren erforderlich, Internetverbindungen oder Mail-Verbindungen zu protokollieren, was aber faktisch gesetzlich nur in sehr engem Rahmen und anonymisiert möglich ist. Auch das Lesen fremder Mails im Notfall, etwa bei einer Erkrankung des Mitarbeiters, wäre ohne vorherige Zustimmung des Betroffenen unzulässig.

Eine Lösung für dieses Dilemma liegt in der Festlegung eindeutiger Regelungen für die Internetnutzung im Unternehmen. Dabei muss vor allem geklärt werden, ob die private Nutzung von Web und E-Mail generell zulässig ist und wenn ja, in welchem Rahmen. Hier bietet sich das Abschließen einer Betriebsvereinbarung oder Internetrichtlinie an, in deren Gestaltung der Betriebsrat - soweit vorhanden - einzubeziehen ist. Eine solche Vereinbarung regelt aber nur die Rahmendaten für eine betriebliche Nutzung des Internets, etwa den Umfang, in dem eine private Nutzung zulässig ist (Beispielformulierung: 'Soweit der Dienstbetrieb nicht gestört wird, dürfen Internet und E-Mail in geringem Umfang auch privat genutzt werden').

Daneben ist ebenfalls das datenschutzrechtliche Problem des Zugriffs auf personenbezogene Daten des Arbeitnehmers, beispielsweise auf E-Mail zu lösen. Das kann und sollte durch individuelle Bestätigungen geschehen, in denen sich der Beschäftigte damit einverstanden erklärt, dass die ihm zugestandene private Nutzung elektronischer Datendienste wie die dienstliche zu behandeln ist. Dort sollte genau festgelegt werden, unter welchen Umständen zum Beispiel die persönliche Mailbox durch Dritte abgefragt werden kann oder welche Nutzungsdaten zu welchem Zweck protokolliert werden. Die Einwilligung des Arbeitnehmers zu derartigen betriebsbedingten Kontrollmaßnahmen kann das Unternehmen sinnvollerweise bereits im Arbeitsvertrag einholen. Verweigert der zukünftige Mitarbeiter seine Zustimmung, so bleibt nur ein striktes Verbot der Privatnutzung.

Im Fall der oben erwähnten Rezeptionistin, über den das Hessische Landesarbeitsgericht Ende 2001 zu entscheiden hatte, gab es derartige bindende Vereinbarungen nicht. Ein einfaches Memo reicht nach Ansicht der Richter hierfür bei weitem nicht aus. Damit war die ausgesprochene Kündigung wirkungslos, da in dem Verhalten der Angestellten keine schwerwiegende Pflichtverletzung, sondern allenfalls ein Grund für eine arbeitsrechtliche Abmahnung zu sehen ist, die jedoch nicht erfolgte. Das Ansehen pornografischer Websites im Büro kann hingegen grundsätzlich zu einer fristlosen Kündigung führen.

FAZIT

Ob eine private Nutzung des Internets in Betrieben erlaubt wird oder nicht - aus rechtlicher Perspektive sollte die Nutzung elektronischer Kommunikation im Büro in jedem Fall eindeutig geregelt werden, um juristischen Fallstricken zu entgehen und für alle Beteiligten klare Verhältnisse zu schaffen. Dabei empfiehlt sich, mit dem Abschluss einer Betriebsvereinbarung zugleich individuelle Vereinbarungen mit den Beschäftigten dahingehend zu schließen, welche Daten wie genutzt werden dürfen.

Private Internetnutzung am Arbeitsplatz/II

JOERG HEIDRICH

Ein Klick auf die Seite des bekannten Nachrichtenmagazins, ein kurzer Blick auf das eigene Konto per Online-Banking, die E-Mail an die Freundin. Es dauert ja nur fünf Minuten ... Darf man für private Zwecke vom Arbeitsplatz aus im Internet surfen? Oder darf man nicht?

Die Frage, inwieweit Mitarbeiter eines Unternehmens Internet- und E-Mail-Dienste am Arbeitsplatz privat nutzen dürfen, hatte sich die iX in der Ausgabe 1/2003 gestellt und zunächst anhand der geltenden Gesetzeslage ganz allgemein beantwortet. Daraufhin erreichte uns eine Fülle von Nachfragen interessierter Leser zu den praktischen Auswirkungen dieser Regelungen an ihrem Arbeitsplatz, die an dieser Stelle beantwortet werden sollen.

Frage: In meinem Betrieb gibt es keine eindeutige Regelung zur privaten Nutzung von Web und E-Mail. Was kann mir passieren, wenn ich trotzdem gelegentlich in meiner Arbeitszeit *'privat' surfe?*

Grundsätzlich hat ein Arbeitnehmer keinen Anspruch auf eine private Nutzung beruflicher Kommunikationseinrichtungen. Auch wenn keine betriebsinterne Vereinbarung getroffen wurde, die die Grenzen einer privaten Nutzung eindeutig festlegt, ist das selbstverständlich kein Freibrief für Arbeitnehmer. Dennoch ist in diesem Fall eine geringfügige Nutzung des Web kein Grund für eine fristlose Kündigung, solange sie sich innerhalb eines gewissen Rahmens hält.

So sah das Arbeitsgericht Wesel (Az.: 5 Ca 4021/00) im Fall einer Arbeitnehmerin, die einen Internetzugang in einem Jahr rund 100 Stunden privat genutzt hatte, zwar einen Grund für eine Abmahnung, nicht jedoch für eine fristlose Kündigung. Die Begründung: Passt dem Chef das Surfen nicht, muss er es zuerst einmal ausdrücklich verbieten und einen Verstoß per Abmahnung rügen. Andernfalls kann der Arbeitnehmer sogar davon ausgehen, dass die private Nutzung des Internet in geringem Rahmen geduldet wird.

Etwas anderes gilt dagegen bei einem eindeutigen betrieblichen Verbot der Privatnutzung. Hier dürfte schon eine deutlich geringere Anzahl von im Internet ohne Arbeitsbezug verbrachten Stunden eine Kündigung ohne vorherige Abmahnung rechtfertigen.

Heimliche Überwachung verstößt gegen Datenschutz

Wer haftet eigentlich für Inhalte, die sich auf Firmen-PCs befinden, zum Beispiel MP3-Dateien und so weiter?

Aus juristischer Sicht trägt zunächst das Unternehmen die alleinige Verantwortung für jedes Bit auf seinem Server. Wenn dort strafbare Inhalte, etwa Kinderpornos, gespeichert werden,

kann die Polizei den Zentralrechner beschlagnahmen - was für viele Unternehmen das Aus bedeuten kann. Persönlich haftbar sind hier, je nach Gesellschaftsform des Unternehmens, in der Regel die Geschäftsführer. Bei zivilrechtlichen Ansprüchen, beispielsweise wegen eines Urheberrechtsverstoßes, haftet das Unternehmen als so genannte ‘juristische Person’. Sofern ein Arbeitnehmer eindeutig als Verursacher einer Rechtsverletzung zu identifizieren ist, kann das Unternehmen bei ihm Regressansprüche geltend machen.

Anders sieht es aus, wenn derartige Inhalte auf einem Einzelplatzrechner gespeichert sind, der eindeutig nur einem einzelnen Arbeitnehmer zur Verfügung steht. In diesem Fall haftet der Angestellte selbst.

Ist die Nutzung oder Speicherung rechtswidriger oder pornografischer Inhalte am Arbeitsplatzrechner ein Grund für eine Kündigung?

Eindeutig ja. So hat etwa das Arbeitsgericht Düsseldorf (Az.: 4 Ca 3437/01) entschieden, dass ein Arbeitnehmer, der seinen Internetzugang im Betrieb nutzte, um Pornos anzuschauen und der darüber hinaus sogar von seinem Arbeitsplatz aus eine eigene Website mit erotischen Inhalten betrieb, ohne vorhergehende Mahnung gekündigt werden darf. Gleiches gilt selbstverständlich erst recht bei strafrechtlich verbotenen Inhalten wie Kinder- oder Gewaltpornografie.

Ob dies auch für strafrechtlich nicht relevante Urheberrechtsverletzungen gilt, etwa bei Sammlung von MP3s am Arbeitsplatz, war bisher noch nicht Gegenstand arbeitsrechtlicher Gerichtsentscheidungen, darf aber bezweifelt werden.

Kann auch meine private Nutzung des Internets von zu Hause aus Auswirkungen auf mein Arbeitsverhältnis haben?

In Ausnahmefällen, die eine extreme Belastung des Arbeitsverhältnisses bedeuten, wird dies von verschiedenen Gerichten bejaht. So hat etwa das Arbeitsgericht Braunschweig (Az.: 3 Ca 370/98) die fristlose Kündigung des Leiters eines kommunalen Kindergartens bestätigt, da bei staatsanwaltschaftlichen Ermittlungen auf dem privaten PC des Arbeitnehmers sechzig aus dem Internet heruntergeladene Bilddateien mit Kinderpornografie sichergestellt wurden und dies den dringenden Verdacht begründete, der Arbeitnehmer habe aufgrund pädophiler Neigungen gehandelt.

Umstrittener ist dies in einem Fall, den das Landesarbeitsgericht Schleswig-Holstein Ende 1998 zu entscheiden hatte (Az.: 2 Sa 330/98). Hier hatte ein Arbeitnehmer auf seiner privaten Website wiederholt beleidigende Inhalte über seinen Arbeitgeber verbreitet. Das Gericht bestätigte die ausgesprochene Kündigung, der jedoch schon mehrere Abmahnungen des Arbeitnehmers vorangegangen waren. Hinsichtlich seiner Veröffentlichungen im Internet konnte sich der Beschäftigte nicht auf sein Grundrecht der freien Meinungsäußerung nach Artikel 5 GG berufen. Dieses jedem Arbeitnehmer zustehende Grundrecht fände seine Schranken in den Grundregeln des Arbeitsverhältnisses. Der Betriebsfrieden sei durch die öffentlichen Äußerungen des Arbeitnehmers erheblich gestört worden.

Nehmen wir an, mein Vorgesetzter kommt zu mir als Admin und sagt: ‘In einer Stunde möchte ich alle E-Mails von Mitarbeiter XY mit Datum und Uhrzeit auf meinem Schr*eibtisch haben!’* Kann ich diese Arbeitsanweisung verweigern? Und kann er mir dafür kündigen?

Grundsätzlich darf kein Arbeitgeber von seinen Angestellten rechtswidrige Handlungen verlangen und ihn schon gar nicht wegen einer berechtigten Weigerung kündigen. Eine solche Aufforderung stellt einen eindeutigen Verstoß gegen datenschutzrechtliche Vorschriften dar. Selbst wenn ein generelles Verbot der privaten Internetnutzung am Arbeitsplatz vereinbart wurde, dürfen nur die äußeren Verbindungsdaten wie Zeit, IP- oder E-Mail-Adressen und allenfalls Mail-Header zur Kenntnis genommen werden, nicht aber die Inhalte der Mails. Allenfalls in Ausnahmefällen, etwa bei Verdacht auf eine Straftat, wiegt hier das Interesse des Arbeitgebers schwerer als das Persönlichkeitsrecht des Arbeitnehmers.

Etwas anderes gilt nur dann, wenn sich der Arbeitnehmer in einer Individualvereinbarung ausdrücklich mit der Überwachung seines Internet- und E-Mail-Verkehrs einverstanden erklärt hat oder bei einer Anforderung von Ermittlungsbehörden.

Wenn ein Mitarbeiter für längere Zeit ausfällt, etwa wegen Krankheit, oder eine Kollegin im Mutterschutz ist, dürfen deren E-Mails an einen anderen Kollegen oder Vorgesetzten umgeleitet werden?

Ohne Zustimmung des Betroffenen darf der Arbeitgeber aus datenschutzrechtlichen Gründen auch in diesen Fällen nicht auf die E-Mails eines Arbeitnehmers zugreifen. Sofern sich eine längere Abwesenheit vorher abzeichnet, sollte eine entsprechende Einwilligung eingeholt werden. Ist das nicht möglich, so empfiehlt sich die Einrichtung eines Autoresponders, der potenzielle Geschäftskunden auf eine andere Adresse verweist.

Was passiert mit meinen privaten Mails, wenn ich nicht mehr bei einem Unternehmen *arbeite? Liest die jemand? Oder werden sie mir 'nachgeschickt'?*

Eine Verpflichtung zur Weiterleitung privater Mails nach Beendigung des Arbeitsverhältnisses besteht in aller Regel nicht. Vielmehr hat der Arbeitnehmer selbst dafür zu sorgen, dass die an ihn persönlich gerichteten Mails ihr Ziel auch erreichen. Da das Unternehmen hinsichtlich eines dort nicht mehr tätigen Angestellten eine wesentlich geringere Schutzpflicht hat, steht es ihm frei, derartige Mails nicht anders als sonstige Geschäftspost zu behandeln und sie zu lesen oder zu löschen.

Was kann ich tun, wenn mein Chef ohne mein Einverständnis oder eine entsprechende betriebliche Regelung auf meine persönlichen Daten zugreift?

Erfährt ein Mitarbeiter, dass der Chef oder andere Mitarbeiter im Unternehmen ihn unberechtigt heimlich kontrollieren und unberechtigt Daten über ihn sammeln, kann er über den Betriebsrat, den betrieblichen Datenschutzbeauftragten oder vor dem Arbeitsgericht Unterlassung fordern.

Gibt es ein Persönlichkeitsrecht des Arbeitnehmers auch beim betrieblichen Schriftverkehr?

Nein, zumindest nicht, soweit ein Brief an das 'Unternehmen XY, zu Händen Mitarbeiter Z' adressiert ist. Hier ist für jeden sichtbar, dass es sich um einen betrieblichen Schriftverkehr handelt. Etwas anderes gilt nur, soweit das Schriftstück eindeutig mit dem Vermerk 'persönlich' versehen ist. Das ist bei E-Mails aber am Header nicht eindeutig erkennbar, was die rechtlich unterschiedliche Handhabung erklärt. Insoweit ist die elektronische Post eher mit Telefonanrufen vergleichbar, die ebenfalls nicht ohne Zustimmung des Betroffenen abgehört werden dürfen.

Gelten die Regelungen in Bezug auf das Persönlichkeitsrecht bei der Internetnutzung am Arbeitsplatz auch für Strafverfolger?

Bei Strafverfolgungsbehörden überwiegt das öffentliche Interesse an der Aufklärung einer möglichen Straftat das Persönlichkeitsrecht des Einzelnen erheblich. Besteht also der konkrete nachweisbare Verdacht auf eine Straftat, dürfen die Behörden auf persönliche Daten des Arbeitnehmers zugreifen.

Beim Verdacht auf strafbares Verhaltens hat der Arbeitgeber unmittelbar die Behörden einzuschalten. Ermittelt der Chef auf eigene Faust, muss er damit rechnen, später wegen Verstößen gegen das Arbeitsrecht oder Datenschutzgesetze selbst 'bestraft' zu werden.

*'Soweit ein Arbeitgeber die private Nutzung elekt*ronischer Dienste gestattet, bietet er wie ein normaler Provider Telekommunikationsdienste im Sinne des § 3 des *Telekommunikationsgesetzes (TKG) an'* - Heißt das, der Arbeitgeber ist dann tatsächlich zu behandeln wie ein Internet Service Provider, zum Beispiel T-Online?

Da diese Vorschrift kein gewerbsmäßiges Anbieten von derartigen Dienstleistungen voraussetzt, gilt auch der Arbeitgeber in diesem Fall als normaler Zugangs-Provider. Als solcher darf er grundsätzlich die persönlichen Daten verlangen, die er benötigt, um den Internetzugang zu realisieren und abzurechnen. Sämtliche sonstigen, für diesen Zweck nicht oder nicht mehr notwendigen Informationen müssen jedoch unmittelbar nach dem Ende der Nutzung gelöscht werden. Da keine Abrechnung erfolgt, darf der Arbeitgeber nur solche Daten speichern, die technisch notwendig sind, um einen reibungslosen Betrieb des Unternehmensnetzwerkes zu ermöglichen. Detaillierte Logfiles über die Aktivitäten einzelner Nutzer oder Inhalte von E-Mails fallen sicherlich nicht unter diese Daten.

*Ist der Betrieb von 'Schnüffelsoftware', wie sie teilweise in den USA in Unte*rnehmen eingesetzt wird, in Deutschland legal?

In Deutschland sind technische Überwachungsmöglichkeiten am Arbeitsplatz nur unter bestimmten Voraussetzungen zulässig. Die Einführung technischer Überwachungseinrichtungen wie Videokameras, Telefonüberwachungssysteme oder Software zur Internetüberwachung gehören gemäß § 87 Abs. 1 Nr. 6 BetrVG zu den mitbestimmungspflichtigen Entscheidungen. So ist die Installation von zur Überwachung der Arbeitnehmer geeigneter Software in Betrieben, die der betrieblichen Mitbestimmung unterliegen, nur nach Zustimmung des Betriebsrates möglich. Gibt es keinen Betriebsrat, sind die Beschäftigten durch öffentlichen Aushang von den Maßnahmen detailliert zu informieren.

Informationen zum Thema Kündigung wegen Krankheit

von Rechtsanwalt Dr. Martin Hensche, Fachanwalt für Arbeitsrecht, Berlin

Was ist eine krankheitsbedingte Kündigung?

Wenn Ihr Arbeitsverhältnis unter das KSchG (Kündigungsschutzgesetz) fällt und Sie daher allgemeinen Kündigungsschutz genießen, braucht Ihr Arbeitgeber nicht nur für eine außerordentliche, sondern auch für eine ordentliche Kündigung einen vernünftigen Grund, damit die Kündigung wirksam ist.

Das KSchG bietet dem Arbeitgeber drei Gründe an, nämlich die Kündigung aus Gründen in der Person des Arbeitnehmers, die Kündigung aus Gründen im Verhalten des Arbeitnehmers und die Kündigung aus betriebsbedingten Gründen. Die krankheitsbedingte Kündigung ist der wichtigste Unterfall der Kündigung aus Gründen in der Person des Arbeitnehmers (personenbedingte Kündigung).

Als "krankheitsbedingte Kündigung" bezeichnet man daher eine vom Arbeitgeber ausgesprochene Kündigung, mit der einem Arbeitnehmer, der durch das KSchG geschützt ist, (trotzdem) in rechtlich zulässiger Weise ordentlich gekündigt werden kann, falls der Arbeitnehmer aufgrund seiner Krankheit den Arbeitsvertrag künftig nicht mehr erfüllen kann.

Kann Ihr Arbeitgeber während einer Krankheit kündigen?

Nach dem Arbeitsrecht der ehemaligen DDR (§ 58d Arbeitsgesetzbuch der DDR) war die Kündigung eines Arbeitnehmers während einer Krankheit ausgeschlossen, d.h. der Arbeitnehmer war vor dem Ausspruch einer Kündigung während der Dauer einer Krankheit sicher. Dies war nach dem Recht der BRD niemals so und ist auch heute anders: Das KSchG schützt den Arbeitnehmer entgegen einer weitverbreiteten Ansicht mitnichten vor einer Kündigung, die während einer Krankheit ausgesprochen wird.

Umgekehrt gilt: Die Krankheit des Arbeitnehmers kann unter bestimmten Voraussetzungen sogar der Grund für eine Kündigung durch den Arbeitgeber sein.

Wann kann Ihr Arbeitgeber wegen Krankheit kündigen?

Nach der Rechtsprechung müssen die folgenden drei Voraussetzungen vorliegen, damit eine krankheitsbedingte Kündigung wirksam ist (fehlt auch nur eine dieser Voraussetzungen, ist die Kündigung unwirksam):

1. Es müssen zum Zeitpunkt der Kündigung Tatsachen vorliegen, die die Prognose weiterer Erkrankungen des Arbeitnehmers in dem bisherigen Umfang rechtfertigen. Diese Voraussetzung heißt "negative Gesundheitsprognose".
2. Es muß feststehen, daß die zu erwartenden Fehlzeiten des Arbeitnehmers zu einer erheblichen Beeinträchtigung der betrieblichen oder wirtschaftlichen Interessen des Arbeitgebers führen. Eine solche Interessenbeeinträchtigung liegt vor allem dann vor, wenn es aufgrund der Fehlzeiten des Arbeitnehmers zu Störungen des Betriebsablaufs oder zu erheblichen Belastungen des Arbeitgebers mit Lohnfortzahlungskosten kommt.

3. Schließlich muß eine Interessenabwägung vorgenommen werden. Sie muß zugunsten des Arbeitgebers ausgehen, d.h. sie muß ergeben, daß ihm bei einer umfassenden Abwägung der beiderseitigen Interessen unter Berücksichtigung der Dauer des Arbeitsverhältnisses, der Krankheitsursachen, der Fehlzeiten vergleichbarer Arbeitnehmer und des Lebensalter des Arbeitnehmers die oben festgestellte Beeinträchtigung seiner Interessen (siehe Punkt 2.) nicht mehr weiter zugemutet werden kann.

Wie gesagt müssen diese drei Voraussetzungen allesamt vorliegen. Fehlt auch nur eine, ist die Kündigung unwirksam.

Muss der Arbeitgeber vor der Kündigung eine Abmahnung aussprechen?

Nein. Anders als bei der Kündigung aus verhaltensbedingten Gründen wird dem Arbeitnehmer bei einer krankheitsbedingten Kündigung keine Verletzung des Arbeitsvertrages zum Vorwurf gemacht. Für Krankheiten kann man nichts. Daher ist vor Ausspruch einer Kündigung aus krankheitsbedingten Gründen keine Abmahnung des Arbeitnehmers erforderlich.

Welche Fallkonstellationen gibt es bei der Kündigung wegen Krankheit?

Die Rechtsprechung der Arbeitsgerichte unterscheidet bei der krankheitsbedingten Kündigung vier typische Fallkonstellationen oder Fallgruppen, bei denen die oben genannten drei Voraussetzungen in jeweils etwas anderer Weise zu prüfen sind. Hierbei handelt es sich um die folgenden Fallkonstellationen:

	Fallkonstellation	Besonderheiten
I.	Häufige Kurzerkrankungen	Der Arbeitnehmer ist vor Ausspruch der Kündigung immer wieder für kürzere Zeit, d.h. für einige Tage oder Wochen arbeitsunfähig krank, so daß die Fehlzeiten auf Dauer ein Ausmaß erreichen, das der Arbeitgeber nicht mehr hinnehmen muß.
II.	Dauernde Arbeitsunfähigkeit	Bei Ausspruch der Kündigung steht fest, daß der Arbeitnehmer auf Dauer arbeitsunfähig krank bleiben wird, d.h. daß eine Wiederherstellung der Arbeitsfähigkeit auszuschließen ist.
III.	Langandauernde Krankheit	Hier ist die Wiederherstellung der Gesundheit zum Zeitpunkt der Kündigung zwar nicht ausgeschlossen, doch weiß der Arbeitgeber aufgrund einer bereits länger andauernder Krankheit nicht, ob und wann mit einer Genesung zu rechnen ist.
IV.	Krankheitsbedingte Leistungsminderung	Die Krankheit des Arbeitnehmers führt dazu, daß der Arbeitnehmer auch dann, wenn er bei der Arbeit erscheint, erheblich hinter der zu erwartenden Leistung zurückbleibt.

Wann ist eine Kündigung wegen häufiger Kurzerkrankungen zulässig?

Häufige Kurzerkrankungen des Arbeitnehmers (Fallkonstellation I) stellen dann einen Kündigungsgrund dar, wenn die folgenden drei Voraussetzungen vorliegen.

Negative Gesundheitsprognose: Es muß von weiteren häufigen Kurzerkrankungen in der Zukunft auszugehen sein. Weil der Arbeitgeber die Ursachen der Kurzerkrankungen zum Zeitpunkt der Kündigung zumeist nicht kennt, darf er nach der Rechtsprechung zunächst einmal davon ausgehen, daß ein Arbeitnehmer, der über einen Beobachtungszeitraum von 24 Monaten aufgrund von Kurzerkrankungen insgesamt mehr als sechs Wochen pro Jahr arbeitsunfähig krank war, auch weiterhin oft krank sein wird. Will der Arbeitnehmer diese negative Prognose im Kündigungsschutzprozeß widerlegen, muß er seine Ärzte von der Schweigepflicht entbinden und konkret darlegen, daß seine häufigen Kurzerkrankungen nicht auf ein chronisches Grundleiden, sondern auf voneinander unabhängige Krankheitsursachen zurückzuführen sind und die häufigen Kurzerkrankungen daher letztlich durch eine unglückliche Verkettung von Umständen bedingt sind.

Interessenbeeinträchtigung: Häufige Kurzerkrankungen sind für den Arbeitgeber vergleichsweise teuer, da er immer wieder erneut bis zu sechs Wochen Entgeltfortzahlung leisten muß, wohingegen er bei einer langandauernden Krankheit nur einmal für sechs Wochen zur Entgeltfortzahlung verpflichtet ist und danach die Krankenkasse Krankengeld zahlt. Die Rechtsprechung geht davon aus, daß wirtschaftliche Interessen des Arbeitgebers in der Regel erheblich beeinträchtigt sind, wenn er über einen Zeitraum von zwei aufeinander folgenden Jahren jeweils mehr als sechs Wochen pro Jahr Entgeltfortzahlung leisten muß. Wirtschaftliche Interessen können auch durch Umsatzeinbußen oder durch zusätzliche Personalkosten beeinträchtigt werden. Eine Beeinträchtigung betrieblicher Interessen nimmt die Rechtsprechung an, wenn immer wieder Aushilfskräfte eingearbeitet werden müssen oder wenn der Betriebsfrieden durch die ständige Mehrbelastung von Arbeitskollegen gestört wird.

Interessenabwägung: Hier ist zu prüfen, ob dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls die zu Punkt 2.) festgestellte Beeinträchtigung seiner betrieblichen und/oder wirtschaftlichen Interessen (noch eben gerade) zugemutet oder eben nicht mehr zugemutet werden kann. Da dieser Prüfungspunkt vom jeweiligen Einzelfall abhängt, läßt sich allgemein nur soviel sagen, daß der Arbeitgeber einem Arbeitnehmer, der 20 Jahre zur Zufriedenheit gearbeitet hat, mehr soziale Rücksichtnahme schuldet als einem erst wenige Jahre beschäftigten und bereits von Anfang an immer wieder krankheitsbedingt ausfallenden Arbeitnehmer. Beruhen die Beeinträchtigungen der Interessen des Arbeitgebers allein auf der Belastung mit Lohnfortzahlungskosten, müssen diese nach der Rechtsprechung pro Jahr für mindestens ungefähr 45 bis 60 Krankheitstage anfallen und damit "erheblich" über dem Sechswochenzeitraum des § 3 Entgeltfortzahlungsgesetz liegen.

Wann ist eine Kündigung wegen dauernder Arbeitsunfähigkeit zulässig?

Bei krankheitsbedingter dauernder Leistungsunfähigkeit des Arbeitnehmers (Fallkonstellation II) ist die Gesundheitsprognose offensichtlich negativ.

Zudem ist in der Regel ohne weiteres von einer erheblichen Beeinträchtigung der (betrieblichen) Interessen des Arbeitgebers auszugehen, d.h. eine Interessenbeeinträchtigung liegt in aller Regel vor. Dies kann ausnahmsweise einmal anders sein, falls der Arbeitnehmer auf einem anderen, "leidensgerechten" Arbeitsplatz weiter beschäftigt werden kann.

Liegt dauernde Leistungsunfähigkeit vor und ist ein leidensgerechter Arbeitsplatz nicht vorhanden, kann die Interessenabwägung nur in seltenen Ausnahmefällen einmal zugunsten des Arbeitnehmers ausgehen.

Im Falle einer krankheitsbedingten dauernden Leistungsunfähigkeit des Arbeitnehmers ist eine Kündigung daher in der Regel zulässig.

Wann ist eine Kündigung wegen langandauernder Krankheit zulässig?

Eine langandauernde Krankheit des Arbeitnehmers (Fallkonstellation III) stellt einen Kündigungsgrund dar, wenn die folgenden drei Voraussetzungen vorliegen.

Negative Gesundheitsprognose: Der Arbeitnehmer muß zum Zeitpunkt der Kündigung bereits "seit längerer Zeit" arbeitsunfähig erkrankt sein. Hier geht es praktisch um Fälle, in denen der Arbeitnehmer zumindest mehr als sechs Wochen bzw. einige Monate lang krank war. Weiterhin muß die Krankheit zum Zeitpunkt der Kündigung für voraussichtlich längere oder für nicht absehbare Zeit andauern. Die Frage, wie lange denn nun die "voraussichtlich längere" Krankheit voraussichtlich dauern muß, damit eine Kündigung zulässig ist, wird durch die Rechtsprechung nicht klar beantwortet, so daß eine Kündigung wegen langandauernder Krankheit mit erheblichen Unsicherheiten für den Arbeitgeber verbunden ist. Klarheit schafft nur die folgende, vom BAG aufgestellte Regel: Ist ausweislich ärztlicher Gutachten mit einer Genesung in den nächsten 24 Monaten nach Ausspruch der Kündigung nicht zu rechnen, steht diese Ungewißheit einer krankheitsbedingten dauernden Arbeitsunfähigkeit (Fallkonstellation II.) rechtlich gleich (BAG, Urteil vom 12.04.2002, 2 AZR 148/01, NZA 2002, S.1081), so daß die Kündigung in einem solchen Fall in der Regel wirksam ist. Da allerdings ein Arzt die Genesung innerhalb eines so langen Zeitraums (24 Monate!) kaum definitiv ausschließen wird, ohne zugleich eine dauerhafte Arbeitsunfähigkeit zu diagnostizieren, ist der praktische Anwendungsbereich dieser Regel gering.

Interessenbeeinträchtigung: Die langandauernde Krankheit muß betriebliche oder wirtschaftliche Interessen des Arbeitgebers beeinträchtigen. Da der Arbeitgeber nach Ablauf von sechs Wochen in der Regel keine weitere Entgeltfortzahlung mehr leisten muß, ist eine Beeinträchtigung wirtschaftlicher Interessen selten gegeben, weshalb die die Rechtsprechung auch dazu tendiert, die Kündigung wegen langandauernder Krankheit einzugrenzen. Der Arbeitgeber muß daher eine erhebliche Beeinträchtigung betrieblicher Interessen darlegen, die sich aus organisatorischen Problemen bei der zeitlich begrenzten Einstellung von Ersatzkräften ergeben kann. - Steht ausnahmsweise einmal fest, daß eine Genesung in den nächsten 24 Monaten auszuschließen ist, liegt eine Interessenbeeinträchtigung (wie bei der Kündigung wegen dauernder Leistungsunfähigkeit) in der Regel ohne weiteres vor.

Interessenabwägung: Hier ist zu prüfen, ob dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls die zu Punkt 2.) festgestellte Beeinträchtigung seiner Interessen (noch eben gerade) zugemutet oder nicht mehr zugemutet werden können. Hier fragt sich vor allem, ob weitere Überbrückungsmaßnahmen nicht mehr möglich sind und daher das Beendigungsinteresse des Arbeitgebers überwiegt. Zudem kommt es natürlich auch hier auf die soziale Situation des Arbeitnehmers an, d.h. auf Alter, Dauer der Betriebszugehörigkeit, Unterhaltsverpflichtungen, Chancen auf dem Arbeitsmarkt usw.

Wann ist eine Kündigung wegen Leistungsminderung zulässig?

Bei krankheitsbedingter Leistungsminderung des Arbeitnehmers (Fallkonstellation IV) ist die Gesundheitsprognose nur negativ, wenn aufgrund vergangener erheblicher Leistungsminderungen auch für die weitere Zukunft mit solchen, d.h. mit erheblichen Minderleistungen zu rechnen ist.

Bei hinreichend gravierenden Leistungsminderungen ist in der Regel von einer erheblichen Beeinträchtigung der wirtschaftlichen Interessen des Arbeitgebers auszugehen. Eine Interessenbeeinträchtigung liegt aber dann nicht vor, wenn der Arbeitnehmer kann auf einem anderen, seiner verminderten Leistungsfähigkeit entsprechenden Arbeitsplatz weiter beschäftigt werden kann.

Liegt eine krankheitsbedingte Leistungsminderung vor, ist eine umfassende Interessenabwägung wie bei Fallkonstellation I. und Fallkonstellation III. anzustellen.

Wann ist eine krankheitsbedingte Kündigung auf jeden Fall unwirksam?

Wie Sie unter dem Stichwort "Kündigungsschutz" nachlesen können, kann der Arbeitgeber bei jeder Kündigung - und also auch bei jeder krankheitsbedingten Kündigung - an bestimmten "Stolpersteinen" scheitern.

So ist zum Beispiel eine Kündigung generell unwirksam, wenn es in dem Betrieb, in dem Sie arbeiten, einen Betriebsrat gibt und Ihr Arbeitgeber den Betriebsrat vor Ausspruch der Kündigung nicht angehört hat.

Unwirksam ist oft auch die Kündigung bestimmter Arbeitnehmergruppen (Mitglieder des Betriebsrats, Schwangere, schwerbehinderte Arbeitnehmer), da der Arbeitgeber hier besondere Voraussetzungen beachten muß, also zum Beispiel vor der Kündigung eines schwerbehinderten Arbeitnehmers die Zustimmung des Integrationsamtes einholen muß u.s.w.

Was tun bei einer krankheitsbedingten Kündigung?

Wenn Sie eine krankheitsbedingte Kündigung erhalten haben, müssen Sie sich innerhalb von drei Wochen nach Zugang der Kündigung entscheiden, ob Sie dagegen Kündigungsschutzklage erheben wollen oder nicht. Wenn Sie diese in § 4 Satz 1 KSchG bestimmte Frist für die Erhebung der Klage versäumen, gilt die Kündigung als von als von Anfang an rechtswirksam (§ 7 KSchG).

Es ist daher von allergrößter Wichtigkeit, daß Sie die gesetzliche Dreiwochenfrist für die Kündigungsschutzklage beachten.

Dies gilt nicht nur dann, wenn Sie mit einer Klage Ihre weitere Beschäftigung durchsetzen wollen. Die Einhaltung der Frist ist genauso wichtig, wenn Sie das Ziel verfolgen, eine gute Abfindung auszuhandeln. Ist die Klagefrist nämlich einmal versäumt, ist eine Kündigungsschutzklage praktisch aussichtslos. In einer solchen Situation wird sich Ihr Arbeitgeber normalerweise auf keine Abfindung mehr einlassen.

Wenn Sie eine Rechtsschutzversicherung haben oder rechtliche Vertretung durch Ihre Gewerkschaft beanspruchen können, riskieren Sie durch eine Kündigungsschutzklage in der Regel nichts. Auf der anderen Seite erhalten Sie in vielen Fällen durch eine Klage die Chance auf eine Abfindung.

Haben Sie keine Möglichkeit einer Kostenerstattung durch eine Rechtsschutzversicherung oder durch die Gewerkschaft, stehen Sie vor der Entscheidung, entweder nichts zu unternehmen oder selbst zu klagen oder sich auf eigene Kosten von einem Rechtsanwalt vertreten zu lassen. Wegen der Schwierigkeiten des Kündigungsschutzrechts sollten Sie sich zumindest anwaltlich über die Erfolgsaussichten einer Klage beraten lassen. Außerdem besteht in je nach Ihrer finanziellen Lage die Möglichkeit, daß der Staat die Kosten für Ihren Rechtsanwalt im Wege der Prozeßkostenhilfe übernimmt.

Claudia Krauß *

Internet am Arbeitsplatz

JurPC Web-Dok. 14/2004, Abs. 1 - 52

Inhaltsübersicht:

A. Einführung

B. Datenschutz-Aspekt
I. TKG
1. Dienstliche Nutzung
2. Private Nutzung
a) Erlaubte private Nutzung
b) Unerlaubte private Nutzung
c) Auswirkung der Anwendbarkeit des TKG
II. TDDSG
1. Dienstliche Nutzung
2. Private Nutzung
III. BDSG und Allgemeines Persönlichkeitsrecht
1. Anwendbarkeit des BDSG
2. Überwachung von E-Mail-Inhalten
3. Überwachung der äußeren Verbindungsdaten

C. Arbeitsrecht-Aspekt
I. Ordentliche Kündigung
II. Außerordentliche Kündigung
III. Verwertbarkeit der erhobenen und gespeicherten Daten als Beweismittel

D. Fazit

A. Einführung

JurPC Web-Dok. 14/2004, Abs. 1

Die modernen Kommunikationstechniken wie E-Mailing, Internet- und Intranetnutzung gehören heute in den meisten Unternehmen und Konzernen zum Berufsalltag. Sie ermöglichen den Unternehmen auf relativ schnellem und einfachem Weg die Kommunikation und den Datenaustausch mit Kunden und Partnern in aller Welt. Diese Arbeitsmittel werden jedoch von den Arbeitnehmern häufig nicht nur zur Erledigung ihrer dienstlichen Aufgaben genutzt. Nach einer Studie des Bonner Informationsdienstes "Neues Arbeitsrecht für

Vorgesetzte" surfen oder mailen über 90% aller vernetzten Arbeitnehmer im Büro auch zu privaten Zwecken. Und die Hälfte davon sogar länger als 3 Stunden pro Woche. Nach Schätzungen soll den Firmen hierbei ein Schaden von etwa 50 Milliarden Euro jährlich entstehen(1). Hier werden dann auch bereits die ersten Interessengegensätze deutlich, die zwischen den Arbeitnehmern und den Arbeitgebern entstehen. Der Arbeitgeber hat ein Interesse daran, die E-Mail und Internetaktivitäten seiner Arbeitnehmer zu beschränken und zu kontrollieren. Die private Nutzung bindet Arbeitszeit und verursacht Kosten. Außerdem ist nicht auszuschließen, dass der Arbeitnehmer Computer-Viren in das betriebliche EDV-Netz einschleppt. Oder sogar bewusst unerlaubte Handlungen vornimmt, wie z.B. das Herunterladen unautorisierter Software, der Verrat von Betriebs- und Geschäftsgeheimnissen. Hier sind vielerlei Fallgestaltungen denkbar.

Abs. 2

Gegebenenfalls will der Arbeitgeber diese Aktivitäten des Arbeitnehmers zum Anlass für eine Kündigung nehmen. Auf der anderen Seite hat der Arbeitnehmer ein Recht darauf, dass seine persönlichen Daten geschützt werden. Er muss auch aus psychischen und physischen Gründen sicher sein, dass er keiner dauerhaften und umfassenden Überwachung unterliegt. Intensive Kontrollen, die quasi zum "Gläsernen Arbeitnehmer" führen würden, können zu Stress und Depressionen führen. Jeder braucht eine Privatsphäre - auch auf dem Arbeitsplatz. Thema der Arbeit ist daher auch, wie dieser Interessenkonflikt zur Zufriedenheit beider Seiten gelöst werden könnte. Gegebenenfalls unter Einbeziehung des Betriebsrates, falls ein solcher vorhanden ist.

Abs. 3

Zu Grunde gelegt sind dieser Arbeit nur private Arbeitsverhältnisse. Für den Bereich des öffentlichen Dienstes kann sich bei dem einen oder anderen Gesichtspunkt ein Unterschied ergeben.

Abs. 4

Die beiden Hauptaspekte der Arbeit sind zum einen die Datenschutzregelungen, die der Arbeitgeber eventuell zu beachten hat, und zum anderen die arbeitsrechtlichen Konsequenzen, die er aus den gewonnenen Daten ziehen darf.

Abs. 5

Zu unterscheiden sind folgende Fallkonstellationen:

- Der Arbeitgeber gestattet ausdrücklich nur die dienstliche Nutzung von Internet und E-Mail.
- Der Arbeitgeber erlaubt ausdrücklich auch die Nutzung für private Zwecke.
- Der Arbeitgeber trifft gar keine ausdrückliche Regelung.

B. Datenschutz-Aspekt

Ein einheitliches Arbeitnehmer-Datenschutzgesetz besteht derzeit nicht. Es wurde zwar unter Arbeitsminister Riester im Jahr 2000 geplant, ein Arbeitnehmer-Datenschutzgesetz vorzulegen. dies ist bis dato jedoch nicht geschehen. Eine gefestigte, insbesondere höchstrichterliche Rechtsprechung zu den Kontrollbefugnissen des Arbeitgebers bei der Internet-/ Intranet-/ E-Mail-Nutzung durch den Arbeitnehmer gibt es ebenfalls noch nicht. Abs. 6

Normen, die gegebenenfalls anzuwenden sind, finden sich im Telekommunikationsgesetz (TKG), im Teledienstedatenschutzgesetz (TDDSG) und im Bundesdatenschutzgesetz (BDSG). Zugrunde zu legen ist dabei auch immer das grundrechtlich verbriefte allgemeine Persönlichkeitsrecht. Abs. 7

I. TKG

Grundsätzlich ist das TKG anzuwenden, wenn eine Telekommunikationsdienstleistung vorliegt oder geschäftsmäßig ein Telekommunikationsdienst erbracht wird. Gem. § 3 Nr. 18 TKG liegt eine Telekommunikationsdienstleistung dann vor, wenn es sich bei der Überlassung der Telekommunikationsanlagen um ein gewerbliches Angebot handelt. Maßgeblich ist hierfür, dass der Anbieter in einer Gewinnerzielungsabsicht handelt. Dies ist im Verhältnis Arbeitgeber/Arbeitnehmer regelmäßig nicht der Fall. Der Betriebszweck liegt normalerweise nicht darin, dem Arbeitnehmer Telekommunikationsdienste zu verkaufen. Nach Nr. 5 der gleichen Vorschrift ist das TKG aber auch auf das geschäftsmäßige Erbringen eines Telekommunikationsdienstes anwendbar. Gemeint ist damit das Angebot von Telekommunikation an einen Dritten. Auf eine Gewinnerzielungsabsicht kommt es in dieser Variante nicht an(2). Fraglich ist vielmehr, ob der Arbeitnehmer "Dritter" ist. Hier ergeben sich Unterschiede, je nachdem in welcher Form dem Arbeitnehmer die Nutzung gestattet oder gerade nicht gestattet ist. Abs. 8

1. Dienstliche Nutzung:

Hat der Arbeitgeber die private Nutzung ausdrücklich Abs. 9

untersagt und nur die dienstliche Nutzung gestattet, ist nach herrschender Meinung der Arbeitnehmer nicht als "Dritter" im Sinne der Vorschrift anzusehen(3). Nach anderer Ansicht soll "Dritter" jeder sein, dem der Dienst in technischer Hinsicht erbracht wird - also auch der Arbeitnehmer(4). Die herrschende Meinung erscheint mir überzeugender. Im Falle rein dienstlicher Nutzung wird dem Arbeitnehmer kein Angebot unterbreitet, dass er nutzen oder ignorieren kann. Die Dienste stellen für ihn Arbeitsmittel dar, die ausschließlich den Zwecken des Arbeitgebers dienen. Der Arbeitnehmer steht in diesem Fall also quasi "im Lager" des Arbeitgebers und ist kein "Dritter". Das TKG findet in diesem Fall daher keine Anwendung.

2. Private Nutzung:

Bei der privaten Nutzung ist zu unterscheiden, ob sie vom Arbeitgeber erlaubt worden ist oder nicht. Hier ist zunächst zu fragen, wann eine Erlaubnis zur privaten Nutzung überhaupt vorliegt. Abs. 10

a.) erlaubte private Nutzung

Sie liegt im einfachsten Fall vor, wenn der Arbeitgeber sie ausdrücklich erlaubt hat. Dann ist der Arbeitnehmer als Dritter anzusehen und das TKG anzuwenden. Der Arbeitnehmer kann vom Angebot des Arbeitgebers Gebrauch machen oder nicht. Der Arbeitgeber erbringt die Leistung hier zumindest auch für andere Zwecke. Abs. 11

Was ist aber, wenn keine ausdrückliche Regelung getroffen worden ist? Abs. 12

Der Arbeitsvertrag gibt dem Arbeitnehmer im Normalfall kein Recht, die Telekommunikationsmittel des Arbeitgebers für eigene Zwecke zu verwenden. Es besteht grundsätzlich ein Verbot der Privatnutzung. Es gelten für die Internet- und E-Mail-Nutzung dieselben Grundsätze wie für den Bereich des privaten Telefonierens vom Dienstapparat aus(5). Ausnahmen des grundsätzlichen Verbots der Privatnutzung kommen allenfalls bei Pflichtenkollisionen und Notfällen und aus dienstlichem Anlass in Betracht. Etwa, wenn ein Arbeitnehmer seinem Partner per E-Mail mitteilt, dass er aufgrund von Überstunden erst später nach Hause kommt. Abs. 13

Die Erlaubnis zur Nutzung kann sich konkludent ergeben. Durch betriebliche Übung oder die konkreten Umstände. Für die Annahme betrieblicher Übung ist erforderlich, Abs. 14

dass der Arbeitnehmer in Kenntnis des Arbeitgebers über einen längeren Zeitraum das Internet für private Zwecke genutzt hat und der Arbeitgeber dies duldet. Nähere Umstände, die ebenfalls für eine Erlaubnis sprechen, sind z.B., dass der Arbeitgeber in der Kantine Internetzugänge bereitstellt oder die Nutzung gegenüber dem Arbeitnehmer abrechnet. Ein weiterer Anhaltspunkt kann auch sein, dass Privattelefonate ausdrücklich erlaubt sind(6). In all diesen Fällen, hat der Arbeitgeber die Regelungen des TKG zu beachten(7).

b.) unerlaubte private Nutzung:

Ist die Nutzung nicht gestattet, erbringt der Arbeitgeber auch keine Telekommunikationsdienste für Dritte. Die Bereitstellung der Dienste soll keinesfalls fremden, sondern nur den eigenen Zwecken dienen(8). Abs. 15

c.) Auswirkung der Anwendbarkeit des TKG:

Dies führt zum Ergebnis, dass der Arbeitgeber nur für den Fall, dass er seinen Arbeitnehmern auch die private Mitbenutzung gestattet hat, die Regelungen des TKG beachten muss. Abs. 16

Dies bedeutet vor allen Dingen, dass er Sorge dafür zu tragen hat, dass das in § 85 TKG normierte Fernmeldegeheimnis gewahrt wird(9). Das Fernmeldegeheimnis verpflichtet den Arbeitgeber strikt dazu, die Verwendung von Daten auf das für das Erbringen der Leistung erforderliche Maß zu beschränken (§ 85 Abs. 3 Satz 1 TKG). Demnach ist die Erfassung und Verwendung der Arbeitnehmer-Daten allenfalls zum Zwecke der Abrechnung und zur Sicherstellung eines geregelten Kommunikationsablaufes zulässig. Der Arbeitgeber darf keine Kenntnis von Inhalten oder den Beteiligten der Kommunikation erlangen(10). Das Fernemeldegeheimnis kann allerdings durch Individualabrede oder Betriebsvereinbarung abbedungen werden(11). Was dem Arbeitgeber zu empfehlen ist, will er die Daten zur Kontrolle dafür verwenden, ob die Arbeitsleistung des Arbeitnehmers durch die Privatnutzung eingeschränkt wird. Das TKG enthält außer dem Fernemeldegeheimnis auch Anforderungen hinsichtlich technischer und organisatorischer Schutzvorkehrungen. Der Arbeitgeber hat die unbefugte Kenntnisnahme von erhobenen Daten durch Dritte zu verhindern. Hierfür ist der Stand der Technik und der von der Regulierungsbehörde und dem Bundesamt für Abs. 17

Sicherheit in der Informationstechnik erstellte Sicherheitskatalog zu berücksichtigen. Für einen Arbeitgeber, dessen Hauptgeschäft nicht bereits in der Erbringung von Telekommunikationsdiensten besteht, bringen die erforderlichen Schutzmaßnahmen einen erheblichen Kosten- und Mehraufwand mit sich(12).

II. TDDSG:

Das TDDSG enthält datenschutzrechtliche Bestimmungen für Anbieter von Telediensten. Was ein Teledienst ist, wird im TDDSG selbst nicht erläutert. Es verweist hierfür auf das Teledienstegesetz (TDG). Nach § 2 TDG sind unter einem Teledienst alle elektronischen Informations- und Kommunikationsdienste zu verstehen, die für eine individuelle Nutzung von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zu Grunde liegt. Telekommunikation ist dabei die Sammelbezeichnung für alle Formen der Nachrichtenübertragung mit Anlagen der Informationstechnik bedeutet. Rechnernetze wie das Internet fallen unstreitig darunter. Abs. 18

1. Dienstliche Nutzung:

Da das TDDSG ein Anbieter-Nutzer-Verhältnis voraussetzt, ist es für den Fall der ausschließlich dienstlichen Nutzung nicht anzuwenden. Der Arbeitnehmer hat nicht die Möglichkeit, die Nutzung grundsätzlich abzulehnen, was für ein Anbieter-Nutzer-Verhältnis aber erforderlich wäre(13). Abs. 19

2. Private Nutzung:

Lässt der Arbeitgeber die private Nutzung zu, wird der Arbeitnehmer zum Nutzer, der unabhängig vom Arbeitsverhältnis das Angebot des Arbeitgebers ablehnen kann. Im Falle der unerlaubten Nutzung ist der Arbeitgeber kein Anbieter. Er will ja gerade nicht, dass der Arbeitnehmer den Dienst für private Zwecke nutzt. Abs. 20

Somit ist auch das TDDSG nur für den Fall der ausdrücklich oder konkludent erlaubten Privatnutzung anwendbar(14). Abs. 21

Nach dem TDDSG darf der Arbeitgeber Daten im Zusammenhang mit der Nutzung nur erheben und verwenden, um dem Nutzer die Inanspruchnahme des Dienstes zu ermöglichen oder um die Nutzung abzurechnen (§ 6 Abs. 1 TDDSG). Weitere Abs. 22

Kontrollbefugnisse stehen dem Arbeitgeber nicht zu.

III. BDSG und Allgemeines Persönlichkeitsrecht:

1. Anwendbarkeit des BDSG:

Die Regelungen des Bundesdatenschutzgesetzes sind im Zusammenhang mit dem allgemeinen Persönlichkeitsrecht zu sehen. Abs. 23

Das BDSG unterscheidet zwischen "öffentlichen" und "nicht-öffentlichen" Stellen. Nicht-öffentliche Stellen sind dabei gem. § 2 Abs. 4 BDSG natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts. Private Arbeitgeber fallen somit unter den Begriff der nicht-öffentlichen Stellen(15). Abs. 24

Die Zulässigkeit der Datenverarbeitung durch nicht-öffentliche Stellen wird in § 28 BDSG geregelt. Danach dürfen Private personenbezogene Daten dann speichern und verwenden, wenn dies "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlicher Verhältnisse mit dem Betroffenen erfolgt" oder "soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung offensichtlich überwiegt". An dieser Stelle ist das allgemeine Persönlichkeitsrecht, das auch das Recht auf informationelle Selbstbestimmung umfasst, mit einzubeziehen(16). Zur Begriffsbestimmung ist zu erklären, dass personenbezogenen Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person darstellen. Abs. 25

Der Arbeitsvertrag ist ein Vertragsverhältnis i.S.v. § 28 BDSG. Es muss also bei der Frage der Datenerhebung der Schutz des Persönlichkeitsrechtes gegenüber den berechtigten Interessen des Arbeitgebers abgewogen werden. Hierbei hat eine umfassende Güter- und Interessenabwägung zu erfolgen. Das allgemeine Persönlichkeitsrecht gilt nämlich nicht schrankenlos. Es findet seine Grenzen dort, wo berechtigte Interessen des Arbeitgebers bestehen(17). Abs. 26

Der Arbeitgeber hat als Gläubiger der Arbeitsleistung ein berechtigtes Interesse daran, dass diese erbracht wird und keine strafbaren Handlungen vom Arbeitsplatz aus vorgenommen werden(18). Als Rechtfertigung eines Eingriffs in das Persönlichkeitsrecht des Arbeitnehmers Abs. 27

kommen daher in Betracht:

- Unterbindung von E-Mails, deren Inhalt geeignet ist, einen Straftatbestand zu erfüllen
- Unberechtigte Weitergabe von Betriebs- und Unternehmensgeheimnissen
- Schutz der firmeneigenen Dateien vor Viren
- Vermeidung der Kostensteigerung durch die unberechtigte Inanspruchnahme der EDV-Einrichtungen.

2. Überwachung von E-Mail-Inhalten:

Die Überwachung von E-Mail-Inhalten beeinträchtigt das Persönlichkeitsrecht des Arbeitnehmers in sehr erheblichem Maße. Sie ist daher grundsätzlich unzulässig. Abs. 28

Fraglich ist aber, ob dies auch für dienstliche E-Mails gilt. Der Arbeitgeber ist grundsätzlich befugt, dienstliche Korrespondenz einzusehen(19). Allerdings hat die Rechtsprechung das heimliche Mithören dienstlicher Telefonate als nicht zulässig angesehen. Nach herrschender Auffassung ist eine E-Mail eine schriftliche Äußerung und soll daher vom Arbeitgeber ebenso eingesehen werden können wie eine in herkömmlicher Papierform geführte Akte. Der Arbeitgeber soll jederzeit den Arbeitnehmer auffordern können, ihm die dienstliche E-Mail zugänglich zu machen, z.B. durch Ausdrucken. Begründet wird diese Auffassung damit, dass die E-Mail-Nachricht erst erstellt werden muss und der Inhalt daher dem Verfasser vor Augen liegt. Es fehle daher am - für das gesprochene Wort typischen - Augenblicksmoment. Äußerungen unter vier Augen erfolgten in aller Regel im Bewusstsein der Flüchtigkeit und jederzeitigen Korrigierbarkeit und würden daher nicht der Weise vorher überlegt wie schriftliche Äußerungen. Daher habe die Rechtsprechung das heimliche Mithören von dienstlichen Telefonaten für unzulässig erklärt. Bei der E-Mail wisse der Absender, dass seine Nachricht dem Empfänger "schwarz auf weiß" vor Augen liegt und er sich daran festhalten lassen muss. Insoweit sei der Vorgang keineswegs so schnell wie das sog. flüchtige Wort im Telefonat(20). Nach anderer Auffassung soll ein Zugriff auf die Inhalte dienstlicher E-Mails dem Arbeitgeber grundsätzlich verwehrt sein, wenn ihm nicht überwiegende Belange als Rechtfertigung zur Seite stehen(21). Abs. 29

3. Überwachung der äußeren Verbindungsdaten:

Die äußeren Verbindungsdaten wie Datum, Absender, Dauer der Verbindung dürfen uneingeschränkt festgestellt werden(22). Die Empfängeradresse dagegen bei privaten E-Mails nicht. Es wäre daher zu empfehlen, dass die Arbeitnehmer private E-Mails besonders kennzeichnen oder sogar für die private Nutzung einen eigenen Account unabhängig vom dienstlichen erhalten. Abs. 30

Die Erhebung und Verarbeitung personenbezogener Daten steht nach § 4 BDSG unter einem Erlaubnisvorbehalt. Der Arbeitnehmer kann also durch Individualabrede oder Betriebsvereinbarung in die Erhebung und Nutzung seiner Daten einwilligen. Dabei hat eine Betriebsvereinbarung gem. § 75 Betriebsverfassungsgesetz aber ebenfalls das Persönlichkeitsrecht des Arbeitnehmers zu wahren. Abs. 31

BDSG und Persönlichkeitsrecht gelten für die dienstliche und die private Nutzung gleichermaßen. Soweit das TKG anwendbar ist, verdrängt es als speziellere Regelung das BDSG. Auch im Falle unerlaubter privater Nutzung gilt das BDSG. Nur weil die Nutzung nicht erlaubt ist, ist nicht automatisch den betrieblichen Belangen der Vorzug einzuräumen. Die Berufung auf das allgemeine Persönlichkeitsrecht ist nicht rechtsmissbräuchlich. Abs. 32

Zusammenfassend lässt sich danach feststellen, dass eine Kontrolle von privaten E-Mail-Inhalten nur erfolgen darf, wenn ein begründeter Verdacht strafbarer Handlungen vorliegt. Die Kontrolle der äußeren Verbindungsdaten greift weniger schwer in das Persönlichkeitsrecht des Arbeitnehmers ein und ist daher zulässig. Abs. 33

C. Arbeitsrecht-Aspekt:

Überwacht der Arbeitgeber nun die Daten seiner Arbeitnehmer, stellt sich die Frage, inwiefern er aus den ermittelten und gespeicherten Daten arbeitsrechtliche Konsequenzen darf. Die bisher veröffentlichte - nicht sehr zahlreiche - Rechtsprechung legt einen an die Rechtsprechung zu den Folgen privater Telefonate angelehnten Maßstab an. Eine Entscheidung des BAG liegt bisher nicht vor. Abs. 34

Eine Verletzung der arbeitsvertraglichen Pflichten durch den Arbeitnehmer ist in folgenden Fallkonstellationen denkbar: Abs. 35

- Der Arbeitnehmer nutzt Internet und E-Mail für private Zwecke, obwohl dies nicht gestattet ist.
- Der Arbeitgeber hat die Nutzung in begrenztem Umfang gestattet und der Arbeitnehmer überschreitet diese

Grenzen.
- Der Arbeitnehmer nimmt mittels Internet und E-Mail strafbare Handlungen vor.

In Betracht kommen sowohl die ordentliche als auch die außerordentliche verhaltensbedingte Kündigung des Arbeitnehmers. Abs. 36

I. Ordentliche Kündigung:

Ist das Kündigungsschutzgesetz anwendbar - hat der Betrieb also mehr als 5 Arbeitnehmer und besteht das Arbeitsverhältnis länger als 6 Monate - ist eine ordentliche Kündigung grundsätzlich gerechtfertigt, wenn das Verhalten des Arbeitnehmers von Bedeutung für das betriebliche Geschehen ist(23). Abs. 37

Die unerlaubte Privatnutzung stellt grundsätzlich einen Verstoß im Leistungsbereich dar. Bei einem Verstoß im Leistungsbereich bedarf es vor dem Ausspruch einer Kündigung in der Regel einer einschlägigen erfolglosen Abmahnung(24). Nach der neueren Rechtsprechung des BAG ist auch für die Kündigung wegen Verstoßes im Vertrauensbereich eine vorherige Abmahnung erforderlich(25). Einen Verstoß im Vertrauensbereich stellt z.B. der Verrat von Betriebsgeheimnissen oder das Herunterladen von Seiten mit pornographischem Inhalt dar. Abs. 38

Entbehrlich ist eine Abmahnung nur dann, wenn der Arbeitnehmer nicht gewillt ist, sich vertragsgerecht zu verhalten oder bei besonders schwerwiegenden Pflichtverletzungen(26). Dies hat die Rechtsprechung bisher für den Fall des Herunterladens pornographischer Dateien angenommen. Abs. 39

Für den Fall der übermäßigen Privatnutzung hat das Arbeitsgericht Wesel entschieden, dass eine Nutzungsdauer von 80 bis 100 Stunden innerhalb eines Jahres keine für den Arbeitnehmer erkennbare Pflichtverletzung darstelle(27). Dies gilt jedoch nur, wenn die private Nutzung nicht ausdrücklich ausgeschlossen ist. Abs. 40

Ist das Kündigungsschutzgesetz nicht anwendbar, braucht der Arbeitnehmer zwar grundsätzlich keinen Kündigungsgrund anzugeben. Nach der Rechtsprechung des BVerfG ist aber aus Art. 12 GG ein grundrechtlich verbürgter Schutz des Arbeitnehmers vor willkürlichen Kündigungen herzuleiten(28). Sowohl die unerlaubte Privatnutzung als auch die Schädigung des Arbeitgebers stellen einen ausreichenden Grund für eine ordentliche Abs. 41

Kündigung dar(29).

II. Außerordentliche Kündigung:

In besonders schwerwiegenden Fällen oder wenn bei weniger schwerwiegenden Fällen bereits mehrfach erfolglos abgemahnt worden ist, kommt auch eine außerordentliche Kündigung gem. § 626 I BGB in Betracht. Für den Fall des Herunterladens pornographischer Daten haben die Arbeitsgerichte bisher uneinheitlich entschieden. Das Arbeitsgericht Frankfurt hat eine außerordentliche Kündigung für nicht gerechtfertigt gehalten, weil das Schwergewicht der den Kündigungsgrund bildenden Störung in der Wiederholungsgefahr liege und der Arbeitgeber dieser Gefahr bis zum Ablauf der Kündigungsfrist begegnen könne(30). Das Arbeitsgericht Düsseldorf hat in einem ähnlich gelagerten Fall die fristlose Kündigung für gerechtfertigt gehalten, weil es eine Wiederherstellung des Vertrauens zwischen Arbeitgeber und Arbeitnehmer für ausgeschlossen hielt(31). Abs. 42

Als wichtiger Kündigungsgrund i.S.v. § 626 BGB kann auch die Schädigung des Ansehens des Arbeitgebers zu berücksichtigen sein. Jede Internetnutzung hinterlässt Spuren, die von sachkundigen Dritten zurückverfolgt werden könne. Dadurch kann festgestellt werden, von welchem Internetzugang auf eine Homepage zugegriffen worden ist, bzw. von wo aus eine Homepage ins Netz gestellt worden ist(32). Abs. 43

III. Verwertbarkeit der erhobenen und gespeicherten Daten als Beweismittel:

Für den Arbeitsgerichtprozess stellt sich über dem die Frage, inwiefern Daten, die der Arbeitgeber durch Überwachungseinrichtungen gewonnen hat, verwertet werden können. Abs. 44

Das deutsche Arbeitsrecht kennt bisher keine besonderen Regelungen für die Verwertbarkeit solcher Informationen. Nach der EG-Datenschutzrichtlinie 46/95 darf sich ein Arbeitgeber nicht auf rechtswidrig gewonnene Daten beziehen. Ein Arbeitgeber, der eine Abmahnung oder Kündigung aufgrund solcher Daten ausspricht, bedient sich der "Früchte des verbotenen Baumes" und kann diese nicht als Beweis in den arbeitsgerichtlichen Prozess einführen(33). Abs. 45

Speichert der Arbeitnehmer aber die Daten auf dem Dienst-PC ab, gehören diese Daten nicht mehr zu seiner Privatsphäre. Es sei denn, der Rechner sei ihm zu rein privaten Zwecken übergeben worden(34). Abs. 46

D. Fazit:

Zusammenfassend lässt sich für den Bereich des Datenschutzes feststellen, dass die Inhaltskontrolle privater E-Mails unabhängig von der Erlaubnis der Privatnutzung nur erfolgen darf, wenn ein begründeter Verdacht besteht, dass das Verhalten des Arbeitnehmers einen Straftatbestand erfüllt. Bei dienstlichen E-Mails ist die Einsicht durch den Arbeitgeber zulässig. Abs. 47

Die Feststellung der äußeren Verbindungsdaten bei E-Mails ist dagegen immer zulässig. Die Empfängeradresse darf zum Schutz der Daten der Empfänger jedoch nur bei dienstlichen E-Mails vollständig erfasst und gespeichert werden. Daher ist es notwendig, dass der Arbeitnehmer entweder die privaten E-Mails kennzeichnet, oder dass er vom Arbeitgeber einen eigenen Account für seine private Nutzung erhält. Abs. 48

Die Überwachung der Internetaktivitäten des Arbeitnehmers stellt einen geringeren Eingriff dar, da hier meist keine persönlichen Informationen offenbart werden. Da aber auch von Web-Sites E-Mails versandt werden können, ist nur die Kontrolle der äußeren Daten zulässig. Eine weitergehende Kontrolle ist nur beim Verdacht strafbarer Handlungen als gerechtfertigt anzusehen. Abs. 49

Hat der Arbeitgeber zulässiger Weise die Daten seiner Arbeitnehmer überwacht und protokolliert, darf er aus diesen arbeitsrechtliche Konsequenzen ziehen. Je nach Schwere des Pflichtverstoßes seitens des Arbeitnehmers kann der Arbeitgeber nach erfolgloser Abmahnung im Wiederholungsfall eine ordentliche oder sogar eine außerordentliche Kündigung aussprechen. Unter bestimmten Umständen ist eine vorherige Abmahnung sogar entbehrlich. Abs. 50

Um Interessenskonflikte von vorneherein auszuschließen, ist es sinnvoll, die Internetnutzung ausdrücklich zu regeln. Dafür kommt eine individualrechtliche Nutzungsvereinbarung zwischen Arbeitgeber und Arbeitnehmer oder der Abschluss einer Betriebsvereinbarung in Zusammenarbeit mit dem Betriebsrat in Betracht. Abs. 51

Von einer intensiven Überwachung oder einem gänzlichen

Verbot der Privatnutzung durch den Arbeitgeber ist abzuraten. Dies führt zu geringerer Leistungsbereitschaft der Arbeitnehmer. Privates Surfen nutzt dem Arbeitgeber auch, da der Arbeitnehmer den Umgang mit dem Medium übt. Von den Arbeitnehmern wird zunehmend Eigenverantwortung, ergebnisorientiertes Arbeiten und Bereitschaft zur Flexibilität verlangt. Krasser Missbrauch wird nach Ansicht des Bundes deutscher Arbeitgeberverbände auch ohne regelmäßige Kontrolle aufgedeckt, weil ein Arbeitnehmer, der ständig privat im Internet surft zwangsläufig in der Arbeitsleistung nachlasse(35). Und hat er die Zeit dazu, liegt ein Führungsproblem vor. Dann ist es versäumt worden, dem Arbeitnehmer genügend geeignete Aufgaben zu übertragen.

Fußnoten:

(1) www.heise.de/newsticker/data/ad-09.02.03-003/
(2) Vehslage, Thorsten: "Privates Surfen am Arbeitsplatz", in: AnwBl 2001, S.145 (146).
(3) Lindemann/Simon: "Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung", in:BB 2001, S. 1950. (1951); Däubler, Wolfgang: "Internet und Arbeitsrecht", 2. Auflage, 2002, RN 234ff.
(4) Post-Ortmann, Karin: "Der Arbeitgeber als Anbieter von Telekommunikations- und Telediensten", in: RDV 1999, S. 102 (103).
(5) Schaub, Günter: Arbeitsrecht-Handbuch, 10. Auflage, 2002, §55 RN 21.
(6) Vehslage, a.a.O., S.156; www.heise.de/newsticker/data/ad-09.02.03-003/; Schaub, a.a.O. §55 RN 21.
(7) Lindemann/Simon, a.a.O., S. 1951; Post-Ortmann, a.a.O. S. 103
(8) Vehslage, a.a.O., S. 147.
(9) Erfurter Kommentar zum Arbeitsrecht, 2. Auflage, 2001, §28 RN 21.
(10) Vehslage, a.a.O., S.147.
(11) Vehslage, a.a.O., S.147.
(12) Post-Ortmann, a.a.O., S. 104.
(13) Post-Ortmann, a.a.O., S.105; Lindemann/Simon, a.a.O., S. 1951.
(14) Post-Ortmann, a.a.O., S.105.
(15) Müller, Andreas: "Datenschutz beim betrieblichen E-Mailing", in: RDV 1998, S. 205 (208).
(16) Müller, a.a.O.,S. 208.
(17) Post-Ortmann, a.a.O., S. 106.
(18) Vehslage, a.a.O., S. 148.
(19) Schaub, a.a.O., §108 RN 51; Vehslage, a.a.O., S.148.
(20) Raffler/Hellich: "Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-E-Mails zulässig?", in: NZA 1997, S. 862 (863); Däubler, a.a.O., RN 248; Lindemann/Simon, a.a.O., S. 1952.
(21) Post-Ortmann, a.a.O., S. 106.

(22) Lindemann/Simon, a.a.O., S. 1952.
(23) Schaub, a.a.O., §130 RN 9.
(24) BAG, DB 1984, S. 2703.
(25) BAG, NZA 1997, S1281.
(26) BAG, Urteil v. 4.6.1997, Az: 2 AZR 526/96; Schaub, a.a.O., § 61 RN 52.
(27) ArbG Wesel, Urteil v. 21.3.2001, Az: 5 Ca 4021/00 = JurPC Web-Dok. 214/2001.
(28) BVerfG, NZA 1998, S. 470.
(29) Vehslage, a.a.aO.; S.149.
(30) ArbG Frankfurt, Urteil v. 2.1.2002, Az: 2 Ca 5340/01 = JurPC Web-Dok. 117/2003.
(31) ArbG Düsseldorf, Urteil v. 1.8.2001, Az: 4 Ca 3437/01 = JurPC Web-Dok. 100/2002.
(32) ArbG Hannover, Urteil v. 1.12.2000, 1 Ca 504/00 = JurPC Web-Dok. 162/2002.
(33) Däubler, a.a.O., RN 271; Balke/Müller: "Arbeitsrechtliche Aspekte beim betrieblichen Einsatz von E-Mails", in: DB 1997, S.326 (330).
(34) ArbG Frankfurt, Urteil v. 2.1.2002, Az: 2 Ca 5340/01 = JurPC Web-Dok. 117/2003.
(35) www.heise.de/newsticker/data/cp-26.08.00-000/.

Hinweise des
Landesbeauftragten für den Datenschutz Baden-Württemberg
zu

Internet und Datenschutz

Stand: 1. März 2006

Inhaltsverzeichnis

1. Was ist das Internet?

2. Datenschutzrisiken

- 2.1 Sicherheitsmängel der Internet-Übertragungsstandards
- 2.2 Aus dem Internet stammende Schadensprogramme
- 2.3 Hohe Zahl potentieller Angreifer
- 2.4 Große Angriffsfläche
- 2.5 Abhören von Informationen
- 2.6 Gefahr der Bildung von Persönlichkeitsprofilen
- 2.7 Risiken spezieller Internet-Dienste

3. Was ist zu tun?

4. Schutz eigener Computer vor Angriffen aus dem Internet

- 4.1 Schutz vor Angriffen auf ein eigenes Computernetzwerk
  - 4.1.1 Nicht allein auf statische Paketfilterung vertrauen
  - 4.1.2 Application Gateways einsetzen
  - 4.1.3 Mehrfachauslegung von Filtern
  - 4.1.4 "Datenschleichwege" versperren
  - 4.1.5 Administration sicherheitsrelevanter Komponenten
  - 4.1.6 Schutz vor Schadensprogrammen
- 4.2 Schutz einzelner PC, die über einen unmittelbaren Internet-Zugang verfügen
  - 4.2.1 Anschluss eines nicht vernetzten PC (Stand-alone-PC) an das Internet
  - 4.2.2 Anschluss von PC, die außer mit dem Internet auch mit einem internen Netz verbunden sein können
- 4.3 Computerviren - ein hartnäckiges Problem

4.4 Höhere Sicherheit vor Viren und anderen Schadensprogrammen

5. Was ist bei der Nutzung der Internet-Dienste zu beachten?

5.1 Vorsicht beim Download

5.2 Übertragung schutzbedürftiger Daten

5.3 Hinweise rund um das Web

5.3.1 Cookies
5.3.2 Cache-Speicherung
5.3.3 History-Liste/Liste zuletzt aufgerufener Web-Seiten

5.4 Passwort für Internet-Zugang und für Web-Services nicht auf dem PC speichern

6. Hinweise für Stellen, die eigene Informationsangebote im Internet bereitstellen

6.1 Anordnung der Server

6.2 Gestaltung der Web-Angebote/Privacy-Policy

6.3 Elektronische Dienstleistungen für den Bürger

6.4 Sicherheitsinteressen der Internet-Nutzer beachten

6.5 Datenschutzgerechte Protokollierung der Abrufe

7. Weitere Informationen zum Themenbereich Internet, e-Government und Datenschutz

---

1. Was ist das Internet?

Das Internet ist ein weltweites Computernetz, das nicht nur von Unternehmen, Forschungseinrichtungen und Behörden, sondern auch von vielen Millionen Privatpersonen genutzt wird, um Informationen auszutauschen, abzurufen oder der Öffentlichkeit zum Abruf anzubieten. Die Internet-Teilnehmer können dazu unterschiedlichste Kommunikationsdienste nutzen. Gebräuchlich sind insbesondere:

- World Wide Web (WWW)
  Dieser Dienst ermöglicht es, Texte, Bilder und Videoanimationen in ansprechender Form im Internet zum Abruf bereitzustellen. Jede WWW-Seite kann Verweise (sog. Links) auf andere WWW-Seiten enthalten, die mitunter auf ganz anderen Computern gespeichert sind. Der Nutzer kann einen solchen Link mit der Maus anklicken und so von einer Seite zu einer anderen und von einem Computer zu einem anderen gelangen. Zum Teil sind mit einzelnen WWW-Seiten auch ausführbare Programme (sog. aktive Inhalte) verbunden, die gleichzeitig mit dem Seiteninhalt auf den PC des Nutzers geladen und automatisch gestartet werden.

- Elektronische Post (E-Mail)
  Diese ermöglicht den Versand von Texten, Tabellen, Programmen oder sonstigen Dokumenten an andere Internet-Nutzer.
- Dateiübertragung (Filetransfer)
  Damit lassen sich Dateien zwischen Computern austauschen. Ein Internet-Teilnehmer kann damit zum Abruf bereitgestellte Dateien von einem entfernten Computer auf seinen eigenen kopieren oder selbst Dateien zum Abruf bereitstellen.
- Terminaldienst (Telnet)
  Mit Hilfe des Terminaldienstes kann man sich an einem räumlich entfernten Computer anmelden und, soweit es die Benutzerberechtigungen zulassen, die auf diesem Computer zur Verfügung stehenden Dialogverfahren nutzen.
- News-Foren/Usenet-News
  Dieser Dienst stellt mit seinen zahlreichen themenbezogenen Rubriken, den sog. Foren, ein elektronisches "Schwarzes Brett" dar. In der Regel kann hierbei jeder Teilnehmer alle Beiträge lesen, die in den einzelnen Foren stehen und sich mit eigenen Beiträgen, etwa Fragen oder Kommentaren zu früheren Mitteilungen, an der weiteren Diskussion beteiligen. Diese Beiträge sind ihrerseits wieder für alle Internet-Teilnehmer les- und auswertbar.
- Dateifreigabe-Dienst (NetBIOS über TCP/IP)
  Dieser Dienst macht es möglich, Teilnehmern im lokalen Netz, aber auch im Internet, Zugriff auf Dateien zu gewähren, die auf einem lokalen Computer gespeichert sind. Umgekehrt kann man mit diesem Dienst auch auf freigegebene Dateien zugreifen, die auf am Internet angeschlossenen Computern gespeichert sind. Viele der im Internet realisierten Tauschbörsen nutzen beispielsweise diesen oder vergleichbare Dienste.
- Internet-Telefonie (Voice over IP, VoIP)
  Leistungsfähige Übertragungswege vorausgesetzt, kann man über Internet einen Sprachtelefondienst realisieren.
- Internet Relay Chat
  In sog. "Chat-Rooms" können Internet-Nutzer, die gleichzeitig im Internet aktiv sind, schriftlich in Echtzeit miteinander kommunizieren.
- Messaging Dienste
  Diese Dienste ermöglichen es einem Internet-Nutzer, zu erkennen, ob ausgewählte andere Internet-Nutzer (z. B. private Bekannte oder dienstliche Ansprechpartner) zur gleichen Zeit mit dem Internet verbunden sind. Diese können dann untereinander schriftliche Nachrichten austauschen.

2. Datenschutzrisiken

Wer das Internet nutzt, sollte sich darüber im Klaren sein, dass dies mit verschiedenen Datenschutzrisiken einhergeht:

2.1 Sicherheitsmängel der Internet-Übertragungsstandards

Bei der Festlegung der im Internet zu verwendenden Übertragungsstandards spielten Sicherheitsaspekte bislang nur eine untergeordnete Rolle. Unter dem Oberbegriff IP Security Protocol (IPSEC) wurden zwar mittlerweile auch Übertragungsstandards erarbeitet, die eine vertrauliche und unverfälschte Kommunikation unterstützen sollen, aber gegenwärtig

dominieren noch die traditionellen Übertragungsstandards, die ohne ergänzende Sicherheitsmaßnahmen keinen verlässlichen Schutz vor Angriffen bieten können. Beispielhaft seien hier folgende grundlegende Sicherheitsdefizite genannt:

- Kein Schutz vor Verfälschung der IP-Adressen
  Jeder an das Internet angeschlossene Computer hat eine weltweit eindeutige Adresse, die sog. IP-Adresse. Verschickt nun ein Rechner ein Datenpaket, so wird seine IP-Adresse dort automatisch als Absenderangabe eingetragen. Wer es aber darauf anlegt, kann diese Absenderangabe fälschen. Da in manchen Fällen allein anhand der Absenderadresse entschieden wird, ob jemand die von einem Computer angebotenen Kommunikationsdienste nutzen darf oder nicht, kann die Adressverfälschung dazu führen, dass der Absender auf dem Zielrechner unter Umständen auch Daten lesen, verändern oder auf seinen Computer herunterladen kann, obwohl ihm dies bei unverfälschter Absenderangabe technisch verwehrt wäre.
- Konzeptionelle Mängel beim Austausch von Routing-Informationen
  Die als Netzknoten verwendeten Router informieren sich teilweise gegenseitig über neu am Internet angeschlossene Computer oder Netzwerke. Wenn ein Router auf diese Weise Informationen darüber erhält, auf welchem Weg er künftig die an einen Computer adressierten Datenpakete weiterleiten soll, so übernimmt er diese Informationen, ohne zu prüfen, ob der Absender dieser Informationen vertrauenswürdig ist. Damit besteht die Gefahr, dass jemand durch Verbreiten falscher Routing-Informationen Daten, die eigentlich für einen anderen Empfänger bestimmt waren, an seinen eigenen Computer umleitet.
- Konzeptionelle Mängel des Domain Name Services (DNS)
  Dieser Dienst ordnet die numerischen IP-Adressen den häufig zur Bezeichnung von Computern benutzten Namen, z. B. "www.datenschutz.de", zu und umgekehrt. Da sich, wenn man eine solche DNS-Anfrage stellt, nicht sicherstellen lässt, dass der DNS-Server, der die Antwort gibt, vertrauenswürdig ist, lässt sich nicht ausschließen, dass die Antwort auf die eigene Anfrage von einem Server stammt, auf dem bestimmten Computernamen absichtlich falsche IP-Adressen zugeordnet werden. Zudem bieten DNS-Server den Domain-Inhabern oft die Möglichkeit, die dort registrierten Daten online zu ändern. In der Vergangenheit gab es zum Teil gravierende Lücken bei der Prüfung der Zugriffsberechtigung mit der Folge, dass die DNS-Einträge hätten verfälscht werden können. In letzter Konsequenz bedeutet dies, dass Aufrufe bestimmter Internet-Adressen nicht zum rechtmäßigen Anbieter, sondern gezielt auf einen anderen Web-Server umgelenkt werden könnten.

2.2 Aus dem Internet stammende Schadensprogramme

Bei der Nutzung einer Reihe von Diensten wie z. B. E-Mail, World Wide Web oder FTP besteht das Risiko, dass Computerviren, sog. Trojanische Pferde oder sonstige Schadensprogramme auf den eigenen Computer gelangen, deren Ausführung Daten von eigenen Computer unbemerkt an Empfänger im Internet sendet (sog. Spyware), die Hintertüren öffnen können, durch die Angreifer aus dem Internet Zugang zum eigenen Computer erlangen (Trojanische Pferde) oder die unerwünschte Veränderungen an gespeicherten Daten und Programmen bis hin zur Löschung ganzer Datenbestände hervorrufen können (sog. Malware). Ein Schadensprogramm kann aber mitunter auch bestimmte Daten der lokalen Festplatte auslesen und ohne Wissen des Computer-Nutzers über

Internet an einen bestimmten Empfänger senden. Solche Schadensprogramme können auf folgende Weise auf einen Computer gelangen:

- Sorgloser Umgang mit empfangenen E-Mails
  Programme, die zur Textverarbeitung, Tabellenkalkulation und für andere Aufgaben eingesetzt werden, bieten vielfach die Möglichkeit, bestimmte regelmäßig wiederkehrende Arbeitsabläufe mit Hilfe eines Makro-Programms zu automatisieren. Ein solches Makro-Programm kann nicht nur nützliche, sondern auch unerwünschte Funktionen oder gar ein Virus enthalten. Problematisch ist dabei, dass jemand, der eine solche Datei erhält, nicht unmittelbar erkennen kann, ob sie ein Makro-Programm enthält oder nicht. Öffnet man die Datei, um sie zu lesen, so kann dies bereits der Auslöser zum Start des Schadensprogramms sein.
- Anklicken von WWW-Seiten, die mit aktiven Inhalten verbunden sind
  Beim Aufruf einer WWW-Seite kann eine aktive Komponente, d. h. ein ausführbares Programm, etwa in Form eines JavaScript-Programms oder eines ActiveX-Controls aus dem Internet auf den eigenen Computer geladen und dort ohne weiteres Zutun des Nutzers gestartet werden. Sofern die dafür vorgesehenen Sicherheitsmechanismen nicht korrekt funktionieren, können auch Java-Applets Schadenswirkungen entfalten. Diese Applets können, wie die ActiveX-Controls, ebenfalls im Rahmen der WWW-Nutzung auf den lokalen Arbeitsplatzcomputer des Internet-Nutzers gelangen.
- Download eines Programms
  Schadensprogramme können übertragen werden, wenn ein Internet-Nutzer ein Programm per Filetransfer aus dem Internet auf seinen Computer herunterlädt, installiert und anschließend startet. Es kann sein, dass es als nützliches Hilfsmittel angepriesen wird, es kann aber neben oder anstelle der gewünschten eine unerwünschte, möglicherweise schadensstiftende Funktion haben (Trojanisches Pferd).

2.3 Hohe Zahl potentieller Angreifer

Angesichts der sehr großen Zahl von Internet-Teilnehmern muss auch von einer hohen Zahl potentieller Angreifer ausgegangen werden. Diese können Sicherheitslücken gängiger Betriebssysteme, Browser oder sonstiger Programme ausnutzen und mit Hilfe ihres Computers im Internet systematisch nach anderen Computern suchen, die die entsprechende Sicherheitslücke aufweisen. Das kann mitunter dazu führen, dass die Angreifer unbefugt auf personenbezogene Daten zugreifen.

2.4 Große Angriffsfläche

Die Größe des Netzes bringt nicht nur eine hohe Zahl von potentiellen Angreifern mit sich, sondern bietet diesen zudem schon rein quantitativ wesentlich mehr Angriffspunkte als ein kleines Netz. Wird eine Sicherheitslücke des Internets oder der Systemsoftware von gängigen, am Internet angeschlossenen Computern bekannt, ist sofort eine Vielzahl von Computern bedroht.

2.5 Abhören von Informationen

Da sämtliche Daten im Internet - ohne Einsatz entsprechender Zusatzprodukte - unverschlüsselt übertragen werden, besteht die Gefahr, dass sie unterwegs von Personen gelesen, gespeichert und genutzt werden, für die sie nicht bestimmt sind. Gefährdet sind nicht nur die jeweils übertragenen Inhaltsdaten, z. B. der Inhalt elektronischer Postsendungen, sondern auch Benutzerkennungen und Passwörter, die von manchen Diensten, wie z. B. Telnet oder FTP, im Klartext übertragen werden. Unberechtigte Zugriffe auf übertragene Daten können dabei - technisch gesehen - sowohl an Übertragungswegen (z. B. Kabeln oder Richtfunkstrecken) als auch an den Netzknoten ansetzen und entweder von deren Betreibern oder von Dritten, z. B. Hackern, durchgeführt werden, denen es gelingt, die Sicherheitsmaßnahmen der Betreiber zu überwinden. Diese Situation ist im Internet besonders problematisch, da der Absender in der Regel nicht weiß, auf welchem Weg die Daten zum Empfänger fließen. Mitunter kann es nämlich vorkommen, dass Absender und Empfänger zwar in der gleichen Stadt wohnen, die Daten aber gleichwohl beispielsweise über Netzknoten in den USA übertragen werden. Unbekannt bleibt außerdem in der Regel, wer die Netzknoten betreibt, über die die Daten fließen, welche Datenschutzvorschriften für diese Betreiber gelten und wie vertrauenswürdig die Betreiber sind.

2.6 Gefahr der Bildung von Persönlichkeitsprofilen

Sowohl die im Internet veröffentlichten Inhaltsdaten (z. B. Inhalt von Web-Seiten) als auch die zur technischen Übermittlung der Inhaltsdaten verwendeten Verbindungsdaten (diese lassen erkennen, welcher Computer über welchen Internet-Dienst Verbindung mit welchem anderen Computer aufnimmt) ermöglichen die Erstellung von Persönlichkeitsprofilen.

- Für die Erstellung von Persönlichkeitsprofilen auf der Grundlage von Inhaltsdaten sind vor allem die im Internet verfügbaren Suchmaschinen von Bedeutung. Diese sind in der Lage, unterschiedlichste WWW-Seiten sowie Beiträge in News-Gruppen zu ermitteln, in denen ein bestimmter Name oder eine E-Mail-Adresse vorkommt. Einzelne Suchmaschinen verfügen zugleich über ein Archiv, in dem WWW-Seiten oder Beiträge aus News-Foren monate- oder jahrelang gespeichert werden. Wer einmal eine Nachricht an eine News-Gruppe gesandt hat oder über wen personenbezogene Daten im World Wide Web veröffentlicht sind, der muss daher damit rechnen, dass alle diese Informationen auch lange nach der Veröffentlichung noch mit Hilfe der Suchmaschinen und Archive zusammengeführt werden können.
- Nutzt ein Teilnehmer einen Internet-Dienst, fallen beispielsweise in den Netzknoten Verbindungsdaten an, ohne dass er dies bemerkt. Die Verbindungsdaten sind für die Dauer der jeweiligen Verbindung erforderlich, um die Daten im Netz übertragen und den richtigen Endgeräten zuordnen zu können. Nach dem Ende der Verbindung werden sie allenfalls noch für Abrechnungszwecke benötigt. Werden die Verbindungsdaten nach dem Ende der jeweiligen Verbindung dauerhaft gespeichert, lässt sich aus ihnen in vielen Fällen entnehmen, wer wann wo auf welche Angebote im Internet zugegriffen oder wer mit wem kommuniziert hat. Technisch machbar wäre, all diese einzelnen Datenspuren zu umfassenden Persönlichkeitsprofilen zusammenzuführen. Zwar fordern das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag von deutschen Diensteanbietern, dass diese die Verbindungsdaten unmittelbar nach Beendigung der jeweiligen Dienstenutzung

löschen müssen, sofern die Daten nicht noch für Abrechnungszwecke benötigt werden. Für ausländische Diensteanbieter gelten diese Regelungen jedoch nicht.

2.7 Risiken spezieller Internet-Dienste

Neben den bislang genannten allgemeinen, mit der Internet-Nutzung verbundenen Risiken, bergen fast alle gebräuchlichen Dienste spezifische Risiken. Dazu nur einige Beispiele:

- FTP:
  Bei schlecht konfigurierten Servern besteht das Risiko, dass Internet-Teilnehmer Daten von dem jeweiligen Server abrufen können, die gar nicht zum Abruf bestimmt sind.
- NetBIOS über TCP/IP:
  Hierbei besteht das Risiko, dass Benutzer Dateien nur im lokalen Netz freigeben wollen, die hierzu vorgenommenen Einstellungen jedoch unter Umständen auch einen Zugriff über das Internet ermöglichen.
- Finger:
  Dieser Dienst ermöglicht es, Benutzerkennungen und andere Informationen über die an einem Computer angemeldeten Benutzer zu erfahren. Ist dieser Dienst unbeschränkt nutzbar, so können Angreifer auf diesem Weg gültige Benutzerkennungen erfahren.

Eine umfassende Übersicht über Sicherheitsrisiken der meisten der unter Nr. 1 erwähnten sowie einer Reihe weiterer Internet-Dienste findet sich in der im Auftrag des BSI erstellten Studie "Gesicherte Verbindungen von Computernetzen mit Hilfe einer Firewall", abrufbar unter

www.bsi.bund.de/literat/studien/firewall/fwstud.htm

3. Was ist zu tun?

Auf Grund der beschriebenen Risiken ist beim Umgang mit dem Internet stets besondere Sorgfalt geboten:

- Wer einen eigenen Computer oder ein eigenes Netzwerk mit dem Internet koppelt, muss ausreichende Sicherheitsmaßnahmen ergreifen, um unberechtigte Zugriffe von Internet-Teilnehmern auf interne Daten zu verhindern.
- Wer personenbezogene oder andere schutzbedürftige Daten über das Internet überträgt, muss Schutzmaßnahmen gegen deren unberechtigte Kenntnisnahme und Manipulation ergreifen.
- Wer im World Wide Web surft, sollte wissen, was er tun kann, um unerwünschte Datenspuren zu vermeiden.
- Wer Informationsdienste im Internet anbietet, muss sowohl bei der Auswahl der veröffentlichten Inhalte als auch beim Umgang mit den bei der Nutzung anfallenden Verbindungsdaten auf die einschlägigen Datenschutzvorschriften achten.

4. Schutz eigener Computer vor Angriffen aus dem Internet

In dieser Frage ist zu unterscheiden, ob man ein Netzwerk an das Internet anschließen will oder nur einzelne PC.

4.1 Schutz vor Angriffen auf ein eigenes Computernetzwerk

Angesichts der zahlreichen Risiken, die der Anschluss eines Computernetzwerks an das Internet mit sich bringt, ist es unverzichtbar, vor der Realisierung eines solchen Anschlusses ein Sicherheitskonzept mit folgenden Bestandteilen zu erarbeiten:

- Es gibt an, welche Mitarbeiter und welche Organisationseinheiten welche Internet-Dienste benötigen (Kommunikationsbedarf).
- Es stellt dar, wie das an das Internet anzuschließende interne Netz strukturiert ist.
- Es dokumentiert und bewertet die mit der Nutzung der erforderlichen Internet-Dienste einhergehenden Risiken und die drohenden Schäden.
- Es legt dar, welche technischen und organisatorischen Maßnahmen erforderlich sind, um den Risiken entgegenzuwirken.

Nach Inbetriebnahme des gesicherten Internet-Anschlusses ist darauf zu achten, dass das Konzept regelmäßig überprüft und bei Bedarf den veränderten Nutzungsanforderungen sowie neu aufgetretenen Sicherheitslücken angepasst wird.

Der Konzeption der Sicherheitsmaßnahmen sind folgende Ziele zugrunde zu legen:

a) Filterung
Die technischen Kommunikationsmöglichkeiten der einzelnen Nutzer sind auf den ermittelten, notwendigen Kommunikationsbedarf zu beschränken.

b) Verbergen der internen Netzstruktur
Informationen über die Struktur des internen Netzes, z. B. Namen interner Computer, Informationen über registrierte Software, freigegebene Festplatten-Verzeichnisse, müssen gegenüber dem Internet verborgen werden.

c) Protokollierung
Sicherheitsrelevante Ereignisse sind zu protokollieren. Wichtig ist daneben, dass Systemverwalter, etwa durch Alarmmeldungen, umgehend über sicherheitsrelevante Ereignisse informiert werden.

Hard- und Softwarekomponenten, die an einer zentralen Übergangsstelle zwischen zwei Netzen, für die unterschiedliche Sicherheitsanforderungen gelten (z. B. zwischen internem Netz und dem Internet), angesiedelt sind und die Schutzfunktionen für mindestens eines der Netze bieten, werden als Firewall bezeichnet.

Zur technischen Umsetzung der genannten Firewall-Grundfunktionen ist noch Folgendes zu sagen:

zu a) Filterung

Um den Datenaustausch mit dem Internet auf das zulässige Maß beschränken zu können, muss die Firewall eine Filterfunktion bieten:
Anhand hinterlegter Regeln entscheidet sie, welche Datenpakete sie durchlässt und welche sie abweist. Die Filterung sollte dabei in jedem Fall nach dem Prinzip organisiert sein, dass alles verboten ist, was nicht ausdrücklich erlaubt wurde. Die Filterung kann auf drei Ebenen erfolgen:

- Statische Paketfilterung:
  Die Filterung erfolgt auf den Schichten 3 und 4 des OSI-Modells für offene Kommunikation. Für die Filterung stehen die Adressen der an der Kommunikation beteiligten Computer, die Port-Nummern sowie die Information über das verwendete Übertragungsprotokoll zur Verfügung.
- Dynamische Paketfilterung:
  Abhängig vom Kommunikationsverlauf kann bei der dynamischen Filterung eine Situations- bzw. kontextbasierte Filterung erfolgen. Damit lässt sich beispielsweise festlegen, dass nur dann ein Datenpaket eines externen Computers ins interne Netz durchgelassen wird, wenn genau dieser externe Computer zuvor mit einem Datenpaket spezieller Art von einem internen Computer angesprochen wurde.
- Anwendungsfilterung:
  Gegenüber einem Paketfilter kann ein Anwendungsfilter (Application Gateway) alle Informationen heranziehen, die auf der Anwendungsebene (OSI-Schicht 7) vorhanden sind, insbesondere Benutzerkennungen.

Damit lassen sich unterschiedliche Firewall-Architekturen realisieren:

- Ausschließlicher Einsatz eines Paketfilters:

  Statische Paketfilter dieser Art werden häufig durch Router realisiert.

- Screened Subnet:
  Hierbei handelt es sich um eine Kombination aus einem Application Gateway und einem oder zwei Paketfiltern, die ein separates Teilnetz bilden.

  Die Filterregeln der Paketfilter müssen dabei so gewählt werden, dass die zwischen LAN und Internet ausgetauschten Datenpakete stets über den Gateway-Rechner geleitet werden.

- Dual Homed Gateway:

Ein Dual Homed Gateway besteht aus dem Application Gateway, das auf einem mit zwei Netzwerkanschlüssen ausgestatteten Computer installiert ist und das durch einen oder, wie in der Abbildung dargestellt, durch zwei Paketfilter flankiert wird. Der Gateway-Computer muss dabei so konfiguriert sein, dass kein Datenpaket unverändert in das interne Netz gelangen kann. Dies lässt sich durch Abschalten des IP-Forwardings realisieren.

zu b) Verbergen der internen Netzstruktur

Um die intern verwendeten IP-Adressen nach außen hin verbergen zu können, ist es erforderlich, in der Firewall eine Adressumsetzung (Network Adress Translation NAT) vorzunehmen. Die Adressen interner Rechner werden dabei durch die Adresse der Firewall ersetzt. Darüber hinaus kann es je nach Architektur der Firewall notwendig sein, auch die Adressen externer Server etwa für E-Mail oder World Wide Web bekannt zu machen.

zu c) Protokollierung

Neben der Ausgabe von Warnmeldungen bei Ereignissen von besonderer sicherheitsrelevanter Bedeutung ist eine aussagekräftige Protokollierung ein ganz wesentliches Element einer Firewall. Die Protokollierung kann einen Beitrag dazu leisten, Angriffe wenigstens im Nachhinein noch feststellen und darauf reagieren zu können. Insbesondere sollten folgende sicherheitsrelevante Ereignisse von der Firewall protokolliert werden:

- abgewiesene Verbindungsversuche (z. B. Versuche, auf nicht freigegebene IP-Adressen oder Port-Nummern zuzugreifen);
- Hinweise auf systematische Eindringversuche (z. B. Nachweis des Einsatzes von Port-Scannern);
- Versuche, vom Internet aus Datenpakete durch die Firewall zu schleusen, die als Absenderangabe die Internet-Adresse eines internen Computers tragen (sog. IP-Spoofing-Attacken);
- erfolgreiche und abgewiesene Versuche des Systemverwalterzugriffs auf Firewall-Komponenten.

Bei der Planung einer Firewall sollte auf folgende weitere Punkte besonderes Augenmerk gerichtet werden:

4.1.1 Nicht allein auf statische Paketfilterung vertrauen

Statische Paketfilterung kann die Dienstenutzung zwar beschränken und die Verbreitung von Informationen über das interne Netz eindämmen. Gleichwohl weisen Paketfilter systembedingte Schwächen auf, die sich nicht ausräumen lassen:

- Eine benutzerbezogene Filterung ist nicht möglich.
- Die Abschottung des internen Netzes gelingt nicht vollständig, denn alle Datenpakete, die ein Paketfilter von innen nach außen passieren lässt, tragen nach wie vor interne Adressen als Absenderadressen. Auf diese Weise werden die Adressen interner Computer im Internet bekannt.
- Die von Paketfiltern erstellten Protokolldaten lassen sich oft nur mit Mühe nachvollziehen.

4.1.2 Application Gateways einsetzen

Die genannten Schwächen der Paketfilter lassen sich durch den Einsatz eines Application Gateways ausräumen, denn:

- Berechtigungen zur Nutzung einzelner Dienste lassen sich für jeden Benutzer individuell festlegen.
- Zum Internet hin müssen nur der Gateway-Rechner sowie etwaige für die Nutzung aus dem Internet bestimmte Server bekannt gemacht werden. Informationen über die übrige interne Netzstruktur lassen sich auf diesem Weg vollständig verbergen.
- Eine aussagekräftige Protokollierung ist möglich.

Um diese Vorteile in der Praxis voll ausschöpfen zu können, ist es wichtig, die Möglichkeiten zur Vergabe differenzierter Zugriffsberechtigungen restriktiv zu verwenden und Protokolldateien regelmäßig auszuwerten.

4.1.3 Mehrfachauslegung von Filtern

Sowohl bei der eingesetzten Hard- und Software als auch bei der Implementierung der Filterregeln können Fehler auftreten. Daher empfiehlt es sich, sicherheitsrelevante Funktionen einer Firewall nicht bloß einfach, sondern mehrfach, und zwar auf technisch unterschiedliche Art und Weise, zu realisieren. Bei dieser Vorgehensweise wird ein Angreifer aus dem Internet, der einen Fehler einer Firewall-Komponente ausnutzen kann, noch durch eine zweite Barriere davon abgehalten, ins interne Netz einzudringen.

4.1.4 "Datenschleichwege" versperren

Der mit der Einrichtung einer Firewall angestrebte Schutz stellt sich nur dann ein, wenn tatsächlich alle Verbindungen zwischen internen und externen Computern über die Firewall laufen. Das bedeutet, dass beispielsweise auch Modem- oder ISDN-Verbindungen nicht an der Firewall vorbei geführt werden dürfen. Um dem Risiko der Einrichtung und Nutzung derartiger "Datenschleichwege" zu begegnen, muss jede Stelle, die eine Firewall betreibt, ihre Mitarbeiterinnen und Mitarbeiter klipp und klar darauf hinweisen, dass es unzulässig ist, solche Verbindungen an der Firewall vorbei herzustellen. Einen gewissen Schutz vor unerlaubten Kommunikationsverbindungen zwischen dem internen Netz und dem Internet bietet in diesem Zusammenhang die Verwendung sog. nicht-offizieller IP-Adressen für Rechner des internen Netzes. Hierbei handelt es sich um Adressen, die ausdrücklich für die Verwendung in nicht allgemein zugänglichen Netzen vorgesehen sind und die in der Regel im Internet nicht weitergeleitet (geroutet) werden.

4.1.5 Administration sicherheitsrelevanter Komponenten

Zu einem datenschutzgerechten Firewall-Betrieb gehört, dass sich Unberechtigte keine Informationen über deren Administration verschaffen können und auch keine Möglichkeit einer missbräuchlichen Nutzung von Administrationsfunktionen besteht. Dies erfordert unter anderem,

- dass auch für den Administrationszugang eine strenge Zugriffskontrolle realisiert wird, die den üblichen Anforderungen an Passwörter gerecht wird. Näheres zur Gestaltung eines datenschutzgerechten Passwortschutzes ist unserem Merkblatt zum Umgang mit Passwörtern zu entnehmen
- dass ferner eine Terminalbeschränkung für die Administration existiert, die sicherstellt, dass eine Anmeldung als Firewall-Administrator nur von wenigen ausgewählten Arbeitsplätzen aus möglich ist und
- dass ein Abhören der zur Administration benutzten Daten verhindert wird. Dies lässt sich beispielsweise durch Verschlüsselung erreichen oder dadurch, dass durch Segmentierung des internen Netzes sichergestellt wird, dass am Teilnetz, durch das die Administrationsdaten fließen, nur Administrations-Arbeitsplätze angeschlossen sind.

4.1.6 Schutz vor Schadensprogrammen

Beim Download von Programmen oder beim Bearbeiten elektronischer Post-Sendungen, die aus dem Internet stammen, besteht das Risiko, dass diese Schadensfunktionen enthalten. Zur Verringerung dieser Gefahr ist der Einsatz von Virenschutzprogrammen erforderlich, die möglichst in die Firewall integriert werden sollten. Zum Schutz vor schadensstiftenden Funktionen in Java-Applets, JavaScript-Programmen oder ActiveX-Controls ist Folgendes zu beachten:

Zur Vermeidung unberechtigter Zugriffe auf lokal gespeicherte Daten verfügt Java über Sicherheitsmechanismen nach dem sog. Sandbox-Modell, die beispielsweise dafür sorgen, dass Schreib- und Lesevorgänge von aus dem Internet erhaltenen Applets auf bestimmte Verzeichnisse der lokalen Festplatte beschränkt bleiben. In der Vergangenheit konnte dieses Sicherheitskonzept allerdings zeitweise aufgrund fehlerhafter Programmierung unterlaufen werden. Bei der Ausführung von JavaScript-Programmen oder ActiveX-Controls gibt es im Gegensatz dazu keine Möglichkeit, deren Zugriffsmöglichkeiten zu begrenzen. Ein Benutzer kann zwar dafür sorgen, dass nur solche ActiveX-Controls zur Ausführung kommen können, die eine Zertifizierungsstelle digital signiert hat. Die Sicherheitsprobleme löst dies jedoch nicht: Eine digitale Signatur bescheinigt lediglich, dass der Hersteller des Controls bekannt ist und es beim Empfänger unverfälscht zur Ausführung kommt; sie sagt jedoch nichts über Inhalt und Funktionsweise des Programms aus. Wie ein Beispiel aus der Praxis belegt, können selbst signierte ActiveX-Controls eine unerwünschte Funktion enthalten. Vor diesem Hintergrund ist es geboten, auf die ActiveX-Funktionalität zu verzichten. Empfehlenswert ist daher, ein zentrales Filterprogramm einzusetzen, das ActiveX-Controls aus dem Datenstrom herausfiltert oder nur mit Browsern zu arbeiten, die die ActiveX-Technologie nicht unterstützen oder in denen diese Unterstützung abgeschaltet wurde. Entsprechend sollte auch verhindert werden, dass JavaScript-Programme ausgeführt werden. Da sich auch beim Umgang mit Java-Applets Risiken nicht restlos vermeiden lassen, empfiehlt sich auch hier ein restriktiver Umgang.

Abschließend ist darauf hinzuweisen, dass die Anbindung eines internen Netzes an das Internet in jedem Fall die Datenschutzrisiken für die im internen Netz gespeicherten Daten

erhöht. Selbst wenn man eine nach allen Regeln der Kunst gestaltete Firewall einsetzt, lässt sich damit also lediglich die Zunahme der Risiken begrenzen.

4.2 Schutz einzelner PC, die über einen unmittelbaren Internet-Zugang verfügen

Nicht immer ist es notwendig, den Internet-Zugang für ein Netzwerk einzurichten, sondern es genügt, dies für einzelne PC zu tun. Der Internet-Anschluss wird in diesen Fällen in der Regel via Modem- oder ISDN-Verbindung direkt, d. h. ohne eine Firewall realisiert, die den in Nr. 4.1 genannten Anforderungen gerecht wird. Auch und besonders in diesen Fällen ist vor der Realisierung des Anschlusses zu prüfen, welche Risiken mit dem geplanten Anschluss einhergehen und wie sie minimiert werden können. In der Praxis sind zwei Arten des direkten Internet-Anschlusses anzutreffen: Zum einen gibt es die Fälle, in denen Stand-alone-PC ans Internet angeschlossen werden. Zum anderen gibt es PC, die zwar direkt mit dem Internet gekoppelt sind oder gekoppelt werden können, aber gleichzeitig oder wahlweise auch eine Verbindung zum internen Netz haben können.

4.2.1 Anschluss eines nicht vernetzten PC (Stand-alone-PC) an das Internet

Schließt man einen unvernetzten PC via Modem- oder ISDN-Verbindung an das Internet an, so besteht hierbei das Risiko, dass Internet-Teilnehmer auf schutzbedürftige Daten zugreifen können, die lokal auf dem PC gespeichert sind. Deshalb sollten auf einem derartigen PC möglichst keine personenbezogenen oder anderen schutzbedürftigen Daten gespeichert und verarbeitet werden. Um unberechtigten Zugriffen von Seiten des Internets technisch entgegenzuwirken, sollte darauf geachtet werden, dass keine Datei-Verzeichnisse oder gar der Inhalt ganzer Laufwerke für einen Zugriff über Netz freigegeben sind. Daten, die nicht für die Allgemeinheit bestimmt sind, können durch verschlüsselte Speicherung vor unberechtigter Kenntnisnahme geschützt werden. Im Übrigen sind auch bei einem mit dem Internet verbundenen Stand-alone-PC Maßnahmen zum Schutz vor Schadensprogrammen zu ergreifen. Hierzu ist ein Virenschutzprogramm einzusetzen und die Möglichkeit zur Ausführung von aktiven Inhalten zu unterbinden.

Sollen auf dem PC auch schutzbedürftige Daten gespeichert werden, so ist zusätzlich der Einsatz eines darauf abgestimmten Firewallsystems (sog. Personal Firewall) erforderlich.

4.2.2 Anschluss von PC, die außer mit dem Internet auch mit einem internen Netz verbunden sein können

Der Anschluss von PC, die via Modem- oder ISDN-Verbindung direkt mit dem Internet und außerdem mit einem internen Netz verbunden sein können, ist mit besonderen Datenschutzrisiken verbunden:

- Bei dieser Anschlussart ist nicht nur der PC gefährdet, der über den Internet-Anschluss verfügt, sondern auch die übrigen, am lokalen Netz angeschlossenen Computer. Falls der PC gleichzeitig mit dem Internet und dem internen Netz verbunden sein kann, ist dieses Risiko größer als in dem Fall, in dem der PC entweder mit dem Internet oder dem internen Netz verknüpft ist. Aber auch dann ist nicht ausgeschlossen, dass beispielsweise ein Computervirus auf dem am Internet angeschlossenen PC gespeichert wird, und sich dieser im lokalen Netz ausbreitet, sobald der PC wieder daran angeschlossen wird.

- Ferner besteht bei dieser Anschlussart auch ein erhöhtes Risiko, dass Internet-Teilnehmer auf schutzbedürftige Daten zugreifen können. Da der PC, von dem aus das Internet genutzt wird, gelegentlich auch im lokalen Netz betrieben wird, sind mitunter einzelne Dateiverzeichnisse oder Laufwerke dieses PC für einen Zugriff über das lokale Netz freigegeben. Wird dieser PC dann mit dem Internet gekoppelt und die Freigabe nicht widerrufen, so besteht auch für Internet-Teilnehmer die Möglichkeit, auf die freigegebenen Daten zuzugreifen.

Aufgrund dieser spezifischen Risiken ist von einer Installation abzuraten, bei der ein PC sowohl an das Internet als auch an das lokale Netz angeschlossen werden kann.

4.3 Computerviren - ein hartnäckiges Problem

Computerviren sind zu einer erheblichen Bedrohung für die Computersicherheit geworden. Ständig entstehen neue Viren oder tauchen Varianten bereits bekannter Viren auf. Nicht selten sind innerhalb weniger Stunden nach dem ersten Auftauchen weltweit bereits viele Millionen Computer infiziert. Häufig trifft es Computer, die mit dem Betriebssystem Windows, gelegentlich auch in Kombination mit dem Programm Outlook, ausgestattet sind. Akut bedroht sind daher auch entsprechende Computer öffentlicher Stellen. Um zu illustrieren, wie die Verbreitung eines solchen Virus vonstatten geht, hier ein Blick auf den "I-love-you"-Virus, der im Jahr 2000 weltweit große Schäden anrichtete:

Seinerzeit landeten E-Mails mit dem Betreff "I love you" in einer Vielzahl elektronischer Postfächer. Der verlockenden Botschaft "Ich liebe dich" konnten Millionen Computernutzer nicht widerstehen, zumal es sich beim jeweiligen Absender der Mail um keinen Unbekannten handelte, sondern um jemanden, von dem man in der Regel bereits früher elektronische Nachrichten erhalten hatte. Sie öffneten die als Anhang zu dieser E-Mail versandte Datei, begierig darauf zu erfahren, was sich denn hinter der elektronischen Liebeserklärung verbirgt. Damit nahm dann das Unheil seinen Lauf. Die Datei enthielt, obwohl sie wie ein harmloser Text daherkam, ein sog. Makro-Programm, das nach dem Öffnen der Datei sofort ausgeführt wurde: Das Programm sandte Kopien der ursprünglichen "I-love-you"-Nachricht an alle Mail-Adressen, die der Empfänger in seinem Outlook-Adressbuch hinterlegt hatte. Die Lawine kam in Gang. Zudem löschte das Virus bestimmte Dateien.

Es ist unerlässlich, dass die für die Datenverarbeitung verantwortlichen Stellen Vorkehrungen gegen derartige Virusinfektionen treffen. Darüber hinaus muss aber auch jeder einzelne Internet-Nutzer für die Viren-Gefahren sensibilisiert werden und lernen, sich richtig zu verhalten. Ein Schaden entsteht nämlich in der Regel erst dann, wenn die Benutzer erhaltene elektronische Post öffnen. Insbesondere sollten sie Folgendes beachten:

- Bei jeder eingegangenen elektronischen Post sollte der Empfänger den Betreff sorgfältig lesen. Vorsicht ist bei auffälligen Betreff-Angaben geboten. Dazu gehören englischsprachige Betreffs wie "I love you", "Important Message from..." oder "Pics for you", selbst wenn diese von ihm bekannten Absendern stammen. Derartigen E-Mails angeschlossene Anlagen dürfen unter keinen Umständen geöffnet werden; stattdessen ist umgehend der Systemverantwortliche zu benachrichtigen.
- Vorsicht ist ebenfalls geboten, wenn man von einem deutschen Absender plötzlich elektronische Post mit einem englischsprachigen Betreff erhält. Auch in solchen

Fällen dürfen die Anlagen der eingegangenen elektronischen Post nicht geöffnet werden.

- Wer als Anlage zu einer elektronischen Postsendung ein ausführbares Programm erhält (Dateien mit den Endungen .com, .bat, .sys, .bin, .exe, .vbs etc.) sollte dieses nur starten, wenn der Versand der Anlage mit dem Absender zuvor abgestimmt wurde. Unangekündigt eingegangene ausführbare Programme sollten dagegen nicht in Gang gesetzt werden. Stattdessen ist entweder Kontakt mit dem Absender der elektronischen Post aufzunehmen oder der Systemverantwortliche der Dienststelle zu unterrichten. In der gleichen Weise sollte der verfahren, der per elektronischer Post komprimierte Dateien erhält und beim Dekomprimieren feststellt, dass ausführbare Programme übersandt wurden.
- Das Herunterladen von Freeware- oder Shareware-Programmen aus dem Internet und das Herunterladen von Spielen sollten grundsätzlich unterbleiben.

4.4 Höhere Sicherheit vor Viren und anderen Schadensprogrammen

Virenattacken à la "I love you" lösten auch Diskussionen um die Sicherheit von Firewalls aus. Denn sie machten deutlich, dass selbst Firewalls keinen ausreichenden Schutz vor Computerviren, die aus dem Internet stammen und via E-Mail versandt werden, bieten können. Unzulänglich schützen Firewalls aber auch vor sog. aktiven Inhalten, die beim Surfen im World Wide Web (WWW) auf interne PC gelangen können und dort vielfach automatisch ausgeführt werden. Es handelt sich dabei um Schadensprogramme, die als JavaScript-Anwendungen, Java-Applets oder Active-X-Controls realisiert sein können. Nicht auszuschließen ist, dass Viren und aktive Inhalte gezielt dazu eingesetzt werden, den Firewall-Schutz zu durchlöchern und schutzbedürftige Daten heimlich ins Internet zu schleusen. Es gilt daher, die Sicherheitstechnik so fortzuentwickeln, dass sie auch solchen Angriffen standhalten kann. Ansätze hierfür sind vorhanden, unter anderem:

- Signatur für Makros
  Mittlerweile lassen sich einige Programme, mit denen Computerbenutzer ihre elektronischen Postfächer leeren, so einstellen, dass ein in einem E-Mail-Anhang enthaltenes Makroprogramm nur dann ausgeführt wird, wenn es durch eine digitale Signatur als vertrauenswürdig gekennzeichnet ist. Nicht-signierte Makros werden dagegen nicht ausgeführt.
- Auslagerung des Browsers
  Aktive Inhalte des World Wide Web können Schaden anrichten, wenn sie auf einen internen Computer gelangen und dort von dem Browser ausgeführt werden, den man zum Surfen im World Wide Web benutzt. Eine Möglichkeit, Schaden durch aktive Inhalte des World Wide Web abzuwehren, beruht auf der Idee, den Internet-Browser aus dem internen Netz zu verbannen und auf einen Computer zu verlagern, der außerhalb des internen Netzes angesiedelt ist und auf dem keine sicherheitsrelevanten oder schutzbedürftigen Daten gespeichert sind. Damit das Internet-Surfen aber weiterhin auch von internen Computern aus möglich ist, wird auf den internen Computern ein Programm eingesetzt, das lediglich den Bildschirminhalt des auf dem externen Computer installierten Browsers, letztlich also eine Menge von Bildpunkten, wiedergibt. Entscheidend ist dabei, dass aktive Inhalte auf diesem Weg gar nicht erst ins interne Netz gelangen können.
- Verschlüsselung schutzbedürftiger Daten
  Eine anderer Ansatz zum Schutz der im internen Netz gespeicherten

personenbezogenen Daten geht davon aus, dass ein hundertprozentiger Schutz vor Angriffen aus dem Internet nicht zu erreichen ist und setzt deshalb auf die Verschlüsselung aller im internen Netz gespeicherten personenbezogenen Daten. Selbst wenn es einem Angreifer gelänge, sich diese Daten zu verschaffen, so wären diese Informationen für ihn wertlos, da er sie nicht im Klartext lesen könnte.

5. Was ist bei der Nutzung der Internet-Dienste zu beachten?

Wer - sei es dienstlich oder privat - Internet-Dienste nutzt, sollte dabei Folgendes beachten:

5.1 Vorsicht beim Download

Um dem Risiko entgegenzuwirken, dass aus dem Internet heruntergeladene Programme mit unerwünschten Schadensfunktionen auf einem eigenen PC ausgeführt werden, sollte jeder Benutzer für dieses Risiko sensibilisiert sein.

5.2 Übertragung schutzbedürftiger Daten

Sofern personenbezogene oder andere schutzbedürftige Daten zu übertragen sind, sollte dies nur verschlüsselt geschehen. Eine nach dem Stand der Technik vorgenommene Verschlüsselung bietet dabei die Gewähr, dass die Daten nicht von Unberechtigten zur Kenntnis genommen werden können. Werden die Daten zusätzlich digital signiert, lässt sich auch die Identität des Absenders zuverlässig nachweisen. Ferner ist anhand der digitalen Signatur zu erkennen, ob die Daten während der Übertragung manipuliert wurden.

Wollen mehrere am Internet angeschlossene Teilnehmer oder Einrichtungen untereinander schutzbedürftige Daten austauschen, so bietet sich hierfür die Einrichtung eines sog. virtuellen privaten Netzwerks (VPN) an.

5.3 Hinweise rund um das Web

Surft man durch das World Wide Web und ruft dabei einzelne Informationsseiten ab, so können sowohl im Internet als auch auf dem PC des Nutzers Datenspuren zurückbleiben. Die auf dem PC zurückbleibenden Spuren sind besonders problematisch, wenn sie in Verzeichnissen gespeichert werden, auf die alle Nutzer des PC Zugriff haben.

5.3.1 Cookies

Ruft man Informationen im World Wide Web ab, so kann es sein, dass der Informationsanbieter auf dem PC des Internet-Nutzers eine kleine Datei, eben das Cookie, speichert. Ruft der Surfer von seinem PC aus später das Web-Angebot erneut auf, so wird das

Cookie vom heimischen PC zurück an den Informationsanbieter übertragen, der anhand der darin enthaltenen Informationen einen Zusammenhang zwischen dem früheren und dem aktuellen Abruf herstellen kann. Vielfach geht die Speicherung von Cookies sogar unbemerkt vom Surfer vonstatten. Zwar stellen Cookies, im Gegensatz zu Viren, keine ausführbaren Programme dar und können daher den betroffenen PC nicht unmittelbar schädigen. Unbedenklich ist der Einsatz von Cookies gleichwohl nicht. Mit ihrer Hilfe lassen sich nämlich Interessenprofile erzeugen. Besonders aussagekräftige Profile entstehen bei Internet-Werbeunternehmen, die sog. Werbebanner in Web-Angebote anderer Informationsanbieter einblenden. Das geht wie folgt vor sich:

Ruft ein Internet-Nutzer das Angebot z. B. eines Gebrauchtwagenhändlers auf, auf dessen Web-Seiten Banner eines Werbeunternehmens eingeblendet werden, so kann dieses Unternehmen auf dem PC des Surfers ein Cookie anlegen und darin festhalten, dass sich dieser für Gebrauchtwagen interessiert. Besucht dieser Internet-Nutzer danach von seinem PC aus das WWW-Angebot eines Warenhauses, das vom gleichen Werbeunternehmen mit Banner-Werbung bestückt wird, so sendet der PC das bereits vorhandene Cookie an das Werbeunternehmen. Dieses kann ihm entnehmen, dass sich der Surfer zuvor für Gebrauchtwagen interessiert hat. Es kann dann an diesem PC gezielt dafür werben. Interessiert sich der Internet-Nutzer beim Besuch des Warenhaus-Angebotes besonders für Jugendstilmöbel, so kann das Werbeunternehmen auf dem PC des Internet-Nutzers ein Cookie speichern, in dem neben dem bereits vorher bekannten Interesse für "Gebrauchtwagen" nun auch das für "Jugendstilmöbel" dokumentiert wird.

Zwar erfährt das Werbeunternehmen auf diese Weise nicht, welche Person die Informationen abrief, gleichwohl entsteht, einem Mosaik gleich, Stück für Stück ein Interessenprofil. Dass große Werbeunternehmen mit vielen tausend Inhaltsanbietern zusammenarbeiten, lässt erahnen, wie detailliert diese Mosaike werden können. Teilt der Surfer, beispielsweise bei der Teilnahme an einem Internet-Preisausschreiben, dann noch seinen Namen mit, so können auch diese Angaben in das Profil aufgenommen und dieses damit unmittelbar auf den Surfer bezogen werden. Aber auch wenn die Interessenprofile zunächst noch keinen unmittelbaren Personenbezug aufweisen, ist dies problematisch, da nicht auszuschließen ist, dass dieser später hergestellt wird. Dabei ist auch zu bedenken, dass für die im Ausland ansässigen Internet-Werbeunternehmen mitunter wesentlich geringere Datenschutzanforderungen gelten als dies hierzulande der Fall ist. Daher empfiehlt sich aus Sicht des Datenschutzes generell ein restriktiver Umgang mit Cookies. Die einfachste Möglichkeit dazu ist, den eigenen Internet-Browser so einzustellen, dass er keine Cookies annimmt.

Manche Internet-Angebote setzen sie aber auch sinnvoll ein, etwa wenn es beim Tele-Shopping darum geht, beim Händler verschiedene Waren gleichzeitig zu bestellen. Ohne den Einsatz von Cookies könnten diese nicht quasi in einem Warenkorb auf einmal, sondern jeweils nur einzeln geordert werden. Will man solche Angebote nutzen, sollte man den Browser so einstellen, dass der Surfer über den Cookie-Einsatz informiert wird und ihn im Zweifel ablehnen kann. Hat man einmal Cookies akzeptiert, so sollte man diese nach Abschluss der Internet-Recherche löschen.

5.3.2 Cache-Speicherung

Jede Angebotsseite, die ein Nutzer im World Wide Web abruft, wird auf der Festplatte seines PC im sog. Cache-Bereich des Browsers abgespeichert. Dies hat folgenden Vorteil: Will der Nutzer auf eine Angebotsseite zugreifen, die bereits auf der Festplatte hinterlegt ist, muss er sie nicht erneut aus dem Internet anfordern, sondern sie lässt sich schnell von der Festplatte

laden. Die Kehrseite dieser Medaille ist freilich, dass alle diejenigen, die Zugriff auf diesen Cache-Bereich haben, feststellen können, auf welche Internet-Angebote frühere Nutzer des PC zugegriffen haben. Wer dies verhindern will, muss die im Cache gespeicherten Seiten löschen, nachdem er seine Arbeit im Internet beendet hat. Manche Browser lassen sich auch so einstellen, dass abgerufene Seiten gar nicht erst im Cache auf der lokalen Festplatte gespeichert werden.

5.3.3 History-Liste/Liste zuletzt aufgerufener Web-Seiten

In der History-Liste sowie in der Liste der zuletzt aufgerufenen Web-Seiten vermerken gängige Browser, welche Web-Seiten in der zurückliegenden Zeit abgerufen wurden. Will man erneut eine Seite laden, die man vor einigen Minuten, Stunden oder Tagen bereits abgerufen, deren genaue Adresse man sich aber nicht notiert hatte, so kann man darin nachsehen und einfach den entsprechenden Eintrag anklicken. Ähnlich wie die Cache-Speicherung birgt dieses Vorgehen das Risiko, dass andere Personen diese Daten lesen und damit erfahren können, für welche Internet-Angebote sich frühere Nutzer interessierten. Wer sich dieser Gefahr nicht aussetzen möchte, sollte die Einträge aus der History-Liste sowie der Liste zuletzt aufgerufener Web-Seiten löschen oder diese Listen deaktivieren.

5.4 Passwort für Internet-Zugang und für Web-Services nicht auf dem PC speichern

Die für den Zugang zum Internet verwendeten Programme bieten mitunter die Möglichkeit, die hierfür erforderlichen Passwörter sowie Passwörter für die Nutzung zugriffsbeschränkter Internet-Dienstleistungen auf dem PC abzuspeichern. Da diese Passwörter mitunter nur unzureichend vor unberechtigter Nutzung geschützt sind, sollte man davon keinen Gebrauch machen.

6. Hinweise für Stellen, die eigene Informationsangebote im Internet bereitstellen

Wer mit einem eigenen Informationsangebot im Internet präsent sein will, sollte aus Sicht des Datenschutzes folgende Punkte bei der Gestaltung des Angebots und beim Betrieb der hierfür erforderlichen Informationsserver beachten:

6.1 Anordnung der Server

Wer über ein eigenes Netzwerk verfügt, das über eine Firewall mit dem Internet gekoppelt ist, und mit Hilfe eines WWW- oder eines FTP-Servers Informationen im Internet anbieten will, steht vor der Frage, wo die dafür notwendigen Informationsserver anzuordnen sind. Folgendes ist dabei zu berücksichtigen:

- Anordnung im internen Netz
  Bindet man den Informationsserver in das interne Netz ein, so lässt er sich über die Firewall vor Angriffen aus dem Internet schützen. Die Notwendigkeit, viele externe

Zugriffe auf einen oder mehrere interne Rechner rund um die Uhr zulassen zu müssen, stellt gleichzeitig jedoch einen Nachteil dar, denn es widerspricht dem Ziel, Zugriffe von außen auf das zu schützende Netz so weit wie möglich zu minimieren.

- Anordnung auf dem Gateway-Rechner
  Gegen die technisch mögliche Installation eines Informationsservers auf dem Gateway-Rechner spricht, dass ein solcher Rechner nur für die sicherheitsrelevanten Aufgaben eingesetzt werden sollte, die er unbedingt erbringen muss, also im Wesentlichen für die Filterung von Datenpaketen, zur Adressumsetzung sowie zur Protokollierung. Dies trägt dem Umstand Rechnung, dass jedes Mehr an Programm-, Daten- und Befehlsumfang auf diesem Computer Sicherheitsrisiken mit sich bringt, etwa aufgrund von Programmfehlern oder weil es die Überwachung des Firewall-Betriebs erschwert.
- Anordnung in einem geschützten Bereich
  Eine weitere Möglichkeit besteht darin, Informationsserver in einem geschützten Bereich ("demilitarisierte Zone") zwischen Gateway-Rechner und äußerem Paketfilter so anzuordnen, dass das Paketfilter zwar WWW- oder FTP-Anfragen aus dem Internet an diesen Server weiterreicht, nicht dagegen andere Zugriffe. Unter Berücksichtigung der Vor- und Nachteile der einzelnen Alternativen stellt diese Möglichkeit die sicherheitstechnisch sinnvollste Lösung dar.

6.2 Gestaltung der Web-Angebote/Privacy-Policy

Das Teledienstegesetz sowie der Mediendienste-Staatsvertrag verpflichten zumindest alle Anbieter geschäftsmäßiger Informationsangebote, ein Impressum in ihr Angebot aufzunehmen und darin den Namen des für den Inhalt Verantwortlichen sowie dessen Postanschrift zu nennen. Es empfiehlt sich, in diesem Zusammenhang, auch gleich über die Verwendung aktiver Inhalte zu informieren sowie darauf hinzuweisen, ob personenbezogene Daten der Nutzer gespeichert werden und, wenn ja, für welchen Zweck dies geschieht und wann die Daten wieder gelöscht werden. Dies ist auch der Ort, um über den Einsatz von Cookies zu unterrichten.

6.3 Elektronische Dienstleistungen für den Bürger

Immer mehr Behörden informieren die Öffentlichkeit in eigenen Internet-Angeboten darüber, welches Amt für welche Anliegen zuständig ist, wo es zu finden ist, wie die Sprechzeiten sind und welche Unterlagen etwa bei einer Ummeldung, der Zulassung eines Kraftfahrzeugs oder der Aufgebotsbestellung im Falle einer Heirat vorzulegen sind. Mitunter besteht für den Antragsteller gleich noch die Möglichkeit, Antragsformulare beispielsweise zur Ummeldung nach einem Umzug oder zur Reservierung eines Kfz-Wunschkennzeichens vom heimischen PC aus abzurufen, auszufüllen und auf elektronischem Weg wieder an die Behörde zu senden, die die Formulare dann ausdruckt. Dabei darf die Information der Bürger über ihre Rechte und die mit dem Datentransport im Internet verbundenen Risiken nicht zu kurz kommen:

- Stellt eine Behörde im Internet amtliche Formulare zum Abruf bereit, so muss sie dafür sorgen, dass die im gedruckten Formular enthaltenen Hinweise zum Datenschutz dem Bürger auch dann gegeben werden, wenn er das Formular über Internet abruft. Das war bisher jedenfalls nicht immer selbstverständlich.

- Soweit im Internet elektronische Formulare verwendet werden, deren Gestaltung amtlich vorgeschrieben ist, wie dies beispielsweise für die Meldung des Zuzugs, Wegzugs oder Umzugs beim Einwohnermeldeamt der Fall ist, ist Folgendes zu beachten: Das amtliche Vordruckmuster enthält nicht nur die Fragen, die man beantworten muss, nebst zugehörigen Erläuterungen, sondern auch Hinweise darauf, in welchen Fällen der Einwohner der Weitergabe seiner Daten durch das Einwohnermeldeamt widersprechen kann. Diese Datenschutzhinweise dürfen natürlich auch im Fall elektronischer An-, Um- oder Abmeldung nicht fehlen; die Behörde muss vielmehr dafür sorgen, dass die Bürger sie zur Kenntnis nehmen, bevor sie ihre Daten elektronisch an die Behörde senden.
- Unverschlüsselt im Internet übertragene Daten sind nicht vor unberechtigter Kenntnisnahme geschützt. Daher sollte jede Stelle, die elektronische Bürgerdienste anbietet, bei denen auch personenbezogene Daten übertragen werden, vorsehen, dass dies verschlüsselt erfolgt. Solange eine solche Möglichkeit nicht zur Verfügung steht, muss sie die Bürger darüber informieren, dass die Daten unverschlüsselt übertragen werden und welche
  Risiken damit verbunden sind. Damit der Bürger es selbst in der Hand hat, von einem elektronischen Versand seiner Daten Abstand zu nehmen, muss ihn die Information natürlich erreichen, bevor er seine Daten eingibt und elektronisch versendet. Sofern medizinische oder andere sensible personenbezogene Daten übertragen werden sollen, stellt die Verschlüsselung eine unverzichtbare Anforderung dar.
- Sollen die elektronisch übermittelten Antragsdaten einen eigenhändig unterschriebenen Antrag ersetzen, so muss sich die Behörde Gewissheit über die Identität des Antragstellers verschaffen. Ansonsten wäre dem Missbrauch Tür und Tor geöffnet: Anträge ließen sich dann unter falschem Namen stellen mit der Folge, dass möglicherweise auf deren Grundlage Verwaltungsentscheidungen getroffen und im Zusammenhang damit falsche Angaben über Bürger gespeichert werden, die unter Umständen finanzielle (Verwaltungsgebühren, Mahnkosten) oder andere Nachteile für die vermeintlichen Antragsteller zur Folge haben können.
  Bei einem herkömmlichen Antrag auf Papier lässt sich im Zweifelsfall anhand der eigenhändigen Unterschrift entscheiden, ob dieser tatsächlich von dem genannten Antragsteller stammt. Als elektronisches Pendant zur eigenhändigen Unterschrift bietet sich die digitale Signatur an: Das zu unterzeichnende elektronische Dokument wird dabei mit Hilfe eines kryptografischen Verfahrens in besonderer Weise gekennzeichnet; jeder kann anhand einer solchen Kennzeichnung überprüfen, von wem diese vorgenommen wurde. Um die gewünschte Fälschungssicherheit und Zuverlässigkeit beim Umgang mit digitalen Signaturen erreichen zu können, müssen zuvor zahlreiche technische und organisatorische Festlegungen über die Erzeugung, Ausgabe und Verwendung der Signaturschlüssel getroffen werden. Hierzu gehören beispielsweise Sorgfaltsregeln für die Stellen (Trust-Center), die die Signaturschlüssel herstellen, Vorgaben zur Frage, wie lange einmal vorgenommene Signaturen als sicher angesehen werden können und auf welche Weise man Signaturschlüssel erkennt, die für eine weitere Verwendung gesperrt wurden. Nun muss nicht jede Stelle, die digitale Signaturen nutzen will, alle diese Maßnahmen selbst festlegen. Entscheidet man sich für die im Signaturgesetz definierte qualifizierte Signatur, so kann man eine Reihe aufeinander abgestimmter und sich gegenseitig ergänzender Maßnahmen zurückgreifen, die im Signaturgesetz und der dazugehörigen Signaturverordnung dargestellt sind und ein verhältnismäßig hohes Maß an Sicherheit bieten. Zusätzliche Sicherheit lässt sich erreichen, wenn das Trust-Center ein Akkreditierungsverfahren bei der Regulierungsbehörde für Post und Telekommunikation durchlaufen hat. Will

man von diesen Standards abweichen, ist darauf zu achten, dass die Sicherheit des Signaturverfahrens am Ende nicht auf der Strecke bleibt.

6.4 Sicherheitsinteressen der Internet-Nutzer beachten

Wie oben bereits dargestellt, gehen Internet-Nutzer, die in ihrem Browser die Ausführung aktiver Inhalte wie Java-Applets, JavaScript-Anwendungen oder ActiveX-Controls gestatten, erhebliche Sicherheitsrisiken ein. Jede Stelle, die ein eigenes Web-Angebot gestaltet, sollte auf die Verwendung dieser Inhalte nach Möglichkeit verzichten. Web-Angebote oder zumindest deren Teile, in denen lediglich Informationen präsentiert werden, sollten grundsätzlich ohne aktive Inhalte auskommen. Wenn die Nutzung dieser Funktionen unverzichtbar ist, sollte Java bevorzugt werden, da es für die Ausführung von Java-Applets ein Sicherheitsmodell gibt, das allerdings in der Vergangenheit wiederholt fehlerhaft programmiert war. Ferner sollten die Nutzer darauf hingewiesen werden, welche Funktionen des Angebots auf diese Weise realisiert werden und weshalb deren Einsatz überhaupt erforderlich ist. In den Teilen des Angebots, in denen die aktiven Inhalte nicht benötigt werden, ist auf deren Einsatz zu verzichten.

6.5 Datenschutzgerechte Protokollierung der Abrufe

Wer eigene Angebote ins Internet einstellt, will in aller Regel wissen, wie oft welche Angebotsseiten abgerufen wurden. Mitunter protokollieren die Betreiber der WWW-Server hierzu nicht nur, wann welche Angebotsseite abgerufen wurde, sondern registrieren auch die Netzadresse des abrufenden Computers, die sog. IP-Adresse.

Bei dieser Vorgehensweise ist Folgendes zu bedenken:
Der numerischen IP-Adresse eines am Internet angeschlossenen Computers lässt sich mit Hilfe des DNS-Dienstes ein Name zuweisen. Daraus geht häufig hervor, in welchem Land der Rechner installiert ist. Zudem gibt der Rechnername oft auch Aufschluss über die Stelle, die den Rechner betreibt, beispielsweise ein Universitätsinstitut. Schon allein dies lässt einen Rückschluss auf den Kreis derjenigen zu, die mit diesem Rechner arbeiten. Vollends zu einem persönlichen Merkmal werden Rechnername und Netzadresse, wenn der Internet-Nutzer immer mit demselben Computer arbeitet, diesen Rechner allein nutzt und die Adresse dieses Computers im Internet verwendet wird. Mit anderen Worten: IP-Adressen können personenbezogen sein. Für die Anbieter von WWW-Angeboten hat dies folgende Konsequenz: Da sie mit ihren Angeboten in der Regel Tele- oder Mediendienste anbieten, müssen sie die Datenschutzregelungen des Teledienstedatenschutzgesetzes oder des Mediendienste-Staatsvertrags der Länder beachten. In beiden heißt es klipp und klar, dass der Diensteanbieter personenbezogene Daten über die näheren Umstände des einzelnen Abrufs spätestens mit dem Beenden der Verbindung löschen muss, es sei denn, er benötigt die Daten noch für Zwecke der Abrechnung. Da die IP-Adressen je nach konkretem Einsatz personenbezogen sein können, dürfen IP-Adressen nach erfolgtem Web-Seiten-Zugriff allenfalls für Abrechnungs- nicht aber für andere Zwecke gespeichert werden.

7. Weitere Informationen zum Themenbereich Internet, e-Government und Datenschutz

Datenschutz bei der Nutzung von Internet und Intranet

Orientierungshilfe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder, Stand: 15. Dez. 2000, herausgegeben vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern

Vom Bürgerbüro zum Internet

Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand 21. Nov. 2000, hrsg. vom Landesbeauftragten für den Datenschutz Niedersachsen

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz vom 8. März 2002

www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/oh-arbeitsplatz.htm

CERT

Hinweise über aktuelle Sicherheitslücken und Gegenmaßnahmen finden sich in den Internet-Angeboten der Computer Emergency Response Teams (CERT), z. B.

- CERT des Deutschen Forschungsnetzes (DFN-CERT):

  www.cert.dfn.de

- CERT der Universität Stuttgart:

  www.cert.uni-stuttgart.de

- CERT für Bundesbehörden (CERT-Bund):

  www.bsi.bund.de/certbund/index.htm

BSI

Das Bundesamt für Sicherheit in der Informationstechnik hält zahlreiche Informationen und Materialien zum Thema IT-Sicherheit zum Abruf bereit

www.bsi.bund.de

IT-Grundschutzhandbuch des BSI

Eine umfangreiche Zusammenstellung sicherheitsrelevanter Aspekte beim Einsatz von Computern, darunter auch solche, die die Realisierung von Internet-Anschlüssen betreffen, sowie entsprechende Maßnahmenkataloge finden sich im IT-Grundschutzhandbuch des BSI.

www.bsi.bund.de/gshb/index.htm

Studien des BSI aus den Jahren 2001 und 1997 zu Firewallprodukten

www.bsi.bund.de/literat/studien/firewall/fwstud.htm

e-Government-Handbuch des BSI

Im e-Government-Handbuch gibt das BSI unter anderem auch einen umfassenden Überblick über die mit eGovernment-Projekten einhergehenden Sicherheitsfragen.

www.bsi.bund.de/fachthem/egov/6.htm

Virtuelles Datenschutzbüro

Weitere Informationen rund um das Thema Datenschutz finden sich im Internet-Angebot des virtuellen Datenschutzbüros, das von zahlreichen nationalen und internationalen Datenschutzbeauftragten getragen wird

www.datenschutz.de

Vom Intranet zum Mitarbeiterportal:

E-Government für die Mitarbeiter – was gehört dazu?[1]

E i n e S k i z z e

(Stand 5. April 2004)

von Heinrich Reinermann, Speyer

Das Verständnis von „Mitarbeiterportalen“ ist keineswegs schon gefestigt.

Es zeichnet sich aber ab, dass es um mehr geht als darum, für die Beschäftigten ein Fenster auf ihre Personalabteilung zu öffnen (obwohl allein dies ein willkommener Schritt nach vorn ist).

Im Folgenden soll unter „Mitarbeiterportal“ der zentrale und direkte elektronische Zugang einer einzelnen Mitarbeiterin oder eines einzelnen Mitarbeiters zu den für sie oder für ihn wichtigen Informationen, Kommunikationsbeziehungen und Transaktionen unabhängig von deren räumlicher Verteilung verstanden werden, in aller Regel über einen Bildschirmarbeitsplatz.

Letztendlich hat eine Institution (Unternehmung, Verwaltung, Behörde) dann – aus Sicht der Beschäftigten – so viele Mitarbeiterportale wie Mitarbeiter.

Der Entwurf eines Mitarbeiterportals muss mit dem Mitarbeiterbild heute und morgen beginnen. Der 30-minütige Einführungsvortrag gliedert sich deshalb in drei Teile:

- Was sind die Merkmale und Trends unserer Arbeitswelt? Nur, wer diese als Leitbild vor Augen hat, kann Mitarbeiterportale sinnvoll einrichten. (Teil I)

- Was sollen Mitarbeiter an ihrem Mitarbeiterportal tun können, wenn sie ihre Arbeit am vorgenannten Leitbild ausrichten wollen? Was müsste das Portal also leisten können? (Teil II)

- Wie ist bei der Einrichtung von Mitarbeiterportalen vorzugehen? (Teil III)

---

[1] Die AWV untersuchte schon vor ziemlich genau 30 Jahren (beginnend im Oktober 1974) empirisch „Strukturellen Aufbau und Leistungsbreite bestehender Personal-Informationssysteme“ (veröffentlicht Frankfurt, Mai 1976, 107 Seiten). Gedacht war die Studie als Ausgangspunkt für ein standardisiertes Modell-PIS für Wirtschaft und Verwaltung, aus dem allerdings nichts wurde. S. 13 hieß es: „Am weitesten fortgeschritten und auch voll EDV-gestützt sind ... Lohn- und Gehaltsabrechnung, Personalstatistik und Personalverwaltung. Die Bereiche der eigentlichen Personalplanung sind bisher noch wenig einbezogen.“
Diese Diagnose galt für lange Zeit (sie gilt zum Teil noch heute), indem die Personalsteuerung mehr über Dienstrecht und Haushalt (Stellenpläne als Erläuterungen zum Haushaltsplan) erfolgte als im Sinne einer eigenständigen Ressourcenplanung, die gleichberechtigt neben Aufgaben-, Organisations- und Finanzplanung zu treten hätte.

Teil I: Die Rahmenbedingungen unserer Arbeitswelt lassen sich durch mehrere (zum Teil interdependente und redundante, aber gerade dadurch einen Trend bestätigende) Merkmale charakterisieren:

1. Es gibt eine „Neue elektronische Erreichbarkeit“ von Personen, Daten, Programmen und Objekten über bisherige Grenzen durch Raum, Zeit oder Hierarchie hinweg – ein nach wie vor unterschätztes Phänomen.

2. So gut wie alle Arbeitsplätze setzen mittlerweile den Umgang mit IT voraus.

3. Uns umgibt eine anhaltend rasche informationstechnische Entwicklung, mit der Schritt zu halten ist.

4. Die Ausbreitung von Innovation wird durch Hypermedien (Verlinkung) enorm beschleunigt („Jeder weiß alles sofort/muss alles sofort wissen“; in der „Wissensgesellschaft“ muss man „ein Leben lang lernen“).

5. Die Bildung von Netzwerken in weltweitem Maßstab schreitet fort (etwa PPP, Outsourcing, Offshoring).

6. Virtuelle Netzwerkinstitutionen (VNI) breiten sich als eine neue Organisationsform aus und beeinflussen alle: als Staaten, als Unternehmen und Behörden, als Einzelpersonen. Versuche des Gegensteuerns („Stop the world, I want to get off...“) scheinen von zweifelhafter Erfolgsaussicht zu sein. Daraus folgt:

    - Man kann überall und sogar global präsent sein, so auch als Anbieter von Arbeit:

        - innerhalb eines Arbeitsverhältnisses (stationär oder mobil, auf Dienstreise, in einem Telearbeitsverhältnis)
        - in mehreren parallelen Arbeitsverhältnissen, Selbständigkeit eingeschlossen (Wettbewerbsverbote lassen sich nur noch für bestimmte Aufgaben durchsetzen, Ich-AGs wie auf Basis von eBay spielen eine wachsende Rolle)
        - nebeneinander bei Arbeit, Erziehung, Weiterbildung, Erholung, Auszeit, etc. („Work-life balance“, „New work“ und ähnliche Konzepte).

    - Man ist aber, als Kehrseite davon, auch weltweitem Wettbewerb ausgesetzt:

        - durch Konkurrenten innerhalb der Institution, für die man tätig ist
        - durch Konkurrenten außerhalb dieser Institution.

7. Die Ökonomisierung des Verwaltungshandelns verlangt von immer mehr Beschäftigten ein Rollenverhalten als „Intrapreneur“ im Rahmen von New Public Management.

8. Good Governance wird als Handlungsmaßstab auch des öffentlichen Dienstes eingefordert, mit Kriterien wie: rechtmäßig („legale Herrschaft“ ist für die Legitimität öffentlichen Handels nach wie vor unabdingbar), demokratisch, verantwortungsbewusst, transparent, partizipativ, nachhaltig, sozial-integrierend, vertrauenswürdig, rechtzeitig, wirkungsvoll und effizient.

9. Die Einstellungen der Beschäftigten werden in der Informations- oder (besser) Netzwerkgesellschaft geprägt durch sogenannte:

    - Netzethik (freien Zugang zu Information haben, „angeschlossen“ sein)
    - Entscheidungsethik (mitwirken können, möglichst selbst ohne Zwischeninstanzen entscheiden können)
    - Arbeitsethik (sich voll für die Belange eines Netzwerks einsetzen, ein professioneller Knoten im Netz sein)
    - Geldethik (Leistungen „auf Gegenseitigkeit“ austauschen, an einer „Economy of sharing“ teilhaben).

Wie, mit welchem Mitarbeiterbild eine Verwaltung oder Behörde auf solche Rahmenbedingungen reagiert, wird unterschiedlich sein, ist aber mitentscheidend für den Entwurf ihrer Mitarbeiterportale. Diese sind folglich keine „neue informationstechnische Modeerscheinung“. Vielmehr geht es bei einem Mitarbeiterportal um die Umsetzung des Selbstverständnisses von Arbeitgeber und Arbeitnehmer in Hardware und Software.

Teil II: Wie muss ein „Mitarbeiterportal“ aussehen, insbesondere: Welche Aktivitäten sind zu unterstützen, damit der öffentliche Dienst den vorgenannten Rahmenbedingungen bzw. dem Leitbild, das eine Verwaltung oder Behörde daraus für sich konkret ableitet, gerecht werden kann? Dies ist heute weit weniger eine informationstechnische Frage („Alles ist möglich“) als eine konzeptionelle.[2]

Zwei Aspekte lassen sich dabei nicht mehr trennen:

- Wie soll ein Mitarbeiterportal aus Arbeitnehmersicht aussehen?
- Wie soll es aus Arbeitgebersicht aussehen?

Denn der typische Arbeitsplatz im öffentlichen Dienst wird heute durch „Knowledge worker“ besetzt (wenngleich damit nicht verkannt werden soll, dass es eine Vielzahl und im Detail unterschiedlicher Arbeitsplätze sowie dass es, auch im öffentlichen Dienst, „Blue collar“-Arbeitsplätze gibt). Immer weniger findet sich im Büro Routinearbeit „von 8 bis 5“. Die Beschäftigten werden längst zum Kreis der „Stakeholder“ von Unternehmungen und Verwaltungen gezählt sowie weniger als Kostenblock denn als Aktivposten verstanden. Außerdem verbringen wir, über unsere Funktion eines „Produktionsfaktors“ hinaus, einen Großteil unseres Lebens mit Arbeit, und wir bringen unsere Persönlichkeit mit zur Arbeit. Immer mehr ist deshalb bei der Gestaltung von IT-Unterstützung „der ganze Mensch“ mit seinem Gesamtbefinden einschließlich seiner persönlichen Ziele und Motivationen im Auge zu haben.[3]

---

[2] Auf die Einbeziehung computergesteuerter Arbeitsräume wird hier verzichtet. Dazu etwa das Verbundprojekt „Office 21 – Zukunft der Arbeit“ des IAO der FhG.

[3] Tatsächlich bestehen für ein Erreichen von Punkt „9,9“ im von Robert Blake und Jane Mouton 1964 vorgestellten „Managerial grid“ (also des Eckpunktes aus maximaler Behördenorientierung und maximaler Mitarbeiterorientierung) heute auch relativ gute Chancen.

Im Ergebnis heißt das: Sowohl die Arbeitgeber- als auch die Arbeitnehmerinteressen müssen sich in ein und demselben Mitarbeiterportal manifestieren (ohne dass diese damit zugleich deckungsgleich zu sein hätten). Aus diesem Grunde sind auch die nachfolgend skizzierten zwei Sichten ebenso interdependent und redundant wie trendanzeigend.

(Eine dritte Sicht, nämlich die Externer wie Staat oder Verbände, kann hier trotz ihrer Bedeutung nicht weiter behandelt werden.)

A) Eher Arbeitgebersicht:

1. Die Arbeitgeber haben ein Interesse daran, die Beschäftigtenarbeitsplätze optimal mit IT auszustatten, damit diese als Modul der Unternehmung/Behörde wettbewerbsfähig sind, also schnell, kostengünstig sowie ziel- und adressatenzentriert arbeiten, zum Beispiel alle nötigen Informationen mit digitalen (nicht unbedingt papierlosen) Verfahren er- und verarbeiten können, oder: Routineauskünfte mit einmaligen Kosten ins Netz stellen, statt mit Telefon- oder persönlichen Auskünften immer wieder dieselben variablen Kosten zu verursachen, oder: bei Auftreten eines Problems schnell ein Team aus Experten zusammenstellen oder Web-Konferenzen abhalten können.

2. Ein maßgeblicher, die Daseinsberechtigung öffentlichen Handelns konstituierender Aspekt ist sicher zu stellen: Der Arbeitgeber muss gewährleistet sehen, dass die richtigen Vorgänge in die vorgesehenen Zuständigkeitsbereiche fallen und die betreffenden Mitarbeiter mit den nötigen Kompetenzen, Regeln, Ressourcen und Qualifikationen ausgestattet sind. Es muss also legal gehandelt werden - „Max Weber“ ist nicht außer Kraft gesetzt. Vielmehr liegt eine der Herausforderungen von Mitarbeiterportalen in der Versöhnung der heute informationstechnisch begründeten Mitarbeiterfreiräume mit dem Anspruch der Bürger auf „legale, rationale Herrschaft“.

3. Das Arbeitsprogramm der jeweiligen Mitarbeiter sollte, schon deshalb, so weit wie möglich als „Regelbasiertes System“ zur Verfügung stehen, also programmiert zwecks:

    - absichtsgemäßer Anwendung und Einhaltung der Vorschriften
    - gezielte Schulung der Normanwender ebenso wie der Normadressaten
    - Erfahrungsaustausch mit anderen, auch externen Normanwendern über das Netz
    - Erfassung von Normwirkungen
    - Ermunterung zur Kommentierung durch Mitarbeiter („Behördliches Vorschlagswesen“) und Adressaten (CRM)
    - Rückkoppelung zum Normgeber
    - gezielte schnelle Informierung der Normanwender über Novellierungen unmittelbar am Mitarbeiterportal.

4. Die Mitarbeiter als einzelne Module müssen optimal in Netzwerke eingebunden werden können (eine traditionelle „8 bis 5“-Kontrolle funktioniert nicht mehr). D.h. Führung durch Zielvereinbarung, Controlling und Management-Informations-Systeme müssen gepflegt werden, damit die Institution möglichst sicher sein kann, dass sich einzelne Module nicht unbemerkt „ausklinken“.

5. Das Mitarbeiterportal muss, im Rahmen von ERP-Systemen sowie analog dem schon länger akzeptierten und professionalisierten Finanzmanagement, ein „Human Resources“-Management unterstützen, also:

   - die Anforderungen an den Arbeitsplatz definieren helfen
   - Bewerbungen und Bewerberauswahl unterstützen
   - Stärken- und Schwächenanalyse der Stellenbesetzung ermöglichen
   - Beurteilungen und Mitarbeitergespräche ergebnisorientiert handhaben können
   - daraus Fortbildungsbedarf ableiten lassen
   - eine gezielte und zeitgerechte Planung und Durchführung von Fortbildungsveranstaltungen unterstützen
   - die Personalentwicklung auf eine möglichst sichere Basis stellen
   - zu rechtzeitiger Personalplanung für Ausscheidende anregen
   - „Abschiedsinterviews“ erheben lassen
   - „Alumni“-Netze unterstützen.

6. Mitarbeiterportale müssen „Klebstoff“ enthalten, damit volatile Module das Netzwerk nicht gegen den Willen des Arbeitsgebers verlassen, das „Humankapital“ erhalten bleibt. Dazu gehören:

   - Informationen, welche die Identifikation mit der eigenen Institution fördern (etwa deren Aufgaben, Leitbilder, Ziele und Erfolge, Pläne und ihre Begründungen)
   - Informationen über die regionale Umgebung (Kultur-, Bildungs-, Freizeitmöglichkeiten und anderes, was mitentscheidend ist, in der Region und der jeweiligen Institution zu bleiben)
   - „Employee Relationship Management“ (ERM) als Ansatz, Mitarbeiterbindung durch Kennen der und Eingehen auf individuelle Bedürfnisse zu erreichen.

7. Andererseits muss ein Mitarbeiterportal „Magnetismus“ enthalten, damit im Wettbewerb um die qualifiziertesten Köpfe Externe zur Ergänzung des eigenen Netzwerks angezogen und gewonnen werden können („War for talents“). Die Arbeitsplätze müssen attraktiv für die Besten sein - eine besondere Herausforderung für den öffentlichen Dienst.

8. Interna („Geschäftsgeheimnisse“) müssen vor Ausplaudern durch die Mitarbeiter oder vor Abhören („Werksspionage“) geschützt werden können.

9. Die Personalverwaltungsaufgaben (also die Information „über“ Mitarbeiter) sollen wirksam und reibungslos, möglichst elektronisch funktionieren, so: Einstellung, Bezahlung, Beförderung, Entlassung; Raumausstattung und –besetzung; Organigramme; Schlüsselverwaltung; Zutritts- und Zugriffsberechtigung; Dienstausweis; digitale Signatur; Terminkalender; etc.

B) Eher Arbeitnehmersicht:

1. Mitarbeiter wollen im „Web workstyle“ arbeiten können, um auf der Höhe der Zeit zu sein, aber auch um beschäftigungsfähig zu bleiben, also mit einer zeitgemäßen IT-Ausstattung umgehen, die Arbeitsressourcen digital und online überall zur Verfügung haben, offen kommunizieren, in einer professionellen Umgebung arbeiten, erfüllende

Tätigkeiten statt stumpfsinniger Routine ausführen, möglichst selbstorganisiert arbeiten (Arbeitszeit und –ort), denselben Informationsstand haben wie die Kollegen, etc. Dabei vermischen sich behördliche und private Nutzung des Mitarbeiterportals, was Regelungsbedarf hervorruft.[4]

2. Die IT-Ausstattung selbst muss als zweckmäßig empfunden werden, mit Eigenschaften wie:

   - Das Mitarbeiterportal muss die benötigten Portaltechniken für Information, Kommunikation und Transaktion bieten (etwa Zugriffs-, Präsentations-, Navigations-, Recherche-, Kommunikations-, Kollaborations-, Dokumentenmanagement-, Prozessmanagement-, Sicherheits- und Personalisierungsdienste („Mein-Arbeitsplatz.de")).
   - Es muss, weil die Beschäftigten mit ihrer Arbeit davon abhängig sind, samt seiner Datenbestände möglichst ausfallsicher sein. Es muss schon von sich aus Bedienungsfehler möglichst gar nicht erst zulassen, andernfalls diese weitestgehend selbsttätig reparieren.
   - Hotline und persönliche Betreuung müssen bei auftretenden Problemen mit dem Portal schnell und zuverlässig funktionieren.
   - Das Portal muss Ansprüchen der Ergonomie (bis hin zu „Single-sign login") und der Barrierefreiheit gerecht werden.
   - Schutz vor „Spam mail" und unerwünschten Netzinhalten muss gewährleistet sein, wo dieses im Mitarbeiterinteresse liegt.
   - Die persönliche, gewohnte, im Portal abgebildete Arbeitsumgebung muss bei Bedarf mitgenommen werden können (also ein „Roaming" mit „Ambient intelligence" ermöglicht werden).
   - Nicht zuletzt muss der Schutz der persönlichen Arbeitnehmerdaten gewährleistet sein („Gläserne Behörde" statt „gläserne Mitarbeiter").

3. Das Portal soll so ausgelegt sein, dass die jeweils übliche Bürosoftware sowie die nötigen Datensicherungsmethoden (wie Aktenmäßigkeit, Verschlüsselung, elektronisch Unterschrift, Virenschutz, Sicherheitskopien) von den Mitarbeitern leicht, möglichst „zwangsläufig" angewendet werden. Ebenso leicht, möglichst automatisch, muss die Aktualisierung von den Mitarbeitern im Web zu pflegender Daten vonstatten gehen.

4. Über das Mitarbeiterportal wollen die Beschäftigten so mit IT und Informationen versorgt sein, dass sie ihre Aufgaben zur Zufriedenheit des Arbeitsgebers erledigen und damit ihren Arbeitsplatz sichern bzw. sich unentbehrlich machen können. Das impliziert u.a.: möglichst gezielten Zugriff auf alle wichtigen Informationen haben, über wesentliche Änderungen wie Rechtsvorschriften (und zwar sowohl die Sachbearbeitung betreffendes Recht als auch das die Mitarbeiter als Klienten betreffende Recht), über Prioritäten der Leitung etc. gezielt informiert werden.

5. Alle wichtigen Pläne, Programme, „To do"-Listen, „Drehbücher" (Was ist in welchem Falle von wem zu tun?), Formulare, Erfahrungen u.ä. müssen im Intranet der Institution zur Verfügung stehen (sogenanntes Wissensmanagement („Wenn Siemens wüsste, was Siemens weiß..."). „Dateninseln" müssen möglichst zusammengeführt werden. Dabei muss das Informationssystem die individuellen

[4] Dazu gibt es einen Vorschlag von BITKOM, Die Nutzung von Email und Internet im Unternehmen, Berlin/Frankfurt 2003.

Informationsbedürfnisse sowie deren Vergangenheit kennen und anwenden. Darüber hinaus müssen die Arbeitnehmer immer wieder durch geeignete Methoden auf die Existenz der im Netz verfügbaren Inhalte aktiv hingewiesen werden, denn die Vorstellung vom „Wissen als Holschuld“ stößt mittlerweile an faktische Grenzen.

6. Externe Informationen von Bedeutung für die einzelnen Mitarbeiter sollten über Links zugänglich und möglichst erschlossen sein, etwa individuelle Verkehrsinformationen für Fahrten von und zur Arbeit (Fahrpläne, Staumeldungen), Finanzinformationen für die „Riester-Rente“ oder andere Vorsorgeaktivitäten, Gesundheits-, Entspannungs- und Freizeittipps, „Travel management“ etc.

7. Mitarbeiterportale müssen dazu angelegt sein, den Beschäftigten die Chance zur Weiterqualifizierung zu eröffnen, weil dies sowohl für eine optimale Erledigung der jeweiligen Tätigkeiten als auch für die Erhaltung der Beschäftigungsfähigkeit („Life-long employability“) erforderlich ist (E-Learning, Web-based training u.a.- allein im IT-Bereich und nur als Beispiele Cisco Networking Academy oder IBM Global Campus). Erworbene Fähigkeiten und Zertifikate müssen mitarbeitergesteuert in die zugehörige Personalakte sowie in das HR-Management einfließen.

8. Das Portal muss Transparenz des internen Arbeitsmarktes ermöglichen (Job-Börsen etc.).

9. Lebens- und Geschäftslagen müssen als digitale Prozessangebote über das Portal unterstützt werden, beispielsweise: gezielter Zugriff auf das Dienstrecht, das Sozialrecht u.a. beziehungsweise möglichst aktive individuelle Informierung der Mitarbeiter über sie persönlich angehende Veränderungen und Erfordernisse (ist z.B. ein Antrag auf Zusatzurlaub rechtmäßig?) in diesen Bereichen; „unbürokratische“ Beschaffung des eigenen Bürobedarfs über das Portal; einfache, möglichst digitale Abwicklung der eigenen Personalverwaltungsaufgaben, die aus dem „Kunden“-Verhältnis der Mitarbeiter zum Arbeitgeber folgen, in Bereichen wie Dienstreisen einschließlich Verkehrsmittel- und Hotelreservierung, Beihilfe, Urlaub, Fortbildung, Krankheit, Beurteilung u.a.; Verwaltung der eigenen Personalangelegenheiten über ein „virtuelles Schließfach“ – die Personalverwaltung als „Service center“.

10. Dabei sollte, wo immer möglich, auf formalisierte Personalverwaltungsverfahren zugunsten von Selbstorganisation verzichtet werden, z.B. Ersatz der Verwaltung von Urlaubs- und Dienstreiseanträgen oder der Kontrolle von Telefongesprächen durch Transparenz im Netz und damit einhergehende soziale Kontrolle; Aktualisierung ihrer Personaldaten durch die Betreffenden selber („Employee self-service“).

Teil III: Was ist bei der Einrichtung von Mitarbeiterportalen zu beachten? (Aus Zeitgründen erfolgen hierzu nur noch Andeutungen, obwohl dieser Teil für die praktische Umsetzung von geradezu erfolgsentscheidender Bedeutung ist.)

1. Am Beginn sollte die gemeinsame Erarbeitung eines Leitbildes stehen. Denn es ist nicht davon auszugehen, dass die in Teil I genannten Rahmenbedingungen allseits bekannt sind. Vor allem ist nicht von vornherein klar, in welchem Maße sie geteilt werden. Es scheint außerdem für Mitarbeiterportale noch ein geringerer externer Druck als für Bürgerportale zu bestehen. Statt wie bei der „Wasserfallmethode“ gleich

mit der Programmierung eines Mitarbeiterportals zu beginnen, ist also zunächst „ein zu lösendes Problem“ zu erarbeiten.

2. Hierzu braucht man ein Projektmanagement mit Lenkungsausschuss (Behördenleitung, Personalrat, Fach-, Personal-, Organisations-, Haushalts- und IT-Abteilungen), Projektleitung und Projektgruppe (hier sind die betroffenen Mitarbeiter unersetzlich, denn sie kennen ihre Wünsche am besten). Ein Prototyp für die jeweilige Verwaltung oder Behörde ist zu konfigurieren, damit die konkreten Mitarbeiterportale zweckgerecht und mit Aussicht auf Akzeptanz gestaltet werden können.

3. Besonders wichtig sind schließlich Anreizstrukturen, damit die Mitarbeiterportale in der Praxis wirklich zur maßgeblichen Informations-, Kommunikations- und Transaktionsplattform werden. Die vorgesehenen Daten müssen von den Mitarbeitern auch eingegeben bzw. abgerufen, also wirklich genutzt werden („Bring- und Holschuld“). Zwischen Pflege und Nutzung besteht darüber hinaus ein enger Zusammenhang (Enttäuschungen bei der Suche von Informationen führen schließlich zur Abwendung vom Mitarbeiterportal). Vermieden werden muss mithin:

   - dass Daten als „Eigentum“ (etwa der Personalabteilung) betrachtet werden oder nach „Wissen ist Macht“ (etwa Horten wichtiger Informationen) verfahren wird
   - dass „kleine Königreiche“ abgegrenzt und von „störenden“ Informationen abgeschottet werden
   - dass sich einige aus der elektronischen Kommunikation „ausklinken“ und dann Medienbrüche sowie Staus im Informationsfluss die Folge sind (insofern ist auch der aus den „Bürgerportalen“ bekannte Multikanal-Zugang bei Mitarbeiterportalen grundsätzlich untauglich, was nicht ausschließen soll, dass Kioske für Beschäftigte ohne Arbeitsplatzcomputer eingerichtet werden).

4. Ob es ein Wunschtraum bleibt, dass bei unserer Verwaltungskultur an die Gestaltung von Mitarbeiterportalen mit der gleichen Begeisterung (um das Wort Inbrunst zu vermeiden) heran gegangen wird wie an die Ausarbeitung von Vorschriften?

R:\AUFSATZ\Bremen220404

Private Internetnutzung am Arbeitsplatz
Rechtslage im Überblick

von RA Prof. Dr. Klaus Sakowski

Inhaltsübersicht

Allgemeines
Arbeitsrecht
Steuerrecht

Allgemeines

Spätestens seit Ausbruch des "Moorhuhn - Fiebers" ist es mit der stillschweigenden Duldung der privaten Internet - Nutzung ("Surfen") am Arbeitsplatz während der Arbeitszeit vorbei. Eine am 29.8.2000 im Auftrag von Sterling Commerce veröffentlichten Studie kommt zum Ergebnis, dass mehr als 60 Prozent aller Arbeitnehmer mit Internetzugang mindestens einmal am Tag aus privaten Gründen am Arbeitsplatz surfen. Jeder Beschäftigte verbringt durchschnittlich 3,2 Std. pro Woche ohne betrieblichen Anlass online. Dadurch entsteht pro Mitarbeiter ein Arbeitsausfall von mehr als 17 Tagen im Jahr. Bei Arbeitskosten von durchschnittlich 49,23 DM / Std. und 16,2 Mio. Arbeitsplätzen mit Internetzugang entstehen im Jahr Kosten von 104 Mrd. DM - ohne Berücksichtigung von Netzgebühren.

Nach einer Mitteilung der F.A.Z. (Nr. 38, 14.2.2003, S. 18), die sich wiederum auf einen Bericht des "Spiegel" von Frühjahr 2002 stützt, hat der Landesrechnungshof von Niedersachsen im vorangehenden Zeitraum binnen 10 Tagen eine Untersuchung des "Internet - Surfverhaltens" der öffentlichen Angestellten des Bundeslandes durchgeführt, die über insgesamt 20.000 PC - Arbeitsplätze Zugang zum Internet haben. Danach konnte bei über 40% der aufgerufenen Seiten auf eine private Nutzung geschlossen werden. Besonders beliebt waren offensichtlich Angebote von "eBay" sowie Sex - Angebote. Der Musik - Download spielte dagegen eine eher vernachlässigbare Rolle (vgl. hierz auch die Pressemitteilung 1/02 des Rechnungshofes, in dem verschiedener Kritik auf die Bewertungen und Ergebnisse der Studie entgegen getreten wird).

Arbeitsrecht

Allgemein

Die Fragen, die mit dem privaten Surfen zusammen hängen, sind in einem Arbeitsvertrag zumeist (noch) nicht ausdrücklich geregelt. Deshalb muss für eine rechtliche Beuruteilung auf allgemeine Grundsätze zurück gegriffen werden.

Auszugehen ist vom Zweck des Arbeitsverhältnisses. Geschuldet wird eine Arbeitsleistung gegen Zahlung von Entgelt. Die Art und Weise der Arbeitsleistung bestimmt der Arbeitgeber kraft seines Direktionsrechts (Weisungsrechts). Er ist berechtigt, die Leistung des Arbeitnehmers zu überwachen und davon Kenntnis zu nehmen, in welcher Weise der Arbeitnehmer seine Arbeitsleistung erbringt. Das Direktionsrecht berechtigt den Arbeitgeber auch, ein generelles Verbot der privaten Nutzung des Internet auszusprechen. Dies kann z.B. in Form einer Rund - Mail oder eines Aushangs geschehen. Soweit ein Betriebsrat eingerichtet wird, ist eine entsprechende Vereinbarung zwischen dem Arbeitgeber und dem Betriebsrat (Betriebsvereinbarung) vonnöten (siehe unten). Der Arbeitnehmer, der gegen das Verbot aus einer Einzelanweisung oder Betriebsvereinbarung verstößt, kann abgemahnt werden. Bei

wiederholtem Verstoß ist eine fristlose Kündigung möglich. Das vorherige Abmahnerfordernis ist nur in seltenen Fällen entbehrlich, z.B. wenn der Arbeitnehmer durch das private Surfen einen Straftatbestand (Stichwort: Kinderpornografie) verletzt.

Auch soweit es grundsätzlich erlaubt ist oder zumindest stillschweigend geduldet wird, darf der Arbeitnehmer am Arbeitsplatz nicht in ausschweifendem Umfang privaten Tätigkeiten nachgehen. Diese gehören nicht zur vertraglichen Arbeitsleistung. Als Folge kommt ein Verstoß gegen die vertragliche Treuepflicht (§ 242 BGB) in Betracht, wenn das im Unternehmen übliche Maß überschritten wird.

Rechtsprechung

In seinem Urteil vom 21.3.2001 (5 Ca 4021/00) entschied das ArbG Wesel, dass eine private Internet-Nutzung in einem Gesamtumfang von 80 - 100 Stunden innerhalb eines Zeitraums von 12 Monaten keinen "wichtigen Grund" darstellt, der eine fristlose Kündigung rechtfertigen würde. Im Betrieb bestand kein generelles Verbot der privaten Internet-Nutzung. Auch eine vorherige Abmahnung wurde nicht für entbehrlich gehalten. Der betroffenen Arbeitnehmerin musste die Schwere der Pflichtverletzung nicht unmittelbar einleuchten, zumal es um die Anfangsphase der Installation der neuen Computeranlage im Betrieb ging. In diesem Zeitraum müsse der Arbeitgeber bei Nichtaussprache eindeutiger Regeln mit einer gewissen "spielerischen Anlernphase" der Mitarbeiter rechnen.

Die Richter stellen, ausgehend von der bereits bestehenden und unten angesprochenen Rechtsprechung zur privaten Nutzung anderweitiger betrieblicher Mittel, folgende Grundsätze auf: Nutzt der Arbeitnehmer das Internet entgegen einem ausdrücklichen Verbot des Arbeitgebers für private Zwecke, so stellt dies eine arbeitsvertragliche Pflichtverletzung dar, die eine Kündigung des Arbeitsverhältnisses rechtfertigen kann. Hat der Arbeitgeber dagegen die private Nutzung genehmigt bzw. über einen gewissen Zeitraum hinweg widerspruchslos geduldet, kommt eine Kündigung nur in Ausnahmefällen in Betracht, nämlich dann, wenn die Nutzung in einem Ausmaß erfolgt, von dem der Arbeitnehmer nicht mehr annehmen durfte, diese sei noch vom Einverständnis des Arbeitgebers gedeckt.

Dementsprechend ist das ArbG Hannover (Urteil vom 1.12.2000 - 1 Ca 504/00 B) der Ansicht, dass die fristlose Kündigung eines Mitarbeiters ohne vorherige Abmahnung rechtmäßig war, der während der Arbeitszeit sowohl Dateien mit pornografischem Inhalt aus dem Internet auf den betrieblichen PC heruntergeladen als auch eine einschlägige Homepage vom betrieblichen PC aus in das WWW gestellt hatte. In diesem Falle war den Arbeitnehmern das private Surfen vom Arbeitgeber in einer Betriebsvereinbarung untersagt worden. Zum selben Ergebnis (fristlose Kündigung ohne Abmahnung gerechtfertigt) kommt das ArbG Düsseldorf (4 Ca 3437/01). Hintergrund war das Betrachten pornografischer Seiten am Arbeitsplatz trotz Verbots privaten Internet - Surfens im Arbeitsvertrag. Allerdings meint das Gericht auch, dass sich der Arbeitnehmer ohne arbeitsvertragliche Regelung auf eine stillschweigende Duldung durch das Unternehmen berufen könne.

Mitbestimmungsrechte

Nach § 87 Abs. 1 Ziff. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einrichtung und Anwendung technischer Kontrolleinrichtungen. Betriebsräte können in Betrieben mit mindestens fünf (Vollzeit-) Beschäftigten gebildet werden. Entscheidend ist die objektive Eignung der Anlage zur Kontrolle, nicht die tatsächliche Absicht oder Handhabung des Arbeitgebers. Hier hat der Betriebsrat das Recht zur Erzwingung einer Betriebsvereinbarung.

Nach § 87 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat auch ein Mitbestimmungsrecht bei der Regelung von Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer im Betrieb. Davon umfasst ist auch der Umgang mit dem Internet - Anschluss. Der Arbeitgeber muss sich in dieser Frage also mit dem Betriebsrat abstimmen und eine Betriebsvereinbarung

schließen. Im Falle einer Nichteinigung entscheidet die betriebliche Einigungsstelle (§ 76 BetrVG).

Reformpläne

Das vom Bundesarbeitsministerium angekündigte "Arbeitnehmer - Datenschutzgesetz", das jedem Arbeitnehmer das Recht geben soll, an seinem Arbeitsplatz auch im Internet zu surfen, ist bislang nicht verabschiedet worden. Dieses "private Surf - Recht" soll jedoch durch arbeits- oder tarifvertragliche Regelungen eingeschränkt werden können. Die Kosten der privaten Nutzung können dem Arbeitnehmer auferlegt werden. Damit muss es aber auch zulässig sein, die Verbindungsdaten zur Ermittlung und Abrechnung dieser Kosten zu erheben.

Arbeitgeber dürfen nach der Entwurfsfassung nicht überwachen, welche Internet - Seiten von den Arbeitnehmern aufgerufen werden. Einschränkungen soll es im Falle strafrechtlicher Ermittlungen gegen den Arbeitnehmer oder bei Vorliegen eines "schwerwiegenden Verdachts auf missbräuchliche Nutzung" geben. Globalauswertungen aller abgerufenen Seiten im Unternehmen soll es geben dürfen. Dies dürfte jedoch bei kleinen Firmen problematisch sein. Den Zugang zu einzelnen Webseiten darf der Arbeitgeber sperren.

Steuerrecht

Wer meint, dass auch dem Steuergesetzgeber im Sinne der Füllung des Steuersäckels daran gelegen sein müsste, dass mehr gearbeitet und weniger Moorhühner geschossen werden, der irrt. Das private Surfen am Arbeitsplatz ist aufgrund einer Gesetzesinitiative des Bundesfinanzministeriums, der die Bundesländer zugestimmt haben, rückwirkend zum 1.1.2000 gänzlich steuerfrei gestellt worden. Danach muss für die Privatnutzung von Internet und TKeinrichtungen keine Einkommensteuer entrichtet werden. Darüber hinaus erfolgt auch eine Befreiung von der Lohnsteuer, was automatisch auch zum Wegfall der bisherigen Aufzeichnungspflichten führt.

Begründet wird die Initiative zum einen damit, dass bürokratische Erschwernisse wie eine Steuer- und Veranlagungspflicht die Menschen von einer Heranführung an die neuen Medien abhalten. Zum anderen wäre zu erwarten, dass die Einnahmen aus einer "Surfsteuer" nicht einmal den verwaltungstechnischen Aufwand decken würden. Die geltende Freigrenze beträgt 50 EUR / Monat.

Eine Befreiung von der Umsatzsteuer darf dagegen offenbar aus europarechtlichen Gründen nicht erfolgen. Wie das Bundesfinanzministerium in einem Schreiben vom 11.4.2001 mitteilt, handele es sich bei der Umsatzsteuer um eine Abgabe auf den gesamten privaten Konsum von Waren und Dienstleistungen. Das gelte für kostenlose betriebliche Internetnutzung ebenso wie für kostenlose Mahlzeiten oder die Bereitstellung eines Dienstwagens. Der Erlass unterscheidet allerdings drei Fallgestaltungen. Wenn der Arbeitgeber dem Arbeitnehmer Computer oder TKgeräte zur privaten Nutzung gegen Entgelt zur Verfügung stellt, ist dieser Vorgang umsatzsteuerpflichtig. Eine Internet - Privatnutzung gegen den Willen des Arbeitgebers liegt dagegen eine nicht willentliche Wertabgabe des Arbeitgebers und damit ein nicht steuerbarer Vorgang vor. Im Falle einer ausdrücklichen Erlaubnis zur Nutzung von Internet oder Telekommunikation für private Zwecke liege dagegen eine steuerpflichtige Wertabgabe vor.

Nach Abschn. 12 Abs. 4 der USt.-RL sind nicht steuerbare Leistungen dadurch gekennzeichnet, dass sie überwiegend durch das betriebliche Interesse des Arbeitgebers veranlasst sind, wenn die Nutzung betrieblicher Einrichtungen zwar auch die Befriedigung eines privaten Bedarfs der Arbeitnehmer zur Folge hat, diese Folge aber durch die mit der Nutzung angestrebten betrieblichen Zwecke überlagert wird.

Einführung in den Bildungsplan 2004

PROFESSOR DR. HARTMUT VON HENTIG
IM AUFTRAG DES BILDUNGSRATES BADEN-WÜRTTEMBERG

Der Titel enthält ein Programm und ein Datum. „Bildungsplan" sagt: Es geht um eine begründete Ordnung des gesamten Auftrags der allgemein bildenden Schulen. „2004" sagt: Es handelt sich um eine Antwort auf die jetzt gegebenen und erkennbaren Erwartungen an diese Einrichtung.

Ein „Bildungsplan 2004" unterscheidet sich von den bisherigen Lehrplänen zunächst durch den Singular – er fasst zusammen, Lehrpläne legen auseinander. Er unterscheidet sich von diesen sodann durch einen in dem deutschen Wort „Bildung" mitgeführten Anspruch: Sie soll junge Menschen in der Entfaltung und Stärkung ihrer gesamten Person fördern – so, dass sie am Ende das Subjekt dieses Vorgangs sind.

Lehrpläne geben an, was „gelehrt" werden soll. Ein Bildungsplan gibt an, was junge Menschen im weitesten Sinne des Wortes „lernen" sollen: Auf welche Anforderungen und Ziele hin sie sich am besten an welchen Erfahrungen formen und welche Mittel zur Gestaltung ihres Lebens, welche Übung in welchen Fähigkeiten dabei dienlich sind – Mittel und Fähigkeiten, die ihnen ermöglichen, als Person und Bürger in ihrer Zeit zu bestehen.

Dieser Vorgang vollzieht sich weitgehend in Schulen und durch die in ihnen tätigen Lehrerinnen und Lehrer. Insofern enthält ein Bildungsplan auch, „was gelehrt wird", stellt dies aber in den Dienst eines umfassenden Erziehungs- und Bildungsauftrags, den sich die Gesellschaft erteilt.

Die Absichten, die die Landesregierung mit dem Bildungsplan 2004 verfolgt, gehen weit über eine „Antwort auf die Ergebnisse von Timss und Pisa" und anderer internationaler Vergleichsuntersuchungen hinaus. In einer sich schnell verändernden Welt sind gerade die Einrichtungen zu aufmerksamer Beobachtung und sorgfältiger Berücksichtigung der Entwicklungen verpflichtet, denen die Gesellschaft beides aufgetragen hat: die Wahrung der Kontinuität und Identität ihres Bewusstseins und die Ermöglichung von geordnetem und ersprießlichem Wandel. In den Schulen werden die Menschheitserfahrungen und die in ihnen erworbenen Maßstäbe für das „gute Leben" weitergegeben – an den Schulen werden zugleich die Instrumente für eine noch unbestimmte Zukunft bereitgestellt. Es geht in ihnen immer um eine Balance zwischen Verantwortung und Unvoreingenommenheit, von Bewahrung und Bewährung. Hier sieht die Landesregierung Anlässe zu maßvollen, aber deutlichen Veränderungen der Gegenstände, Verfahren und Gewohnheiten der Schule.

Die wichtigsten Anlässe für die Vorlage eines neuen Bildungsplans seien hier kurz aufgezählt – jeweils mit dem einen oder anderen Beispiel:

- *Die Wissenschaft* bringt nicht nur ständig neue Erkenntnisse über Sachverhalte hervor, sondern auch über ihre eigenen Voraussetzungen, Wirkungen, Vermittlungsformen und Folgen. Die Hirnforschung etwa legt eine andere Einstellung zum Frühlernen nahe; die Lernforschung hat den Blick für die außerordentliche Wirksamkeit der Lernumstände geöffnet. Die beschleunigte Ausdehnung des verfügbaren Wissens verlangt nach Strategien der Zusammenfassung und nötigt zu veränderten Formen des Lernens.
- *Die Technik* nimmt dem Menschen physische und geistige Mühsal ab, fordert aber im Gegenzug die Steuerung ihrer immer komplexeren Aggregate, eine bewusstere Berücksichtigung ihrer Folgen für die Natur und für unsere körperliche und seelische Gesundheit, ein weiterreichendes Verantwortungsbewusstsein für die sich verselbstständigenden Mittelsysteme. Die neuen Medien etwa verändern das Verhältnis von Wissen, Denken und Erfahrung in der Bildung; sie verändern auch das Verhältnis des Menschen zu Zeit und Entfernung, Geld und Arbeit.

- Das *wirtschaftliche und politische Zusammenwachsen* der Welt erhöht die Zahl der Beziehungen, in die die Menschen zueinander treten, und damit die Notwendigkeit von Verständigung und die Gefahr von Missverständnis und Konflikt. Es entstehen größere Regelungseinheiten – Europa, die Vereinten Nationen, die Ökumene, international tätige Nicht-Regierungs-Organisationen (NGOs), und multinationale Konzerne –, in die man nicht hineingewachsen ist, sondern zu denen sich eine Loyalität erst bilden muss; die Heterogenität der in ihnen lebenden Bevölkerung, die Wanderbewegungen, das soziale Gefälle nehmen zu. Darum wird etwa das Lernen von Sprachen und das Verstehen fremder Lebensformen für den Einzelnen und die jeweilige Gesellschaft überaus wichtig.

Die Grundtatbestände, die in die Stichworte und Stichdaten „Tätervolk“ oder „11. September 2001“, „Contergan“ oder „Tschernobyl“, „demografische Entwicklung“ oder „Klimawandel“, „Internet“ oder „Globalisierung“, „Hoyerswerda“ oder „Erfurt“ eingegangen sind, verlangen heute mehr als die enzyklopädische Wissensbildung des 19. Jahrhunderts. Schon gar nicht genügt die Bescheid-Wissens-Bildung, zu der sich diese im Laufe des 20. Jahrhunderts abgewandelt hat. Jene Grundtatbestände verlangen etwas, was Humboldts Vorstellung von „formaler Bildung“ nahe steht – eine Konfiguration von wenigen, aber grundlegenden „Kompetenzen“. Eine Kompetenz ist eine komplexe Fähigkeit, die sich aus richtigem Wahrnehmen, Urteilen und Handelnkönnen zusammensetzt und darum notwendig das Verstehen der wichtigsten Sachverhalte voraussetzt. Die neue Konfiguration von Kompetenzen und die in den Wörtern „richtig“ und „wichtig“ enthaltenen normativen Momente darzustellen und zu begründen, ist die Absicht dieses Bildungsplans 2004 – in ihr sind die angedeuteten Anlässe zusammengefasst.

Die mit dem Bildungsplan 2004 unternommene Anstrengung wird zusätzlich motiviert durch die Ergebnisse wissenschaftlicher Untersuchungen, die aufdecken, dass die Bildungseinrichtungen sich über die Wirksamkeit ihrer Arbeit täuschen. Der Bildungsplan hat also die gedanklichen und institutionellen Bedingungen dafür zu schaffen, dass solche Selbsttäuschung nicht eintritt: Er muss klare Maßstäbe für die Überprüfung aufstellen.

Jeden Bildungsplan wird man künftig daran messen, ob die ihm zugrunde liegenden Vorstellungen und die von ihm veranlassten Maßnahmen geeignet sind, in der gegenwärtigen Welt

- die Zuversicht junger Menschen, ihr Selbstbewusstsein *und* ihre Verständigungsbereitschaft zu erhöhen,
- sie zur Wahrnehmung ihrer Aufgaben, Pflichten und Rechte als Bürgerinnen und Bürger anzuleiten,
- sie in der Urteilsfähigkeit zu üben, die die veränderlichen, komplexen und abstrakten Sachverhalte unseres Lebens fordern,
- ihnen die Kenntnisse zu erschließen, die zum Verstehen der Welt notwendig sind,
- sie Freude am Lernen und an guter Leistung empfinden zu lassen,
- ihnen Unterschiede verständlich zu machen und die Notwendigkeit, diese unterschiedlich zu behandeln: die einen zu bejahen, die anderen auszugleichen.

Dies alles sollte in Formen geschehen, die auch den Lehrerinnen und Lehrern, Erziehern und Erzieherinnen bekömmlich sind.

Keines dieser Kriterien kann ohne genauere Bestimmung der planbaren Voraussetzungen erfüllt werden. Die Zusammenfassung dieser Voraussetzungen ist die Aufgabe eines Bildungsplans.

Die Verbindlichkeit des Bildungsplans 2004 ist in drei Ebenen gestuft. In der ersten Ebene werden staatliche Vorgaben gemacht; sie sind also für die einzelnen Schulen verpflichtend. Auf der zweiten Ebene werden diese Vorgaben anhand von ausgewählten Beispielen veranschaulicht; diese selbst sind nicht verbindlich, wohl aber das in ihnen jeweils zum Ausdruck kommende Niveau. Auf der dritten Ebene werden Varianten für die praktische Umsetzung zur Verfügung gestellt. Die zentralen Prüfungen und Vergleichsarbeiten beziehen sich auf die erste Ebene.

Im Bildungsplan 2004 sind die Bildungsstandards ein Mittel zur vereinfachten und übersichtlichen Ordnung des Bildungsgangs. Das geschieht dadurch, dass Erwartungen auf bestimmten Stufen benannt werden, an denen dann überprüft werden kann, ob die Schule/die Schulen fähig waren, sie zu erreichen. Bildungsstandards werden also im Bildungsplan 2004 den einzelnen Schularten und Fächern beziehungsweise Fächerverbünden zugeordnet, müssen sich aber an den allen allgemein bildenden Schulen gemeinsamen Erwartungen ausrichten. Letztlich lassen sich diese nicht aus dem Gesamtzusammenhang des Bildungsplans herauslösen, der sich darum hier in der Einführung einer gemeinverständlichen Gliederung und untechnischer Termini bedient: Im Bildungsplan kommt (1) eine bestimmte Vorstellung vom Auftrag der Schule zur Geltung; werden (2) die von den Schülern und Schülerinnen zu erreichenden Ziele aufgeführt – unterschieden als (a) Erfahrungen, die sie machen, und „Einstellungen", die sie daran gewinnen sollen, (b) „Fähigkeiten", die sie beherrschen sollen, und (c) „Kenntnissen", die sie haben sollen; werden (3) die didaktischen und methodischen Prinzipien genannt, denen zu folgen ist; werden (4) die Maßnahmen und Einrichtungen aufgeführt, die der Sicherung des Auftrags, der Ziele und der Prinzipien dienen. In diesem Teil dienen die Bildungsstandards einer spezifischen Aufgabe: der Überprüfung.

DER AUFTRAG DER SCHULE

Die neuzeitliche Pflichtschule verdanken wir der Reformation und dem Merkantilismus – alle Menschen sollten die Bibel lesen können und alle sollten einem für das Gemeinwesen nützlichen Gewerbe nachgehen können. Die Adelskultur, in der sich praktische und politische, gelehrte und gesellige, zeremonielle und schöne Künste vereinten, lernte man bei Hofe, bei eigens dazu berufenen Hofmeistern und am Ende auf den ökonomischeren Ritterakademien. Das nachdrängende Bürgertum begnügte sich mit Schreibschulen und später mit Gelehrtenschulen, die den gesellschaftlichen Aufstieg ermöglichten und deren Ergebnis, die Schulbildung, bezeugte, dass man „dazugehörte". Der Nationalstaat sorgte dafür, dass auf allen Schulstufen und in allen Schularten die gewünschte patriotische Gesinnung gelehrt wurde. Erst im 20., im republikanischen Jahrhundert bildete sich ein Bewusstsein von „politischer" Bildung, die die öffentliche Schule dem Staatswesen und den jungen Bürgerinnen und Bürgern schuldet. In neuester Zeit wird aus diesen das Zukunftspotenzial, die *human resource,* von der die Standortsicherheit der jeweiligen Gesellschaft abhängt.

Aus diesem Gemenge von Absichten und Aufträgen muss die Bildungsplanung eine Auswahl treffen und diese in eine begründete Ordnung bringen, die allgemeine Zustimmung findet. Im vorliegenden Bildungsplan 2004 sieht das so aus:

1. Die von der Schule zu erbringende Leistung sei „Bildung". Bildung hat drei Bestimmungen. Sie ist *erstens* das, was „der sich bildende Mensch" aus sich zu machen sucht, ein Vorgang mehr als ein Besitz. Diesem Streben folgt er auch unabhängig von der Gesellschaft. Selbst Robinson gibt sich Rechenschaft über die vergehende Zeit; er pflegt seine Erinnerungen; er macht sich Gesetze/Regeln; er beobachtet und erklärt die Natur; er liest, dichtet, singt – und vervollkommnet sich darin; er bildet Vorstellungen aus – Hoffnungen auf Rettung und einen „Sinn" für den Fall, dass diese ausbleibt. Das ist die *persönliche Bildung,* die, wie man sieht, stark von der Kultur bestimmt wird, in der einer aufgewachsen ist, die aber auch ohne sie Geltung hat.

Bildung ist *zweitens* das, was den Menschen befähigt, in seiner geschichtlichen Welt, im *état civil,* zu überleben: Das Wissen und die Fertigkeiten, die Einstellungen und Verhaltensweisen, die ihm ermöglichen, sich in der von seinesgleichen ausgefüllten Welt zu orientieren und in der arbeitsteiligen Gesellschaft zu überleben. Das ist die *praktische Bildung.*

Bildung ist *drittens* das, was der Gemeinschaft erlaubt, gesittet und friedlich, in Freiheit und mit einem Anspruch auf Glück zu bestehen: Sie richtet den Blick des Einzelnen auf das Gemeinwohl, auf die Existenz, Kenntnis und Einhaltung von Rechten und Pflichten, auf die Verteidigung der Freiheit und die Achtung für Ordnung und Anstand. Sie ist für die richtige Balance in der Gesellschaft zuständig. Sie hält zur Prüfung der Ziele, der Mittel und ihrer beider Verhältnisses an. Sie befähigt zur Entscheidung angesichts von Macht und begrenzten Ressourcen in begrenzter Zeit. Das ist die *politische Bildung.*

Alle drei Bildungsaufgaben haben wir der Schule übertragen. Keine darf der anderen geopfert werden. Angesichts der Entwicklungen in der Weltwirtschaft, auf dem Arbeitsmarkt, in der Technologie liegt es nahe, die unmittelbar verwertbaren Ergebnisse von Bildung, die *marketable skills,* besonders zu fördern. Der Bildungsplan 2004 der Landesregierung muss auf der Gleich-

gewichtigkeit aller drei Aufträge bestehen – der Ausbildung der Gesamtpersönlichkeit der Schülerinnen und Schüler, der Überlebensfähigkeit der Gesellschaft und der Übung der jungen Menschen in der Rolle des Bürgers unserer Republik, des entstehenden Europa, der zukünftigen Weltgemeinschaft. Der Schule freilich fällt es nicht leicht, sie in Einklang und Gleichgewicht zu halten. Es gibt – meist durch äußere Umstände und Entwicklungen begünstigt – mal ein Übergewicht der einen, mal der anderen Aufgabe. Dann müssen die Verantwortlichen korrigierend eingreifen und die Ausgeglichenheit wiederherstellen.

2. Den Maßstab für ihr Handeln finden sie in der Verfassung des Landes Baden-Württemberg und im Schulgesetz des Landes, die auf der freiheitlich-demokratischen Grundordnung der Bundesrepublik beruhen.

3. In ihnen ist das Verhältnis von „Erziehungsanspruch" der Eltern und „Bildungsanspruch" der öffentlichen Schule behutsam geregelt. Die letztere ist ein Lernfeld für die Beziehungen der jungen Menschen untereinander und zwischen ihnen und Personen aus anderen Kulturen, mit anderen Biografien, Wertvorstellungen, Lern- und Denkgewohnheiten – mit anderen Stärken und Schwächen, Erwartungen und Erschwernissen. Die Schule hat darum immer auch einen Erziehungsauftrag, so wie das Elternhaus selbstverständlich nicht aufhört, an der Bildung der Schülerinnen und Schüler mitzuwirken. Der Auftrag der öffentlichen Schule verpflichtet diese zu enger und einvernehmlicher Zusammenarbeit mit den Eltern und legt eine sachliche Kooperation mit außerschulischen Partnern (Kommunen, Kirchen, Betrieben, Vereinen, Kultureinrichtungen) nahe.

4. Die Schule und die sie anleitenden Pläne haben über die drei genannten Formen der Bildung hinaus psychische, soziale und wirtschaftliche Wirkungen. Kein Kind kommt ohne jegliche Prägung in die Schule: Jungen und Mädchen, Einzelkinder und Geschwisterkinder, Kinder aus behütendem und begütertem Elternhaus und Kinder aus unordentlichen und benachteiligten Verhältnissen. Jeder junge Mensch hat ein Recht auf Erziehung und Bildung. Die öffentliche Schule schuldet ihm jede zur Erfüllung dieses Rechts nötige Hilfe – unabhängig von Herkunft, Geschlecht, wirtschaftlicher Lage und unter ausdrücklicher Berücksichtigung seiner besonderen Begabung. Kein Kind darf fallengelassen werden. Kein Schüler, keine Schülerin sollte die Schule verlassen, ohne wenigstens die „Ausbildungsfähigkeit" erreicht zu haben. Diese wird vor allem in dem der Hauptschule gewidmeten Teil des Bildungsplans 2004 gründlich neu bedacht. Die Durchlässigkeit der Schularten füreinander dient der Erprobung anderer Wege für den Einzelnen, der pädagogischen Nutzung gegebener Vielfalt, der Korrektur verfehlter Entscheidungen. Die Schule ist zu angemessener Förderung und Motivation auf allen Stufen und in allen Schularten verpflichtet.

5. Die Landesverfassung und das Schulgesetz erteilen den Schulen den Auftrag: „... die Kinder auf der Grundlage christlicher und abendländischer Bildungs- und Kulturwerte" zu erziehen. Diese wiederum gebieten christliche Toleranz und die Achtung der Würde und Überzeugung anderer; die Schulen sind offen für Schülerinnen und Schüler anderer Kulturen; sie bemühen sich, die Einwanderer in unser Land zu integrieren.

ZIELE, DIE DIE SCHÜLERINNEN UND SCHÜLER ERREICHEN SOLLEN

Die Aufstellung der von den Schülerinnen und Schülern zu erreichenden Ziele ist eine notwendige, befriedigende, geläufige und darum oft ausufernde Übung von Bildungsplanern. Wirksam wird eine solche Liste durch drei Eigenschaften: Sie muss knapp sein und Profil zeigen; die Ziele müssen dem Auftrag der Schule entsprechen; die Ziele müssen mit den der Schule zu Gebote stehenden Mitteln und Verfahren erreichbar sein.
In dieser Einführung kann die dritte Bemühung nur angedeutet werden; die Ausführung bleibt dem Bildungsplan 2004 selbst in seinen einzelnen Teilen vorbehalten.
Diese Einführung nimmt eine einfache, ohne Expertenwissen verständliche Einteilung der Erwartungen vor – in (a) Einstellungen, (b) Fähigkeiten und (c) Kenntnisse.

(a) Einstellungen

Die erstrebten, von der Schule zu fördernden Einstellungen umfassen Haltungen, Bereitschaften, Hemmungen, Gewohnheiten, Überzeugungen, Gewissheiten und Zweifel; sie werden gestützt und erhellt durch Vorstellungen – vom Menschen, von der Gemeinschaft, von Lebensaufgaben und Lebenssinn, von Befriedigung und Glück, von Frieden und Gerechtigkeit, von Schuld und Vergebung, von Geschichtlichkeit und Natur, von Gesundheit, Schönheit, Endlichkeit, Schicksal, von Gott. Solche Einstellungen sind nur sehr begrenzt lehrbar (und was „lehrbar" ist, fällt bei den „Kenntnissen" an). Sie sind nicht auf bestimmte Veranstaltungen, zum Beispiel Unterrichtsfächer, der Schule beschränkt. Sie sind nicht abprüfbar, nicht irgendwann als „erreicht" abzubuchen wie die „Kompetenz" Autofahren oder die „Kompetenz" freie Rede. Sie sind darum jedoch einer systematischen Pflege, Übung, Bewusstmachung keineswegs entzogen.

Man hat vor zwanzig Jahren in empirischen Untersuchungen gezeigt, in welchem Maß eine Schule für ihr „Ethos“ aufkommen kann und in welchem Maß dies dem Wohlbefinden und der Leistungsfähigkeit des Einzelnen, der Schulgemeinschaft und ihrem Klima förderlich ist. An den Gewinn zu erinnern, den die Gesellschaft von bestimmten Einstellungen ihrer gegenwärtigen und künftigen Bürgerinnen und Bürger hat, ist der Sinn der folgenden Liste. Sie verknüpft bestimmte Einstellungen deutlich mit dem „Auftrag der Schule“ in einer Welt, in der das Schwinden der „Kohäsionskräfte der Gesellschaft“ beklagt wird.
Die aufgeführten Einstellungen sind sämtlich dem Bildungsplan 2004 selbst entnommen. Diesem zufolge bemüht sich jede Schule, ihren Schülerinnen und Schülern durch das Verhalten der Erwachsenen; durch freundliche und geduldige Ermutigung; durch öffentliche Belobigung und individuelle Belohnung; durch Gewährung von Spielraum, Mitwirkung, geeigneten Herausforderungen; durch Bereitstellung von Bewährungsmöglichkeiten, Aufgaben und sinnvollen Ordnungen die folgenden zehn prägenden Erfahrungen zu geben:

1. Schülerinnen und Schüler gewinnen Lebenszuversicht, überwinden mitgebrachte Ängste, haben Freude am Lernen, an *trial and error;* sie entfalten ihre Neugier und lenken sie in befriedigende Bahnen, erwerben die Bereitschaft, immer weiter zu lernen.

2. Schülerinnen und Schüler gewinnen nicht weniger Freude am Bewahren und Schützen gefährdeter Güter der Natur, des Kleinen, Schwächeren, Verletzlichen, der vorgefundenen guten Ordnung, der ihnen selbst gewährten Freundlichkeit, Sicherheit und Rechte.

3. Schülerinnen und Schüler erfreuen sich der Verlässlichkeit anderer und bringen diese darum selber auf; sie übernehmen ihren Part in der arbeitsteiligen Welt; sie verbinden damit die Befriedigung, gebraucht zu werden; ihre Leistungsbereitschaft steigert sich mit der Wahrnehmung guter Leistung.

4. Schülerinnen und Schüler entwickeln erst ein Gefühl, dann eine Pflicht für die Gestaltung und Verbesserung der gemeinsamen Lebensverhältnisse, für deren Voraussetzungen und Ziele; sie wollen nun aktiv am Leben erst der kleineren, dann der großen Gemeinschaft teilnehmen; sie stellen sich der Verantwortung für ihr Handeln.

5. Schülerinnen und Schüler lernen, dass sie dazu Überzeugungen, Wertvorstellungen, Maßstäbe brauchen, dass ihnen zusteht, Kritik zu üben, und dass sie Konflikte wagen müssen; sie entwickeln Gelassenheit und Leidenschaft im öffentlichen Streit; sie erfahren, dass es lohnt, „durchzuhalten“ – sie lernen, wann es gut ist, nachzugeben; sie erkennen die der Demokratie zugrunde liegenden schwierigen, aber heilsamen Prinzipien; sie erkennen die Not von Randgruppen, beziehen sie ein, geben ihnen Hilfe.

6. Schülerinnen und Schüler lernen, der Gewalt zu entsagen – der physischen wie der psychischen; sie nehmen die friedens- und sicherheitsgebende Funktion des Rechtes und des staatlichen Gewaltmonopols wahr; sie erfahren die Notwendigkeit und außerordentliche Wirksamkeit der Zivilcourage – oder die Scham darüber, dass sie sie nicht aufgebracht haben.

7. Schülerinnen und Schüler gewinnen ein klares Verhältnis zum eigenen und zum anderen Geschlecht, zu den biologischen und seelischen Funktionen der Geschlechtlichkeit, zu Freundschaft und Familie, zu den Lebensphasen, zu den Alten und deren Eigenarten, zu den ganz Jungen, die sie selbst eben noch waren; sie lernen den Unterschied zwischen privatem und öffentlichem Leben und wie man das erstere abschirmt; sie erfahren ihre „Identität“, indem sie sich entscheiden; sie erfahren auch, dass die Stärke ihrer Entscheidung in der Wahrhaftigkeit der Begründung liegt: Ohne sie ist Ich-Stärke eher eine Schwäche.

8. Schülerinnen und Schüler lernen genießen: Ruhe, Bewegung, Spiel, Schönheit, Natur, Kunst; sie lernen, wie man Genuss dosiert und verfeinert.

9. Schülerinnen und Schüler weiten ihren Blick über die Nachbarschaft, die Stadt, die Republik hinaus zu Nachbarländern, zu Europa, zur Welt – sie gewinnen mit der weltbürgerlichen Freiheit einen Sinn für die Besonderheit ihres eigenen Volkes, ihrer eigenen Sprache, ihres eigenen Landes.

10. Schülerinnen und Schüler lernen, sich „letzten Fragen" zu öffnen – sie entscheiden sich zwischen Aufklärung und Glaube oder für eine Verbindung von beidem.

Einstellungen gibt es nicht „absolut". Sie sind immer von Fähigkeiten abhängig und mit Sachverständnis verbunden, wenn sie wirksam sein sollen. Sie dürfen diesen aber nicht nachgestellt oder geopfert werden, nur weil sie sich nicht in gleicher Weise „operationalisieren" lassen. Sie stehen darum hier an erster Stelle.

(b) Fähigkeiten

Das Wort „Fähigkeiten" dient in der Pädagogik von alters her der begrifflichen Abgrenzung von diesen zu „Kenntnissen" und zu „Einstellungen". Das Wort macht etwas benennbar, was nicht in oder hinter den anderen Forderungen verschwinden soll. In der Praxis aber sind die in der Schule angestrebten Fähigkeiten von bestimmten Sachverhalten wie von bestimmten seelischen Dispositionen nicht zu trennen. Die klare begriffliche Trennung hat den Vorteil, dass die Zusammenfügung ebenso klar vorgenommen werden kann.

Das Wort „Kompetenz" hat man einem internationalen Trend folgend auch in Deutschland eingeführt, gerade um die begriffliche Unterscheidung aufzuheben. Die Kompetenz „Lesefähigkeit" beispielsweise soll erweitert werden: um Lesebereitschaft, Lesegewohnheit, Freude am Lesen, den Willen zur „Entzifferung" der schriftlichen Botschaft, ein Bewusstsein von der allgemeinen Wichtigkeit des Vorgangs einerseits und eine „sachliche" Vertrautheit mit den Textsorten, Darstellungs- und Wirkungsabsichten, Verdichtungs-, Verschlüsselungs-, Verfremdungstechniken, die der Schreiber verwendet, und nicht zuletzt um die Kenntnis der Hilfsmittel, die dafür zur Verfügung stehen, andererseits.

Der Vorteil des Kompetenzbegriffs liegt in der kategorischen Entfernung von hier bloßer Stoffhuberei und da Gesinnungspflege. Er erlaubt bildungslaufbahn- oder curriculumunabhängige Vergleiche; er bringt die Schularbeit den Lebensaufgaben näher, die in der Tat weder der Einteilung in die drei Qualifikationskategorien noch gar in die Fächer oder Kenntnisgebiete folgen.

Der Bildungsplan 2004 entscheidet sich nicht für das eine, gegen das andere Modell; er beschreitet beide Wege: Er benennt die Kompetenzen, über deren Bezeichnung sich Einigkeit abzeichnet,

- personale Kompetenz,
- Sozialkompetenz,
- Methodenkompetenz,
- Fach- (oder Sach-)Kompetenz,

enthält sich aber einer Festlegung der Bestandteile und ihrer Gewichtung.

Wieder begnügt sich diese Einführung mit zehn Beispielen aus der Fülle der im Bildungsplan 2004 postulierten Fähigkeiten.

1. Die Schülerinnen und Schüler erwerben im Unterricht die Fähigkeit sowohl allgemeiner wie gezielter Aufmerksamkeit; Beobachten und Zuhören werden bewusst geübt und in den Dienst von Erkenntnisgewinn genommen; die Schülerinnen und Schüler lernen zwischen Beobachtung und Bewertung zu

unterscheiden; sie verstehen das Prinzip der „Objektivierung“ und lernen beispielhafte Mittel dieses Verfahrens kennen; sie nehmen den Unterschied zwischen „science an Sachen“ und „science an Lebewesen“ wahr; deduktive und induktive Vorgehensweisen werden verglichen; sie lernen, Sachverhalte zu recherchieren, Beobachtungen zu protokollieren, unter verschiedenen Beobachtungs-Gesichtspunkten zu wählen, ihre Erkundungen zeitlich und sachlich zu planen.

2. Die Schülerinnen und Schüler werden im Unterricht durch geeignete Fragen zum Denken angeleitet; erstrebt wird die Fähigkeit, neben gleichsam alltagssprachlichen Denken aus gegebenem Anlass begrifflich zu denken. Definitionen, Folgerungen, Begriffsabgleichungen begleiten die Aufnahme und Prüfung von Sachverhalten.

3. Die Fähigkeit, über das mechanische Lesen hinaus, Texten unterschiedlicher Länge und Machart den in ihnen gemeinten Sinn zu entnehmen, kann durch vielerlei Techniken erleichtert werden, geht aber in diesen nicht auf. „Mit dem Bleistift lesen“ erzwingt eine Unterscheidung zwischen Wichtigem und Beiläufigem, garantiert aber nicht, dass man sie richtig trifft. Die Lesefähigkeit wird darum ständig durch Lese-Erörterung zu begleiten und zu steigern sein. Exzerpieren, Protokollieren, Zusammenfassen, Kontrollfragen, die man sich selbst stellt, das „visuelle Gedächtnis“ werden routinemäßig geübt.

4. Redefähigkeit ist im Zeitalter von Mitsprache und Demokratie, aber auch angesichts der verfügbaren technischen Mittel von nicht geringerer Bedeutung als die Lesefähigkeit. Die Schülerinnen und Schüler erfahren im Unterricht, was wirksame und verständliche Rede ist; der Diskurs erfährt eine geeignete Übung durch das organisierte Streitgespräch (debating). Auch die eigene Person, nicht nur der Streitgegenstand gewinnt durch die Darstellungsfähigkeit; die Ordnung der Gedanken und Empfindungen im Gespräch wie in der schriftlichen Aufzeichnung dürften von wenigen Bildungsvorgängen in ihrer Wirkung übertroffen werden.

5. Schülerinnen und Schüler erwerben fremde Sprachen noch immer im Wesentlichen in der Schule. Sie erlernen Fremdsprachen umso leichter, je früher sie damit beginnen können. Deshalb sieht der Bildungsplan 2004 das Erlernen einer Fremdsprache ab Klasse 1 vor: Französisch als Sprache unserer Nachbarn am Oberrhein, Englisch in den anderen Landesteilen. Im Laufe ihrer Schullaufbahn ist für alle Schülerinnen und Schüler Englisch vorgesehen. Französisch hat auch in den weiterführenden Schulen eine herausragende Rolle. Griechisch und Latein können und sollten von Gymnasiasten in Formen gelernt werden, die ihnen dabei helfen, die Geschichte Europas, seine Denk- und Sprachformen zu entschlüsseln.

6. Die Fähigkeit, in gegebenen Sachverhalten die sie klärenden mathematischen Relationen zu erkennen, ist gewiss nicht ohne Kenntnisse der (reinen) Mathematik möglich. Gleichwohl gilt es in erster Linie, mit elementaren mathematischen Mitteln die Mathematisierung eines Problems vorzunehmen, durch die dieses verständlich und lösbar gemacht werden kann.

7. Im Zeitalter des Computers ist eine Beherrschung dieses Gerätes und ein sinnvoller Gebrauch des Internet-Zugangs unerlässlich. Neben dem Computer als Arbeitsmittel und dem Internet als Ressource bleiben Einrichtungen wie Bibliotheken, Videotheken, Museen und Sammlungen notwendige, insbesondere in der Schule und durch die Schule zugänglich zu machende Hilfsmittel. Die Schülerinnen und Schüler lernen, sich der Auskunftsmittel – vom Sachbuch und Nachschlagewerk bis zur CD und CD-ROM – geläufig zu bedienen.

8. Im Zeitalter zunehmender Mitspracherechte erwächst dem Einzelnen eine Mitsprachepflicht. Er muss dazu die im Abendland ausgebildeten Ordnungen und Verfahren kennen: Die Verfahrensregeln *(parliamentary procedure)* sollten an allgemein bildenden Schulen aus jedem geeigneten Anlass geübt und dadurch in ihrer Funktionsweise verstanden werden.

9. In der arbeitsteiligen Welt haben Kooperationsfähigkeit und die Möglichkeit, sich anderen verständlich zu machen, die Bereitschaft, sich ihren Fragen auszusetzen, hohen Rang.

10. Alle Schülerinnen und Schüler müssen rechtzeitig auf die Bewältigung ihres zukünftigen Lebens zu blicken lernen – sich Lebensentwürfe machen und ihre Ausstattung dafür selber zu planen lernen.

(c) Kenntnisse

Die insbesondere seit Pisa erkennbare und befolgte Absicht der Bildungsplaner, von den Wissenspyramiden wegzukommen, die die alten Lehrpläne kennzeichneten, nimmt eine frühere Bemühung wieder auf, die volkstümlich „Entrümpelung" hieß und bildungstheoretisch mit der „Exemplarizität" des jeweils zu lernenden Gegenstandes begründet wurde.

Auch unter diesem Gesichtspunkt verhält sich der Bildungsplan 2004 „konservativ". Die Kenntnisse, die in ihm als „verbindlich" erklärt werden, bleiben weitgehend den Fächern und, wo es sie inzwischen gibt, den Fächergruppen zugeordnet. Vor allem aber kann hier nur in großer Allgemeinheit von „schulartübergreifenden" Standards gesprochen werden. Ein gegliedertes Schulsystem, das die Wissensgegenstände (den so genannten „Inhalt" der Bildung) nicht gliedert, würde sich selbst widerlegen.

Wieder versucht diese Einführung eine Vorstellung davon zu vermitteln, was durch strenge Konzentration, durch die Einführung von Kerncurricula und Kontingentstundentafeln und durch einen Kanon „zentraler Themen" erreicht werden kann: größere Übersicht, ein Sinn für die Einheit der Bildung, eine Vereinfachung des Gesamtplans, Spielräume für individuelle Schulcurricula.

Und wiederum beschränkt sich diese Einführung auf zehn Gebiets- oder Themenangaben, die die Grundtendenz des Bildungsplans 2004 veranschaulichen: Konzentration, Konsistenz, Kontur.

1. Der Mensch, seine Anlagen und seine Kultur. Die hier zu erwerbenden Kenntnisse reichen von anthropologischen Grunddaten, geographischen und klimatischen Lebensbedingungen bis zu den in Mythen, Geschichtsdeutungen und Kunstwerken der Kulturen gefassten „Menschenbildern": Schöpfungsgeschichte, Prometheus-Sage, Evolutionstheorie, vorgeschichtliche und geschichtliche Befunde, homo sapiens / homo faber / homo psychologicus.

2. Welt, Zeit, Gesellschaft. Die Schülerinnen und Schüler erwerben Kenntnisse von den wichtigsten Machtgebilden (Herrschaftsformen), Lebensgemeinschaften, Bewegungen, Entwicklungen, Revolutionen, von Abhängigkeit und Spontanität menschlichen Handelns, von Konflikten und Katastrophen an ausgewählten geeigneten Beispielen aus Vergangenheit und Gegenwart; daneben und dazu wird ein Epochen- und Daten-Gerüst aufgebaut.

3. Geschichtlichkeit, Geschichtsbilder, geschichtliche Gestalten. Innerhalb dieses Gerüsts gewinnen die Schülerinnen und Schüler deutliche Vorstellungen von den folgenden ausgewählten Vorgängen oder Themen: von der Antike, vom Mittelalter, vom Ausgreifen Europas auf die Welt, von der Aufklärung (Französische Revolution), vom I. und II. Weltkrieg und der Hitler-Zeit, von der Nachkriegsgeschichte; sie kennen die Taten und Wirksamkeit einzelner Personen in der Geschichte.

4. Materie, Natur, Technik. Die Schülerinnen und Schüler erarbeiten elementare Kenntnisse über die uns umgebende und tragende physische Welt, über lebende Organismen und ihre Entwicklung, über chemische Substanzen und ihre Verbindungen, über die klassischen Gebiete und wesentlichen Gesetze der Physik – und über die an ihnen entwickelte „science", deren Segnungen und andere Folgen, über „Werkzeug" und Technik, über deren typische Verfahren, ihre ökonomischen und ökologischen Wirkungen je an geeigneten Beispielen.

5. Wirtschaft, Arbeit, Gesundheit. Die Schülerinnen und Schüler bilden sich einfache Vorstellungen von den gesellschaftlichen Mittelsystemen. Dass der Bürger nicht ausreichend weiß, wie die ineinander greifenden Faktoren Arbeit, Rohstoff, Kapital, Produktivität, Handel, Verkehr, soziale Auffangnetze, Gesundheitsversorgung funktionieren, macht einen Teil der Krisen aus, die die statischen Republiken im gegenwärtigen Wandel der Verhältnisse durchmachen. Anschauliche Modelle der elementaren Abhängigkeiten können für ein größeres Maß an Klarheit und Entscheidungssicherheit sorgen.

6. Mathematik als Geisteswissenschaft. Über die „Fähigkeit" der Mathematisierung hinaus verfügen die Schülerinnen und Schüler über rudimentäre Kenntnisse der euklidischen Geometrie und der Algebra, also über die mathematischen Grundfunktionen: Zählen, Messen, Relationieren, Strukturieren (in Raum und Zeit), Algorithmisieren. Sie verstehen, was es heißt: „eine gegebene Größe in ein Verhältnis zu einer anderen setzen" und was in der Statistik, im Kalkül, in der Wahrscheinlichkeitsrechnung geschieht. Sie verfügen über mathematische Lösungsmodelle – wiederum elementarer Art – und über ein Repertoire an mathematischen Darstellungsformen: Tabellen, Diagramme, Koordinatensysteme – eine Mischung aus Fähigkeit und Kenntnis. Schließlich: Die Schülerinnen und Schüler haben Mathematik als ein ästhetisches Ereignis erfahren.

7. Sprache und Sprachen. Auch hierbei handelt es sich um ein Gemisch aus Fähigkeiten und Kenntnissen. Eindeutig zu den Kenntnissen zählt der Aufbau des indogermanischen Satzes und damit einhergehend die Beherrschung der gemeinsamen grammatischen Nomenklatur. Die Schülerinnen und Schüler verbinden ihre Sprachkenntnisse mit Vorstellungen von der Lebensweise des Volkes, das die jeweilige Sprache spricht. Sie verfügen über die Regeln der jeweiligen Rechtschreibung.

8. Die Literatur. Die Schülerinnen und Schüler kennen die wichtigsten zum Verständnis der Literaturgattungen und -epochen notwendigen Einteilungen. Als Ergebnis eines gelungenen Literaturunterrichts wird erwartet: Jede Schülerin, jeder Schüler kann zwei Gedichte nach Wahl auswendig und kann die Wahl begründen; jede Schülerin, jeder Schüler hat drei erzählende Werke ganz gelesen, kann ihren Inhalt wiedergeben und erklären, warum sie ihr/ihm wichtig sind; jede Schülerin, jeder Schüler hat zwei Theaterstücke gesehen, zwei weitere gelesen und möglichst an der Aufführung eines Stückes mitgewirkt – und weiß, welche Wirkung es tun will/wollte, jetzt tut oder verfehlt. Der Umgang mit ausgewählten Werken hat die Schülerinnen und Schüler zu neugierigen, genauen, der historischen Schwierigkeiten bewussten Leserinnen und Lesern gemacht, zu Lesern, die sich fragen, wie es zu diesen wunderbaren Wirkungen kommt, wie sich Dichtung zu Wirklichkeit verhält, welche Möglichkeiten sie selber hätten, so etwas zu schreiben, und die mit dieser Gewohnheit ihr Leben lang fortfahren. Insofern gehört dies eher zu den „Einstellungen" als zu den „Kenntnissen". – Wer an einem Lesekanon festhält, wird dies am besten mit dem Argument tun, eine Kultur erhalte sich mit gemeinsamen „Geschichten" auch eine gemeinsame Verständigungsmöglichkeit. Nicht „gelesen haben", sondern „gern und mit Gewinn lesen" ist das Ziel.

9. Die Künste. Die „Kenntnis" der Künste besteht in erster Linie im Anhören und Betrachten der Werke – mit Muße, konzentriert und wiederholt. Dann erst wollen sie verstanden sein. Kunst- und Musikgeschichte und -theorie können dabei behilflich sein, wenn sie zugleich ein Stück Kulturgeschichte sind.

10. Alle Schülerinnen und Schüler sollten eine Vorstellung von der Vielfalt der Religionen in der Welt haben. Die Unterweisung im Christentum in Form der evangelischen und katholischen Religionslehre ist den Schulen Baden-Württembergs durch das Gesetz vorgeschrieben – für die, die dies in Anspruch nehmen. Diese sollten darüber hinaus Kenntnis von ihren Unterschieden untereinander und zu den anderen Religionen haben. Wer keiner Religionsgemeinschaft angehört, sollte dennoch am Religionsunterricht teilnehmen dürfen. Alle Schülerinnen und Schüler sollten in die Grundfragen und -begriffe der Ethik eingeführt werden. Alle Schülerinnen und Schüler sollten zur Klärung ihres alltäglichen Philosophierens einige große Philosophen-Gestalten und deren Lehre kennen.

DIDAKTISCHE UND METHODISCHE PRINZIPIEN

Die Entwicklung der Schule weg von der Belehrungsanstalt, hin zu einer pädagogischen Einrichtung vollzieht sich in Deutschland seit Jahrzehnten in den einzelnen Schulgemeinden, Schulen, Unterrichtsfächern und Unterrichtsarten („on the classroom level"). Der Bildungsplan 2004 zieht in vieler Hinsicht nur nach. Mit ihm und insbesondere mit der Formulierung bestimmter didaktischer und methodischer Prinzipien (nicht Methoden!) unterstützt die Schulverwaltung die Lehrerschaft; sie leitet nicht so sehr zu bestimmten Vorgehensweisen an, sie gibt diesen vielmehr zustimmend Ausdruck. Sie warnt gleichzeitig vor möglichen Fehlentwicklungen, die mit anderen wichtigen Entwicklungen einhergehen könnten – mit der Einführung neuer Medien in den Unterricht, mit der systematischen Überprüfung (Evaluation) durch standardisierte Tests, mit einer vielfach nahegelegten und mit den heutigen technischen Mitteln möglichen radikalen Individualisierung und Materialisierung des Lernens (Arbeitsbögen ersetzen den gemeinsamen Unterricht). Die Ablösung der Belehrung (das Abarbeiten von Stoffplänen) durch eine Anstiftung zum selbstständigen Erwerb von Fähigkeiten, Kenntnissen und Verhaltensdispositionen vollzieht sich vermutlich eher aufgrund der hier angesprochenen Prinzipien als aufgrund der bisher dargestellten veränderten Lernziele und Kompetenzlisten.

Wiederum folgen hier beispielhaft – also nicht auf Vollzähligkeit hin bedachte – didaktische und Verfahrensprinzipien.

1. Das Lernen ist in einem doppelten Sinn handlungsorientiert, nämlich erstens auf seine spätere Anwendbarkeit – im Alltag und im Beruf – hin ausgelegt: Man weiß oder kennt eine Angelegenheit nicht nur, man kann in ihr handeln; das Lernen vollzieht sich zweitens zu einem großen Teil durch Handeln; im Bildungsplan 2004 kommt darum häufig der Ausdruck „im Handlungsvollzug" vor; in der pädagogischen Theorie heißt dies „learning by doing" (Lernen durch Handeln).

2. Die Lernhandlung erlaubt nicht nur, sie verlangt Selbstständigkeit, Eigenverantwortung, Selbstkontrolle (selfdirection). Ein Logbuch (das ist die Protokollierung des täglichen Lernens), die bewusste Mitteilung des Gelernten an andere (Präsentation), die Sammlung der eigenen Leistungen (im Portfolio) leisten mehr für das Qualitätsbewusstsein als Lehrerurteil und Zensur. Die Verantwortung für das eigene Lernen findet eine wichtige Ergänzung und Anregung in der Verantwortung für das gemeinsame (von der Lehrkraft veranstaltete) Lernen. Die Schülerinnen und Schüler werden an der Planung des Unterrichtsverlaufs, an der Wahl der Anlässe und Gegenstände beteiligt, was wiederum die Teilnahme am Unterricht verstärkt.

3. Das Lernen – wie auch das Lehren – soll für die eigene Person bedeutsam und bewegend sein. Es nimmt darum von der Frage, dem Verstehens- oder Lebensproblem der Schülerinnen und Schüler seinen Ausgang. „Aktiv-entdeckend" heißt es im Bildungsplan 2004. Auch der Lehrer, die Lehrerin lehrt nicht „Fertiges" und „Endgültiges", sondern etwas, das ihn oder sie noch umtreibt und an dem er oder sie vorlebt, wie man zu einer Lösung kommt. Was ein Lehrer, eine Lehrerin lehrt, sollte ihm oder ihr immer wichtig sein.

4. Ermutigung, die Vermeidung von unnötigem Versagen (Demotivation), die lustvolle Herausforderung sind hohe Künste und können nicht in einem Bildungsplan verordnet werden. Ein hier einschlägiges Prinzip aber ist die von der Klärung der Sachverhalte ausgehende Lernzuversicht. Die wichtigste Leistung der Lehrenden ist, Verstehen zu ermöglichen.

5. Wenn Lehrende einen hohen Leistungsbegriff haben und originelle, abweichende, nicht geplante Lösungen anerkennen (und diese zur geplanten Lösung in Beziehung zu setzen vermögen), ist das Ausweis ihrer Sachkenntnis mehr als ihrer Lässlichkeit.

6. Kinder lernen viel voneinander, jüngere vor allem von älteren (cross-age teaching), aber auch ältere, indem sie jüngeren

etwas erklären; vollends aber lernen sie gemeinsam. Kooperation ist, wie das Handeln und die Selbstständigkeit, nicht nur Ziel, sondern Mittel des Lernens.

7. Wie der Zusammenhang des Lernens unter den Schülerinnen und Schülern ansteckend ist, so ist es auch der Zusammenhang der Gegenstände und Kompetenzen. Eine Kompetenz im Sinne des Bildungsplans ist immer mit einer anderen Kompetenz verbunden. Fachkompetenz tritt „nie isoliert" auf, heißt es. Soziale Kompetenzen sind mit personalen, Fachkompetenzen mit methodischen Kompetenzen verschränkt und gemeinsam zu entwickeln.

8. Der Erfolg des veranstalteten Lernens ist stark von einer sinnvollen Rhythmisierung abhängig – einem Wechsel von Konzentration und Gelassenheit, von Aufnahme und Wiedergabe, von körperlich-sinnlicher und geistiger Beanspruchung.

9. Das Lernen wird durch „Lernstrategien" erleichtert; diese sind jeweils in der Lernsituation und am geeigneten Gegenstand bewusst zu machen und zu üben. Die Lehrenden sorgen für geeignete Anlässe zur Wiederholung, Abwandlung, „Transfer" des Gelernten – neben der Übung in den oben auf Seite 13 aufgezählten Techniken. Den Lehrenden muss das Prinzip des Spiralcurriculums (Steigerung und Erweiterung wiederkehrender Anforderungen) geläufig sein – den Lernenden nicht unbedingt.

10. Außerschulische Erfahrungen und außerschulischer Einsatz tragen in hohem Maß zur Lernmotivation bei, sind darum systematisch einzubeziehen und bei der Bewertung hoch zu veranschlagen. „Aus der Schule gehen – etwas in die Schule mitbringen", diese Maxime steigert die Wirksamkeit der Schule und ihrer Gegenstände.

MASSNAHMEN UND EINRICHTUNGEN ZUR SICHERUNG DES AUFTRAGS, DER BILDUNGSZIELE, DER DIDAKTISCHEN UND METHODISCHEN PRINZIPIEN

Mit Maßnahmen sind dienstbare einzelne Vorkehrungen gemeint, die die Struktur der Schule unberührt lassen. Sie werden hier nicht um ihrer selbst willen dargestellt. Wichtig sind sie gleichwohl; ihre Tragweite dürfte sogar die Strukturveränderungen übertreffen, die in der Vergangenheit so heiß umkämpft worden sind.

Der Bildungsplan im eigentlichen Sinn wird durch diese Maßnahmen in sich dynamisiert, insbesondere durch die den Einzelschulen auferlegte Aufgabe, eigene Schulcurricula aufzustellen. Auch hier bringt die Einführung nur eine Auswahl der im Bildungsplan 2004 aufgeführten Maßnahmen zur Anschauung, die für die Absichten des Planes charakteristisch sind.

1. Für die einzelnen Fächer der einzelnen Schulart werden Kerncurricula verbindlich vorgegeben. Sie nehmen zwei Drittel der Unterrichtszeit der Schülerinnen und Schüler in Anspruch. Der Sinn der Kerncurricula ist, erstens ein Maß der erwarteten Lern- und Unterrichtsleistungen zu definieren und damit zweitens den Freiraum für das schuleigene Curriculum zu sichern.

2. Die Schulcurricula sollen von den Schulen selbst erarbeitet werden. Aus diesem Planungsvorgang wie aus seiner selbstständigen Ausführung wird ein erhöhtes Interesse für und ein intensiver Einstand in die projektierte pädagogische Aufgabe erwartet. Die Schulcurricula werden durch bestimmte Leitgedanken (zur Bedeutung des jeweiligen Faches im jeweiligen Bildungsgang) geordnet. Die im Bildungsplan 2004 genannten Motive lauten „Erweiterung des Repertoires" und „Vertiefung/Intensivierung" des Umgangs mit bestimmten gewünschten, in den örtlichen Gegebenheiten angelegten Lernmöglichkeiten.

3. Der Bildungsplan stellt Leitfragen zu den einzelnen Leitaufträgen der Schulen:

Lernen und Arbeiten
- Welche Möglichkeiten eröffnet die Schule für eigenverantwortliches Lernen und Arbeiten?
- Wie werden wir der Rolle der Sprache (insbesondere der deutschen) in allen Unterrichtsfächern und Fächerverbünden gerecht?
- Mit welchen schulinternen Konzepten stärken wir die muttersprachlichen und fremdsprachlichen Kompetenzen der Schülerinnen und Schüler?
- Wie tragen wir der Vielsprachigkeit im Hinblick auf die Bedeutung der Herkunftssprachen der Schülerinnen und Schüler Rechnung?
- Wie unterstützen wir bilinguales Lernen und Arbeiten?
- Wie können leistungsstarke und leistungsschwache Schülerinnen und Schüler erkannt, beraten und differenziert gefördert werden?
- Wie wird das kreative künstlerische Potenzial (zum Beispiel durch Chor, Orchester, Theater) gefördert?
- Wie gestalten wir ein schulspezifisches Curriculum zur Entwicklung der Kompetenzen?

In Gemeinschaft leben
- Welche Vereinbarungen treffen wir, um die Beziehungen untereinander zu gestalten und Orientierung zu geben?
- Welche pädagogischen Möglichkeiten nutzen wir zur Lösung von Konflikten?
- Welche Hilfen bieten wir zur Bewältigung von Lebensproblemen unserer Schülerinnen und Schüler?
- Wie kann die schulische Gemeinschaft besonderen Lebensumständen von Schülerinnen und Schülern und unterschiedlichen Lebenswelten im schulischen Umfeld Rechnung tragen?
- Wie kann in der Schule erreicht werden, dass Mädchen und Jungen sich bei aller Verschiedenheit als gleichberechtigt und gleichwertig wahrnehmen, um zu einer geschlechtlichen Identität zu finden?

Demokratie lernen
- Welche Formen der Mitsprache und Mitgestaltung gibt es auf der Ebene der Klasse und der Schule?
- Wie fördern wir die Übernahme von Verantwortung und die Sprachfähigkeit so, dass Schülerinnen und Schüler an der Ordnung der gemeinsamen Angelegenheiten mitwirken können und wollen?
- Welche Unterstützung erhält die Schülermitverantwortung?
- Welche Anschauung geben wir von der politischen Demokratie „draußen“?

Mit Eltern und außerschulischen Partnern kooperieren
- Wie gestalten wir die Erfüllung des gemeinsamen Erziehungsauftrags mit den Eltern?
- Wie beteiligen wir Eltern und außerschulische Partner an der Entwicklung und Umsetzung unseres Schulkonzepts?
- Wie wird die außerschulische Jugendarbeit in den Unterricht/in die Schule integriert?

Zentrale Themen und Aufgaben der Schule
- Wie setzt die Schule die folgenden zentralen Themen altersgerecht um? Hier nur in zehn ausgewählten Beispielen vertreten:
  - Berufliche Orientierung und Arbeitswelt;
  - Dialog der Generationen;
  - Europa;
  - Geschlechtserziehung;
  - Gesundheitserziehung und Suchtprävention;
  - Konfliktbewältigung und Gewaltprävention;
  - Leseförderung;
  - Medienerziehung;
  - Umwelterziehung und Nachhaltigkeit;
  - Verbrauchererziehung und Freizeitgestaltung.

4. Die Schulen werden zu definierten Fördermaßnahmen und Stützangeboten für leistungsschwache oder benachteiligte Schülerinnen und Schüler angehalten und befähigt. Diese Arbeit wird in vielen Fällen vor allem durch ein Zusammenwirken mit außerschulischen Partnern ermöglicht.

5. Im Bildungsplan 2004 werden Fächerverbünde zum ersten Mal verbindlich eingeführt, zum Beispiel in der Hauptschule:
- Welt – Zeit – Gesellschaft;
- Materie – Natur – Technik;
- Wirtschaft – Arbeit – Gesundheit;
- Musik – Sport – Gestalten.

Diese Verbünde erlauben und verlangen ihrerseits eine andere Zeiteinteilung und eine größere Nähe ihrer Themen zum Leben.

6. Die Schulen werden nicht nur zentral und periodisch evaluiert, sie werden zur Selbstevaluation angehalten, befugt und befähigt. „Selbst- und Fremdevaluation bedingen einander und dienen einer empirisch gesicherten, zielgerichteten und systematischen Qualitätsentwicklung vor Ort." Die zentralen Prüfungen und „Vergleichsarbeiten" beziehen sich auf die Kerncurricula. In ihnen vor allem werden die Bildungsstandards wirksam.

7. An den Schulen Baden-Württembergs beginnt das Lernen einer Fremdsprache im ersten Schuljahr.

8. Ganztagsschulen werden in dem Maß entstehen, in dem die Gegebenheiten dies fordern oder zulassen. Die Entwicklung dahin wird begrüßt und gefördert, weil sie über den Unterricht hinaus ein Schulleben ermöglicht und erlaubt, pädagogischere Zeiteinteilungen vorzunehmen. Die Schulen können die damit verbundenen zeitlichen Spielräume auch für das Zusammenwirken mit außerschulischen Partnern und für besondere Lernprojekte in der Förderung benachteiligter und begabter Schülerinnen und Schüler nutzen. Aber auch ohne Ganztagsbetrieb kann die Schule – aufgrund der Kontingentstundentafeln und ihrer neuen Autonomie – zu anderen pädagogischeren Zeiteinteilungen kommen (siehe oben Seite 14).

9. Den alten Satz „Es wird gelernt, was geprüft wird" (oft ergänzt durch den Satz „und es wird so gelernt, wie geprüft wird") zitiert man gemeinhin, um die Ohnmacht der pädagogischen Absicht und der didaktischen Kunst zu bestätigen. Der bezeichnete Sachverhalt lässt sich auch zu deren Stärkung benutzen, indem man die Prüfungen bewusst so gestaltet, dass sie dem gewollten Lernvorgang entsprechen. Das Kultusministerium beobachtet mit Interesse Versuche, die mit der Abgleichung der Bildungspläne mit den Prüfungen beginnen und damit die allgemein geforderte so genannte „output-Steuerung" erst zu dem machen, was sie sein soll: eine Verbesserung des Unterrichts.

10. Sport, Spiel und Bewegung erfahren in allen Schulen eine über den Sportunterricht hinausgehende Förderung – in den Pausen, auf Exkursionen, im Zusammenwirken mit Sportvereinen. Ein an vielen Grundschulen eingeführtes Programm „Grundschule mit sport- und bewegungserzieherischem Schwerpunkt", das die Bewegungsfreude der Schülerinnen und Schüler weckt und stärkt, soll in den kommenden Jahren auf alle Grundschulen ausgedehnt werden.

Die in dieser Einführung gegebene Übersicht über die wichtigsten Absichten, Maßstäbe und Maßnahmen des Bildungsplans 2004 gilt für alle Schularten des Landes – Grundschule, Hauptschule, Realschule, Gymnasium. Dies legt eine Allgemeinheit und Offenheit der Darlegung nahe, die in den folgenden Einzelplänen von Präzisierungen und Festlegungen abgelöst werden. Die „Einführung" und die jeweilige „Ausführung" sollen als einander ergänzende Teile gelesen werden – eben als der eine Bildungsplan 2004.