BÜNDNIS 90
DIE GRÜNEN
Bundestagsfraktion

lang & schlüssig 14 25

JAN. 2001

Informations-
schrift

DATENSCHUTZ IM INTERNET

Impressum

Herausgeberin	Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin http: // www.gruene-fraktion.de
Verantwortlich	Arbeitskreis III Innen, Recht, Frauen und Jugend Grietje Bettin MdB Medienpolitische Sprecherin Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin Tel.: 030 – 227 7 50 52 Fax: 030 – 227 7 60 51 eMail: grietje.bettin@bundestag.de
Redaktion	Peter Schaar
Bezug	Bündnis 90/Die Grünen Bundestagsfraktion Info-Dienst Platz der Republik 1 11011 Berlin Fax: 030 / 227 56566 eMail: public@gruene-fraktion.de
Schutzgebühr	EUR 1,50
Redaktionsschluss	Januar 2001

Datenschutz im Internet

Eine Information der Bundestagsfraktion von Bündnis 90/Die Grünen

Inhalt

Datenschutz im Internet

Eine Information der Bundestagsfraktion von Bündnis 90/Die Grünen

Kaum ein Tag vergeht, an dem nicht neue Nutzungsmöglichkeiten elektronischer Dienste erfunden und der Öffentlichkeit präsentiert werden. Im Mittelpunkt dieser rasanten Entwicklung steht das Internet. Die auf seiner Basis entwickelten Dienste bringen für Wirtschaft und Verwaltung, aber auch für die Bürgerinnen und Bürger eine Vielzahl von Chancen mit sich. Bündnis 90/Die Grünen treten dafür ein, diese Entwicklung der Informationsgesellschaft aktiv zu gestalten. Von besonderer Bedeutung ist dabei die Gewährleistung des Datenschutzes, d.h. des Rechts auf *informationelle Selbstbestimmung* der Internet-Nutzerinnen und -Nutzer.

Das Internet als globale Datenbank

Wohl noch nie war es so einfach wie heute, an persönliche Daten zu kommen: Das Internet ist eine aus Millionen vernetzten Computern bestehende globale Datenbank, in der eine Vielzahl personenbezogener Daten zur Verfügung stehen. Bereits jetzt gibt es Agenturen, die sich auf persönliche Recherchen im Internet spezialisiert haben. Diese "Internet-Detekteien" beschaffen innerhalb weniger Stunden Anschriften, Familienstand, Telefonnummern, Daten zur Bankverbindung und zum Schuldenstand, Angaben über das Beschäftigungsverhältnis, Vorstrafen, Sozialversicherungs- und Führerscheinnummern und und und...

Wer irgendwann einmal im Internet etwas veröffentlicht hat, sei es eine eigene Homepage, einen Beitrag in einer *Newsgroup* oder in einem *Chatroom*, sollte sich nicht wundern, wenn diese Informationen auch noch Jahre später nachzuvollziehen und zu recherchieren sind. Wer eine eigene *Domain* auf seinen Namen registrieren lässt, muss hierfür nicht nur seine Anschrift, sondern auch seine Telefonnummer offenbaren. Diese Angaben werden von den Domain-Vergabeorganisationen gespeichert und sind weltweit abrufbar (http://www.denic.de; http://www.ripe.net).

Bereits jetzt stehen eine Vielzahl sehr leistungsfähiger *Suchmaschinen* zur Verfügung. Eine einfache Suche in AltaVista (http://www.altavista.com) oder in "deja.com" (http://www.deja.com) gibt erste Aufschlüsse darüber, was über eine Person bereits im Netz gespeichert ist. Kombiniert mit anderen Informationsquellen, z.B. einem elektronischen Telefonbuch auf CD-ROM, ergibt sich häufig schon ein recht aussagekräftiges Bild. Zumindest diese Informationen kann jeder erhalten, der Zugang zum Internet hat, also auch Vermieter, Nachbar oder Arbeitgeber.

Der Spruch „ich habe keine Geheimnisse" war noch nie so dumm wie heute!

Der gläserne Surfer

Auch das Surfen im *World Wide Web* (WWW oder kurz: Web) ist fast vollständig überwachbar: jeder Rechner im Netz hat eine eigene Kennung, die *IP-Nr.*; jede Ressource im Web besitzt eine eigene Adresse, die *URL* (Uniform Resource Locator). Durch Auswertung von *Nutzungsdaten* lässt sich nachvollziehen, wer wann auf welche Inhalte zugegriffen hat. Dies gilt auch für die Fälle, in denen die IP-Nummer dynamisch vergeben wird (bei der dynamischen Vergabe wird dem Surfer bei jeder Nutzung des Internet eine zufällig vergebene IP-Nummer des jeweiligen Anbieters zugewiesen). In diesen Fällen muss allerdings der *Zugangs-Provider* (der Anbieter des Internet-Zugangs) bei der Identifizierung des Nutzers mitwirken, denn er kennt ja die Namen und Anschriften seiner Kunden oder kann diese Informationen zumindest in Erfahrung bringen.

Auf vielen Rechnern werden *Logprotokolle* geführt, die jeden Zugriff registrieren. Durch die Auswertung der Logprotokolle können die Spuren im Netz zu *Nutzungsprofilen* verdichtet werden. In die Nutzungsprofile fließen darüber hinaus auch Daten aus anderen Quellen ein, z.B. Informationen, die bei der Registrierung von Diensten erhoben werden und auch Anfragen in "Suchmaschinen". Selbst das Abspielen von Videoclips oder Musikstücken, die aus dem Netz bezogen wurden, wird in den Nutzungsprofilen registriert. Derartige Nutzungsprofile verraten manches über die Verhaltensweisen und Interessen der einzelnen Nutzerinnen und Nutzer.

Aus Nutzungsprofilen lässt sich zum Beispiel ablesen, ob man sich für eine Sportart, ein Hobby oder für ein bestimmtes politisches Thema besonders interessiert. Nutzungsprofile geben unter anderem Auskunft darüber, ob man das Internet lieber morgens, abends oder nachts nutzt, welchen Computertyp und welches Betriebssystem man mit welchem Browser einsetzt, welche elektronisch angebotene Zeitung man bevorzugt und welchen Artikel man gelesen hat.

Es liegt auf der Hand, dass es für Nutzungsprofile eine ganze Reihe Interessenten gibt. Zu nennen sind in erster Linie Unternehmen, die Werbung im Internet betreiben. Wenn bekannt ist, dass sich ein Nutzer/eine Nutzerin besonders für einen bestimmten Sport interessiert, werden in die Web-Seiten gezielt solche "*Werbebanner*" eingeblendet, die etwas mit dieser Sportart zu tun haben. Aber auch für andere Unternehmen, z. B. die Hersteller von Sportartikeln, besteht ein brennendes kommerzielles Interesse an den Daten der Nutzer mit den entsprechenden Präferenzen, um diese Informationen für gezielte Kundenpflege (*CRM* - Customer Relations Management) zu verwenden.

Cookies und anderes Gebäck

Da viele Surfer nicht immer mit derselben IP-Nummer im Netz unterwegs sind, haben sich Unternehmen, die sich auf die Erstellung und Vermarktung von Nutzungsprofilen spezialisiert haben, etwas einfallen lassen: die *Cookies*. Dabei handelt es sich um kleine, unscheinbare Textdateien, die auf den Rechnern der Nutzerinnen und Nutzer gespeichert werden. Diese Cookies werden von den Anbietern ausgelesen und gestatten so eine Zusammenführung und Auswertung des Nutzungsverhaltens in großen Datenbanken.

Damit nicht genug: in jüngster Zeit werden verstärkt auch Methoden verdeckter Datenerhebung im Netz eingesetzt. Eine besondere Rolle spielen dabei *Web Bugs*. Dabei handelt es sich um versteckte *Links* zu anderen Anbietern. Während der Nutzer die Einblendung von Werbebannern zumindest noch erkennen kann, ist dies bei den Web Bugs anders. Auf Grund ihrer geringen Größe und der Verwendung von anderen Tarnmechanismen ist es für den Nutzer praktisch nicht möglich, zu erkennen, dass er zur Registrierung seines Nutzungsverhaltens an einen Drittanbieter weitergeleitet wird.

Die Firma DoubleClick, ein amerikanisches Unternehmen, das viele Millionen Profile von Internet-Nutzern gesammelt hatte, hat kürzlich eine Kreditauskunftei aufgekauft, die das Kaufverhalten der meisten amerikanischen Versandhauskunden auswertet. Offenbar versprach sich DoubleClick von der Zusammenführung der verschiedenen Datenbestände zusätzlichen Profit. Zum Glück ist dieses Vorhaben von der Internet-Gemeinde frühzeitig entdeckt worden und DoubleClick musste den Rückzug antreten. Leider gibt es nicht immer solch ein Happy End...

Kein bisschen vertraulich

Informationen, die im Internet übertragen werden, sind alles andere als vertraulich. Jedes Datenpaket, das über das Netz geschickt wird, kann an jeder Station gelesen, gespeichert, manipuliert oder unterdrückt werden. Dies gilt für *eMails* genauso wie für andere Kommunikationsformen, etwa die Versendung von Formularen und die Dateiübertragung mit *FTP* (File Transfer Protokoll). Sogar viele Passwörter werden unverschlüsselt über das Netz übertragen und können ohne allzu große Schwierigkeiten abgehört und missbraucht werden. Die Vertraulichkeit von Informationen, die im Internet übertragen werden, ist allenfalls vergleichbar mit derjenigen einer Postkarte, die jeder lesen kann, der darauf Zugriff hat. Schlimmer noch: bei der Postkarte kann man ziemlich sicher sein, dass sie nur von Mitarbeitern der Post, die auf das Postgeheimnis verpflichtet sind, gelesen werden können. Im Internet ist dies anders: angesichts der Vielzahl der im Internet verknüpften Rechner lässt sich nicht einmal mit Sicherheit vorhersagen, über welche Länder ein Datenpaket gesandt wird. So kann es durchaus vorkommen, dass eine eMail, die ich an meinen von Nachbarn schicke, über einen anderen Kontinent geleitet wird. Und das in Sekundenschnelle.

Von Bertolt Brecht stammt der Satz: Was ist ein Bankraub für ein Verbrechen gegenüber der Gründung einer Bank? Auf das Internet übertragen könnte es heute heißen: Wie kriminell ist Hacking verglichen mit dem Betrieb eines Internet-Knotens? Nach ernst zu nehmenden Presseberichten werden eine Vielzahl der über die USA vermittelten Internet-Verbindungen vom amerikanischen Computer-Geheimdienst NSA überwacht.

Verschlüsselung tut not!

Immerhin werden inzwischen viele Internet-Verbindungen durch *Verschlüsselung* geschützt. Trotzdem sollte dies nicht zur Arglosigkeit verführen: noch überwiegt die unverschlüsselte und ungeschützte Kommunikation über das Netz, und nicht jede Verschlüsselung ist wirklich sicher. Durch Einsatz leistungsfähiger Computer lassen sich verschlüsselte Informationen häufig schon innerhalb weniger Minuten oder spätestens nach einigen Stunden lesen, wenn der Verschlüsselungs-Mechanismus zu schwach oder die Schlüssellänge zu kurz ist. Aus gutem Grund haben die USA den Export starker Verschlüsselungsverfahren eingeschränkt.

Diese Maßnahmen haben jedoch nicht verhindern können, dass inzwischen auch außerhalb der Vereinigten Staaten leistungsfähige Verschlüsselungssoftware zur Verfügung steht. Am weitesten verbreitet ist *PGP* (Pretty good Privacy), ein Software-Paket, das sich kostenlos aus dem Internet beziehen lässt.

Immer wieder wird - insbesondere aus Sicherheitskreisen - vorgeschlagen, die Verwendung leistungsfähiger Verschlüsselungssoftware zu verbieten oder zumindest einzuschränken (*Kryptodebatte*), damit die Strafverfolgungsbehörden und Geheimdienste auch weiterhin auf die Inhalte der Kommunikation zugreifen können. Eine derartige Regelung würde dazu führen, dass sich in Zukunft derjenige, der seine Kommunikation wirksam gegen unbefugtes Mitlesen schützt, strafbar machen würde. Zudem spricht gegen ein Verbot oder die Einschränkung der Verwendung leistungsfähiger Verschlüsselungstechnik, dass sich diejenigen, die schwere Verbrechen unter Verwendung des Internet planen, ein solches Verbot leicht umgehen könnten. Bündnis 90/Die Grünen begrüßen es daher, dass die rot-grüne Bundesregierung inzwischen erklärt hat, derartige Beschränkungen in Deutschland auch in Zukunft nicht einzuführen.

Empfänger unbekannt

Ein weiterer Unsicherheitsfaktor im Internet ist darin zu sehen, dass man nicht immer sicher sein kann, mit wem man es am anderen Ende einer Verbindung zu tun hat. Dies gilt für Anbieter und Nutzer von Internet-Diensten gleichermaßen.

Internet-Anbieter schützen sich gegen Missbrauch häufig dadurch, dass sie den Zugang zu ihren Angeboten von der Eingabe eines Passwortes oder durch sonstige Sicherheitsmechanismen beschränken. Dagegen ist der Nutzer einem Missbrauch noch immer weitgehend schutzlos ausgeliefert. So ist es durchaus möglich, dass sich hinter dem vermeintlichen Angebot der Stadtverwaltung nicht diese, sondern eine Firma versteckt. Es ist sogar wiederholt vorgekommenen, dass Web-Angebote von Hackern übernommen oder verändert wurden. Nicht zuletzt deshalb sollte sich niemand im Web allzu vertrauensselig verhalten.

Wer sich über die Vertrauenswürdigkeit eines Anbieters nicht im klaren ist, sollte mit der Preisgabe personenbezogener Daten besonders vorsichtig sein. Vor allem sollte man sich davon vergewissern, wer für ein Angebot verantwortlich ist. Von Angeboten, in denen die *Anbieterkennzeichnung*, die durch das deutsche Recht verbindlich vorgeschrieben ist, gänzlich fehlt oder unvollständig ist, sollte man besser die Finger lassen.

Erst durch die Einführung *digitaler Signaturen* wird sich die Situation deutlich verbessern. Dabei handelt es sich um softwaregesteuerte Möglichkeiten, digitale Dokumente elektronisch zu unterschreiben. Digitale Signaturen setzen umfangreiche Infrastrukturen von vertrauenswürdigen Einrichtungen voraus, die die Echtheit der Signaturen beglaubigen. Die rot-grüne Bundesregierung hat die Entwicklung entsprechender Verfahren und die Einrichtung von vertrauenswürdigen Zertifizierungsstellen gefördert. Wir halten es für einen großen Schritt in die richtige Richtung, dass in Zukunft digitale Signaturen mit handschriftlichen Unterschriften weitgehend gleichgestellt werden sollen.

Cybercrime: Straftaten und Strafverfolgung im Cyberspace

Entgegen anders lautenden Gerüchten ist das Internet kein rechtsfreier Raum. Was in der realen Welt verboten ist, ist auch im Internet nicht erlaubt. Allerdings gestaltet sich die Verfolgung von Straftaten im Internet besonders schwierig

Das Internet verknüpft Rechner in nahezu allen Ländern der Erde. Da sich die nationalen Rechtsordnungen voneinander unterscheiden, ist manches, was hierzulande strafbar ist, in anderen Ländern erlaubt - und umgekehrt. Dies müssen wir derzeit besonders schmerzhaft im Zusammenhang mit rechtsextremistischer Propaganda feststellen: Im Internet gibt es eine Vielzahl von Angeboten, die den Straftatbestand der Volksverhetzung erfüllen und deshalb bei uns verboten sind. Allerdings lassen sich diese Straftaten kaum verfolgen, denn die Angebote erfolgen aus Ländern, in denen sie erlaubt sind - und die Urheber sind häufig nicht auszumachen.

Sollen deshalb die deutschen Internet-Anbieter den Zugang zu denjenigen ausländischen Rechnern zu sperren, auf denen sich verbotene Inhalte befinden? Wir halten dies für unverhältnismäßig, denn auf denselben Computern befinden zumeist eine Vielzahl anderer Angebote, die auch nach deutschem Recht zulässig sind. Eine Sperre würde bedeuten, dass auch diese Angebote aus Deutschland nicht mehr abgerufen werden könnten. Zudem wäre die Umgehung der Sperre nicht sehr kompliziert, denn die Urheber könnten gesperrte Angebote ohne größeren Aufwand auf andere Rechner verlagern.

Keine automatische Internetüberwachung!

Strafverfolgungsbehörden und Geheimdienste erheben immer wieder die Forderung, auf den Rechnern von Internet-Anbietern Überwachungseinrichtungen zu installieren, über die sie auf eMails und andere Formen der Internet-Kommunikation zugreifen können. In den USA ist eine derartige Überwachungssoftware bereits im Einsatz (http://www.fbi.gov/programs/carnivore/carnivore.htm). Auch in Deutschland sollten nach den Plänen der CDU/FDP-Bundesregierung alle Internet-Anbieter durch die Telekommunikations-Überwachungsverordnung (TKÜV) zur Einrichtung entsprechender Schnittstellen verpflichtet werden.

Auch die Forderung der Innenminister-Konferenz vom 24. November 2000, für Zwecke der Strafverfolgung den Providern eine vorsorgliche umfassende Protokollierungs- und Aufbewahrungspflicht der 'digitalen Spuren', die jeder Internetnutzer grundsätzlich hinterlässt, vorzuschreiben, geht in die falsche Richtung. (http://www.im.nrw.de/pm2000/news_478.htm) Wir teilen die Kritik der Datenschutzbeauftragten, die eine solche Vorgabe für verfassungswidrig halten. Die Forderung der Innenministerkonferenz nach Aufzeichnung aller IP- Adressen durch Zugangs-Provider und Server-Betreiber wäre vergleichbar mit einer Verpflichtung für die Post, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern und für den Zugriff der Sicherheitsbehörden bereitzuhalten.

Das Bundesverfassungsgericht hat dagegen wiederholt festgestellt, dass die Speicherung personenbezogener Daten nicht zu einer Rundumbeobachtung der Bürger führen darf. Eine solche umfassende Beobachtung würde für das Internet mit der angestrebten Regelung entstehen. Das von den Innenministern angestrebte Verfahren würde den mit den Vorschriften über Tele- und Mediendienste gewährleisteten Datenschutz unterlaufen. Es widerspräche auch dem von der Bundesregierung selbst vorgelegten Entwurf einer Novelle zum Bundesdatenschutzgesetz, das die Entwicklung und den Einsatz von technischen Verfahren vorsieht, die mit einem Minimum an personenbezogener Datenverarbeitung betrieben werden können. Das Vorhaben der Innenministerkonferenz würde zu einem unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung von Millionen rechtstreuer Internetnutzer führen, die keineswegs alle potenzielle Straftäter sind. Das gesamte Vorhaben wäre zudem zur Verfolgung von schweren Straftaten untauglich, weil Straftäter ohne größere technische Schwierigkeiten auf Provider in anderen Ländern ausweichen könnten.

Zwar muss es hingenommen werden, dass - wie dies bereits nach derzeitigem Recht möglich ist - in Fällen schwerer Kriminalität, insbesondere zur Aufklärung von Kapitalverbrechen, im Einzelfall auch die elektronische Kommunikation überwacht wird. Bündnis 90/Die Grünen wenden sich aber entschieden gegen alle Vorhaben, die die Vertraulichkeit der Nutzung des Internet einschränken. Die Einrichtung derartiger Überwachungsverfahren würde dem Missbrauch und einer lückenlosen Kontrolle Tür und Tor öffnen. Solche Vorhaben werden deshalb von uns abgelehnt.

Aus den gleichen Gründen wenden wir uns auch gegen Forderungen der Software- und Musik-Industrie, für Zwecke der Durchsetzung des Urheberrechts automatische Kontroll- und Blocking-Programme bei den Internet-Anbietern zu installieren. Auch derartige Verfahren würden eine lückenlose Überwachung der Internet-Kommunikation ermöglichen; sie wären zudem eine Infrastruktur zur umfassenden Zensur von Internet-Inhalten, die insbesondere autoritäre Regimes geradezu zum Ge- und Missbrauch einladen.

Angriffe aus dem Netz: Hacking, Viren, Würmer und trojanische Pferde

Die ans Internet angeschlossenen Rechner sind vielfältigen Gefahren ausgesetzt. Hierzu gehören *Hacking*-Angriffe, Computer-*Viren*, *Würmer* und *trojanische Pferde*. Leider sind viele Programme, die für die Nutzung des Internets verwendet werden, von Hause aus nicht ordentlich gegen derartige Gefahren geschützt und die weite Verbreitung von Betriebs- und Anwendungssoftware eines einzigen Herstellers (Software-Monokultur) bereiten derartigen Angriffen ein fruchtbares Feld.

Internet-Browser werden häufig so ausgeliefert, dass sie den Zugriff aus dem Internet auf die Festplatte des Nutzers gestatten. Von den Herstellern ist zu fordern, dass sie die Sicherheitsmaßnahmen in der Software verbessern und die Nutzer über die mit bestimmten Einstellungen verbundenen Gefahren angemessen aufklären. Es ist zu vermuten, dass die Hersteller häufig eigene wirtschaftliche Interessen daran haben, dass nicht der höchste Sicherheitsstandard gewährleistet ist, weil dadurch z.B. das Setzen von Cookies erschwert würde. Deshalb treten Bündnis 90/Die Grünen dafür ein, dass sich die Software-Hersteller auf freiwilliger Basis einer unabhängigen Zertifizierung zu unterwerfen (*Datenschutz-Audit*).

Angesichts der Hacking-Fälle und der Gefahren von Viren wird aus Sicherheitskreisen die Forderung erhoben, die Überwachung des Internet zu verstärken. Wir halten dies für den falschen Weg. Nicht nur die von dem Nutzer verwendete Software, sondern auch die Netzstrukturen müssen so weiter entwickelt werden, dass bösartige Viren und andere Schadprogramme keine Chance haben. Zu diesem Zweck muss die Produkthaftung ausgebaut werden: die Hersteller müssten Schadensersatz leisten, wenn sie fehleranfällige Systeme ausliefern.

Die vorsorgliche Registrierung und Überwachung des Nutzungsverhaltens, wie sie zum Beispiel in dem Entwurf für eine Cybercrime-Konvention des Europarates vorgesehen ist, halten wir für falsch. Sie würde zu einer vollständigen Registrierung des Nutzungsverhaltens aller Surfer führen und damit auch die überwiegende Mehrheit derjenigen treffen, die sich rechtmäßig verhalten.

Für ein Grundrecht auf unbeobachtete Kommunikation!

Das *Post- und Fernmeldegeheimnis* wird durch Art. 10 des Grundgesetzes geschützt. Wir setzen uns dafür ein, den Grundrechtsschutz ausdrücklich auf alle Formen der elektronischen Kommunikation und Mediennutzung zu erstrecken. Das Post- und Fernmeldegeheimnis muss zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter entwickelt werden. Das Mediennutzungsgeheimnis soll auch die Vertraulichkeit der Abrufe aus dem Internet garantieren. Jeder Nutzer soll im Prinzip selbst darüber entscheiden, wer welche Kenntnisse über sein Nutzungsverhalten erhält.

Gesetzlich muss zudem gewährleistet werden, dass nicht nur staatliche Stellen sondern auch private Unternehmen zur Einhaltung des Mediennutzungsgeheimnisses verpflichtet werden.

Datenschutzrecht - auch im Internet!

Bereits heute gelten die Datenschutzgesetze auch im Internet: wer über das Internet Waren oder Dienstleistungen vermarktet, muss sich - wie in der "Offline-Welt" - an das *Bundesdatenschutzgesetz* halten. Bündnis 90/Die Grünen beteiligen sich an der Modernisierung des Datenschutzrechts. Im Frühjahr 2001 soll die erste Stufe der Novellierung des Bundesdatenschutzgesetzes abgeschlossen werden. Wir haben uns mit unserem Koalitionspartner darauf geeinigt, noch in dieser Legislaturperiode das Datenschutzrecht einer umfassenden Überarbeitung zu unterziehen und dabei die Rechte der Betroffenen auszuweiten und die Rechtsvorschriften zu vereinfachen.

Die Daten der Internet-Nutzerinnen und -Nutzer werden darüber hinaus durch besondere Rechtsvorschriften - das *Teledienstedatenschutzgesetz* und den *Mediendienstestaatsvertrag* - geschützt. Nach diesen Rechtsvorschriften ist die Verarbeitung von *Nutzungsdaten* ohne ausdrückliche Einwilligung des Nutzers nur zur Vermittlung des entsprechenden Angebots und für Abrechnungszwecke zulässig. Wir treten dafür ein, dass es dabei bleibt.

Transparenz: Es werde Licht!

Angesichts des großen wirtschaftlichen Interesses an Daten über das Surfverhalten setzen sich Bündnis 90/Die Grünen für mehr Transparenz bei der Erhebung und Verarbeitung personenbezogener Daten im Internet ein.

Bereits das geltende Recht sieht vor, dass diejenigen, die Nutzungsdaten erheben, verarbeiten oder nutzen, dies nur dann dürfen, wenn sie die Betroffenen zuvor angemessen aufgeklärt haben. Wir setzen uns dafür ein, diese Informationspflichten durchzusetzen und weiter zu verbessern.

Entscheidungsfreiheit des Nutzers

Die Nutzerinnen und Nutzer haben das Recht selbst zu entscheiden, ob sie mit der Registrierung einverstanden sind. Der Zugriff auf Internet-Angebote darf bereits nach der gegenwärtigen Rechtslage nicht nur deshalb verweigert werden, weil der Betroffene mit der Verwendung seiner Daten für Werbezwecke nicht einverstanden ist. Bei der Novellierung des Teledienstedatenschutzgesetzes werden wir auf die Klarstellung achten, dass sich die Entscheidungsmöglichkeiten des Nutzers auch auf solche Nutzungsprofile beziehen, die (noch) nicht unter dem Namen des Nutzers, sondern unter einem Pseudonym erstellt werden.

Leider halten sich viele Anbieter nicht an diese gesetzlichen Vorgaben. Wir setzen uns auf Bundes- und Landesebene dafür ein, die *Datenschutz-Aufsichtsbehörden* zu stärken und ihnen wirksame Mittel zur Durchsetzung der Vorgaben des Datenschutzrechts in die Hand zu geben.

Anonyme oder Nutzung und Verwendung von Pseudonymen

Das Tele- und Mediendiensterecht sehen vor, dass Internet-Angebote so gestaltet werden müssen, dass dabei keine oder so wenig wie möglich personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Im Mittelpunkt steht dabei die Möglichkeit, Angebote anonym oder unter *Pseudonym* zu nutzen.

Bei der anstehenden Novellierung des Bundesdatenschutzgesetzes sollen diese Vorgaben auf sämtliche Formen der Verarbeitung personenbezogener Daten ausgeweitet werden. Wir sehen darin eine deutliche Verbesserung des Datenschutzes.

Dein gutes Recht als Nutzer

Auskunftsrecht: Jeder Internet-Nutzer hat ein Auskunftsrecht bezüglich derjenigen Daten, die über ihn vom Anbieter gespeichert werden. Der Anbieter ist verpflichtet, diese Auskünfte unentgeltlich und jederzeit - auch elektronisch - zu erteilen.

Einwilligung: Die Verwendung der personenbezogenen Daten von Internet-Nutzern für Zwecke der Werbung, Beratung und Marktforschung oder zur bedarfsgerechten Gestaltung des Internet-Angebot ist nur zulässig, soweit der Nutzer ausdrücklich eingewilligt hat. Wenn die Einwilligung elektronisch erteilt wird, ist sie nur dann wirksam, wenn sichergestellt ist, dass der Nutzer die elektronische Einwilligung selbst und bewusst abgegeben hat.

Widerrufsrecht: Der Nutzer hat das Recht, seine Einwilligung jederzeit und mit Wirkung für die Zukunft zu widerrufen. Diese Widerrufsrecht ist nicht an eine bestimmte Form gebunden, das heißt der Widerruf kann sowohl schriftlich, telefonisch oder per *eMail* erteilt werden.

Datenlöschung: Die Daten von Internet-Nutzern müssen gelöscht werden, sobald sie für die Erbringung des Dienstes nicht mehr erforderlich sind. Nutzungsdaten müssen dann gelöscht werden, wenn sie für die neue Vermittlung des Angebots und für Abrechnungszwecke nicht mehr erforderlich sind.

Internet am Arbeitsplatz

Inzwischen hat das Internet auch im Arbeitsleben Einzug gehalten. An einer Vielzahl von Arbeitsplätzen werden Internet-Dienste als Arbeitsmittel verwendet, z.B. sind manche Arbeitsprozesse ohne *eMail* kaum noch zu bewältigen. Die Arbeitserleichterungen, die mit der neuen Technik verbunden sind, gehen jedoch mit neuen Risiken einher. Dabei eignen sich gerade solche Maßnahmen, die das Unternehmen gegen das Eindringen von Hackern und die Einschleusung von Computer-Viren ergreifen, in besonderem Maße zur Überwachung des Verhaltens der Arbeitnehmerinnen und Arbeitnehmer:

So haben viele Unternehmen zwischen das betriebliche *Intranet* und das Internet eine *Firewall* gesetzt. Alle eingehenden und ausgehenden Datenpakete werden durch die Firewall geleitet und von dieser auf verdächtige Inhalte inspiziert. Auf diese Weise sollen Angriffe auf das interne Netz verhindert und aufgedeckt werden. Von *Virenscannern*, die ebenfalls in der Firewall installiert sind, verspricht man sich das Erkennen und Ausfiltern derartiger Schadprogramme. Es liegt auf der Hand, dass Firewalls sich sehr gut dazu eignen, die Inhalte der Kommunikation und das Surfverhalten am Arbeitsplatz auch anderweitig zu überwachen. Dabei kann man sich der Funktionen bedienen, die eigentlich dazu gedacht sind, die internen Netze technisch abzusichern. So ist es ohne weiteres – und für den Nutzer unbemerkt – möglich, an einer Firewall *eMails* nach beliebigen Inhalten zu durchsuchen. Und in Logprotokollen, die ebenfalls auf der Firewall geführt werden, können die URLs aller *WWW*-Seiten protokolliert werden, die durch die Arbeitnehmer abgerufen wurden.

Auch eMails am Arbeitsplatz unterliegen dem *Fernmeldegeheimnis*. Zwar hat der Arbeitgeber das Recht, vom Arbeitnehmer auch über die Arbeitsprozesse informiert zu werden, die über elektronische Dienste abgewickelt werden, und kann deshalb eine ordnungsgemäße Verwendung dieses neuen Arbeitsmittels verlangen; dazu gehört auch, dass er im Einzelfall die Herausgabe von dienstlichen eMails durch den Arbeitnehmer verlangen kann. Es ist aber nicht hinzunehmen, wenn ein Arbeitgeber die eMails regelmäßig mitliest oder sich sogar heimlich von ihnen Kenntnis verschafft.

Die Installation von Internet-Schnittstellen am Arbeitsplatz ist stets mitbestimmungspflichtig, denn es handelt sich um Einrichtungen, die sich zur Überwachung des Verhaltens der Beschäftigten eignen. Betriebs- und Personalräte müssen deshalb frühzeitig an entsprechenden Projekten beteiligt werden. Wegen der Überwachungsgefahren raten wir zum Abschluss von Betriebs- und Dienstvereinbarungen über die Internet-Nutzung, denn auf diese Weise gibt es klare Regelungen zum betrieblichen Einsatz des Internet. In den Vereinbarungen sollte insbesondere geregelt werden, dass Protokollierungen nur kurzfristig und nur in dem Umfang vorgenommen werden, der unbedingt erforderlich ist, um die Netzsicherheit zu gewährleisten. Ferner muss festgelegt werden, dass die protokollierten Daten nicht zur Verhaltens- und Leistungskontrolle der Arbeitnehmer verwendet werden dürfen. Schließlich sind auch Regelungen zur Verwendung von eMails erforderlich, in denen eindeutig festgelegt ist, wer sich für welche Zwecke Kenntnis von eMails verschaffen darf, z.B. in Vertretungs- und Krankheitsfällen.

Bündnis 90/Die Grünen setzen sich dafür ein, die Internet-Nutzung am Arbeitsplatz in einem Arbeitnehmerdatenschutzgesetz zu regeln, das noch in dieser Legislaturperiode verabschiedet werden soll. Wir erteilen den Vorstellungen des Bundesfinanzministeriums eine Absage, das die lückenlose Protokollierung von Internet-Zugriffen am Arbeitsplatz für Zwecke der Besteuerung gefordert hatte.

Für wirksamen Datenschutz

Wir treten dafür ein, dass die Rechte der Nutzerinnen und Nutzer des Internet nicht nur durch gesetzliche Vorschriften weiter gestärkt werden, sondern auch ihre Umsetzung. Hierzu gehört vor allem die Durchsetzung des uneingeschränkten elektronischen Auskunftsrechts über alle Daten, die bei der Nutzung des Internet anfallen und die Überwachung der Löschungsregelungen. Damit die Datenschutzrechte nicht nur auf dem Papier bestehen, muss die Datenschutz-Aufsicht und -Beratung verstärkt werden. Die Datenschutz-*Aufsichtsbehörden* müssen wirklich unabhängig sein, wie es bereits die *EU-Datenschutz-Richtlinie* vorsieht, und sie müssen Mittel in die Hand bekommen, um die Vorgaben des Datenschutzrechts auch im Internet durchzusetzen.

Bündnis 90/Die Grünen setzen sich dafür ein, den Datenschutz nicht nur in der EU besser zu koordinieren, sondern wollen auch auf Verbesserungen in den so genannten "Drittstaaten" und den USA hinwirken. Gerade im Internet bleibt der Datenschutz lückenhaft, wenn er sich in nationalen Regelungen erschöpft.

Nützliche Links

- Das virtuelle Datenschutzbüro ("erste Adresse" zum Thema Datenschutz; Links zu allen Datenschutzbeauftragten und zu weiteren Datenschutzangeboten): http://www.datenschutz.de

- Datenschutz-Server der Zeitschrift „Datenschutz und Datensicherheit": http://www.dud.de
- Selbsttest: Wie sicher sind meine Browser-Einstellungen: http://www.lfd.niedersachsen.de/service/service_selbstt.html
- Internationaler Datenschutz - Privacy International (PI): http://www.privacy.org
- Projekt „moderner Datenschutz": http://www.moderner-datenschutz.de/akteure/gruene.html
- Deutsche Vereinigung für Datenschutz (DVD) e.V.: http://www.aktiv.org/DVD/
- Arbeitsgemeinschaft der Verbraucherverbände zur Anbieterkennzeichnung im Internet: http://www.agv.de/politik/verbraucherrecht/polkonvent.htm

Glossar

Anbieterkennzeichnung

Das deutsche Recht sieht vor, dass Angebote im Internet mit einem Impressum zu versehen sind, das den Verantwortlichen und seine Adresse ausweist.

Aufsichtsbehörden

Behörden, die die Einhaltung des BDSG und anderer Datenschutzvorschriften im nichtöffentlichen Bereich überwachen. Derzeit sind die meisten Datenschutz-Aufsichtsbehörden noch bei den Innenministerien der Länder angesiedelt. In den Stadtstaaten, in Niedersachsen, Nordrhein-Westfalen und in Schleswig-Holsteins nehmen die Landesbeauftragten für den Datenschutz diese Aufgabe wahr.

BDSG

Abk. für Bundesdatenschutzgesetz. Das BDSG enthält Vorschriften über den Datenschutz für öffentliche Stellen des Bundes und für den privaten Bereich.

Chatroom

Virtueller Treffpunkt im Netz, in dem üblicherweise zwischen den Teilnehmern Text- Informationen ausgetauscht werden. Chatrooms setzen voraus, dass auf den beteiligten Computern eine entsprechende Software installiert ist. Im Internet weit verbreitet ist der IRC (Internet Relay Chat)

Cookies

Kleine Textdateien, die von Anbietern auf dem Rechner des Nutzers platziert werden. Cookies werden zur Verbindungssteuerung und für die Bildung von Nutzungsprofilen verwendet.

CRM

Abk. für Customer Relations Management; CRM beschreibt Verfahren zur individuellen Kundenansprache und Pflege von Kundenbeziehungen. Für diese Zwecke wird häufig auf Nutzungsprofile zurückgegriffen.

Datenschutz-Audit

Verfahren zur datenschutzrechtlichen Bewertung von Software, elektronischen Dienstleistungen und Geschäftspraktiken durch unabhängige Gutachter. Nach Abschluss des Datenschutz-Audit werden Qualitätssiegel vergeben.

digitale Signatur

Automatisch erzeugte elektronische "Unterschrift". Die digitale Signatur soll die Echtheit und die Urheberschaft von elektronischen Dokumenten sicherstellen. Ihr kommt insbesondere beim eCommerce zunehmende Bedeutung zu. In Zukunft sollen digitale Signaturen weitgehend mit handschriftlichen Unterschriften gleichgestellt werden.

Domain

Bezeichnung eines abgegrenzten Bereiches im Internet. Domains sind hierarchisch gegliedert. Die "Top-Level-Domains" sind üblicher Weise durch die Kürzel .de, .com, .org usw. gekennzeichnet. Die Vergabe von Domain-Namen erfolgt durch die jeweiligen zu-

ständigen nationalen Vergabeorganisationen (z.B. Deutsches Network Information Centre - DeNIC - http://www.denic.de). Das höchste internationale Vergabegremium ist die Internet Corporation for Assigned Names and Numbers -ICANN.

eMail

Electronic Mail (kurz eMail) ist der am weitesten verbreitete Internet-Dienst. eMail 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 eMail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um eMails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. eMail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z.B. FTP, WWW) genutzt werden.

EU-Datenschutz-Richtlinie

Richtlinie der Europäischen Union über die Gewährleistung des Schutzes personenbezogener Daten in den Mitgliedstaaten der Europäischen Gemeinschaft. Die Richtlinie schreibt vor, dass personenbezogene Daten nur dann an Drittstaaten außerhalb der Europäischen Gemeinschaft übermittelt werden dürfen, wenn in den Empfängerländern ein angemessenes Datenschutzniveau gewährleistet ist. Die Vorgaben der EU-Datenschutzrichtlinie werden mit der Novelle des *BDSG* in deutsches Recht umgesetzt.

Firewall

Hard- und Software, die verwendet wird, interne Netze von Betrieben und Verwaltungen vom weltweiten Internet abzuschotten. Auf Firewall-Systemen laufen unter anderem Virenscanner, mit denen Schadprogramme erkannt und blockiert werden, und es werden Logprotokolle über die Inanspruchnahme des Internet geführt.

FTP

Abk. für "File Transfer Protocol". FTP dient dem Übertragen von Dateien zwischen Rechnern. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung ist das Vorhandensein einer Zugangsberechtigung, die durch ein Passwort geschützt wird. Ferner gibt es öffentliche Zugriffsmöglichkeiten auf 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 bereit halten.

Hacking

Unbefugtes Eindringen in fremde Rechnersysteme.

informationelles Selbstbestimmungsrecht

Das Recht des einzelnen, grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, wird durch das Grundgesetz gewährleistet. Vom Bundesverfassungsgericht im Volkszählungsurteil als Grundrecht anerkannt, das sich aus den Art. 1 und 2 Grundgesetz ergibt. Einschränkungen dieses Rechts bedürfen eines Gesetzes. Sie sind nur im überwiegenden Allgemeininteresse zulässig.

Intranet

Internes Netz eines Unternehmen oder einer Verwaltung, das auf derselben technischen Basis wie das Internet funktioniert. Intranets sind häufig mit dem Internet verbunden. Zwischen Inter- und Intranet werden üblicher Weise *Firewalls* installiert.

IP-Nummer

Jeder Rechner im Internet hat 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 zumeist über eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adressinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Telekommunikationsverbindungen (Kupferkabel, Satellitenverbindungen, Glasfaser usw.) aus.

Kryptodebatte

Diskussion über das Verbot bzw. die Einschränkung der Verwendung von *Verschlüsselung*sprogrammen. Das Verbot wird von der überwiegenden Mehrheit der Informatikerinnen und Informatiker und von der Internet-Gemeinde abgelehnt. Die Bundesregierung hat öffentlich erklärt, dass sie keine Pläne zum Verbot oder zur Begrenzung des Einsatzes von Verschlüsselungsprogrammen plant.

Link

Verweis auf eine andere Internet-Adresse, zu der der Nutzer entweder durch Mausklick verzweigt oder zu der automatisch eine zusätzliche Verbindung aufgebaut wird. Automatische Links werden vor allem für die Einblendung von Grafik-Dateien eingesetzt. Dies haben sich die Anbieter von Werbebannern und Web Bugs zu Nutze gemacht.

Logprotokoll

Zusammenstellung von Informationen über die Nutzung eines bestimmten Computers oder Dienstes. Es ist üblich, dass die Anbieter von Internet-Inhalten umfangreiche Logprotokolle führen, die neben der IP-Nummer des Nutzers auch die URL und Angaben zu dem vom Nutzer verwendeten technischen System enthalten.

Mediendienstestaatsvertrag

Länder-Staatsvertrag über die Nutzung von Mediendiensten. Dabei handelt es sich um Angebote, die sich an die Öffentlichkeit wenden, z.B. elektronisch veröffentlichte Zeitungen. Die Datenschutzbestimmungen im Mediendienstestaatsvertrag entsprechen denjenigen im TDDSG.

Newsgroup

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. Zur Zeit 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.

Nutzungsdaten

Diejenigen Daten, die bei der Inanspruchnahme des Internet über den Nutzer anfallen. Typische Nutzungsdaten sind die IP-Nummer, die URL der Ressourcen, auf die zugegriffen wurde, Zeit- und Datumsangaben, Datenmengen usw.

Nutzungsprofil

Sammlung von Nutzungsdaten bestimmter Nutzer, die bei wiederholter Inanspruchnahme von Internet-Diensten anfallen. Die Daten können anhand des Namens oder anderer Zuordnungsmerkmale einzelnen Nutzern zugeordnet werden. Derzeit üblich ist die Zuordnung anhand automatisch generierter Identifizierungsnummern, die in Cookies auf den Rechnern der Nutzer abgelegt werden.

PGP

Abk. für "Pretty Good Privacy". Es handelt sich um eine Software zur *Verschlüsselung*, die es für verschiedene Betriebssysteme gibt. PGP gilt als sicher und kann von Privatanwendern kostenfrei genutzt werden (Public Domain Software); Bezugsadresse im Internet: (http://www.pgpi.org/) PGP gibt es für verschiedene Betriebssystem-Plattformen und kann problemlos in die meisten eMail-Programme eingebunden werden. Der Autor von PGP Phil Zimmermann (http://www.pgp.com/phil/) ist wiederholt angeklagt worden, durch Bereitstellung der „zu sicheren" Software gegen amerikanische Rüstungsexportbestimmungen verstoßen zu haben.

Post- und Fernmeldegeheimnis

Schutz der Vertraulichkeit der Brief- und Fernmeldekommunikation. Art. 10 Grundgesetz schützt das Post- und Fernmeldegeheimnis vor unberechtigten Eingriffen staatlicher Stellen. Das einfachgesetzliche Fernmeldegeheimnis von § 85 Telekommunikationsgesetz bindet auch die privaten Anbieter von Telekommunikationsdiensten. Die Kommunikation mittels eMail ist durch das Fernmeldegeheimnis geschützt.

Pseudonym

Eine fremde oder erfundene Identität ohne direkte Rückschlussmöglichkeit auf die Person des Trägers.

Systemdatenschutz

Neue Mechanismen für den Schutz personenbezogener Daten, die eine datenschutzfreundliche Gestaltung der Datenverarbeitungstechniken zum Gegenstand haben. Hierzu gehört insbesondere die Vorgabe für die Anbieter von Tele- und Mediendiensten, die die Gestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen (§ 3 TDDSG/§ 12 Abs. 5 MDStV); ferner die Verpflichtung, die Nutzung von Tele- und Mediendiensten anonym bzw. unter Pseudonym zu ermöglichen (§ 4 Abs. 1 TDDSG/§ 13 Abs. 1 MDStV). Bündnis 90 Die Grünen haben sich dafür eingesetzt, dass die Vorschriften zum Systemdatenschutz auch in das allgemeine Datenschutzrecht (BDSG) übernommen werden.

Suchmaschine

Internet-Dienste, mit denen sich Angebote im WWW systematisch nach frei vergebenen Suchbegriffen auswerten lassen. Sehr bekannt und leistungsfähig sind die Suchmaschinen AltaVista, Lycos, Yahoo, Google, deja.com. Daneben gibt viele, zum Teil fachbezogene Suchmaschinen.

TDDSG

Abk. für Teledienstedatenschutzgesetz. Das TDDSG regelt den Datenschutz bei Telediensten. Zu den Telediensten gehört auch die Vermittlung des Zugangs zum Internet und interaktive Internet-Dienste, z.B. im elektronischen Handel (eCommerce).

URL

Abk. für Uniform Ressource Locator; einheitliche Adresse für Ressourcen im Internet. Jede Seite im *WWW* ist durch eine bestimmte URL eindeutig identifizierbar.

Verschlüsselung

Veränderung von Informationen derart, dass sie von Unbefugten nicht oder zumindest nur mit unverhältnismäßigem Aufwand zur Kenntnis genommen werden können. Der Zugriff auf verschlüsselte Informationen ist nur denjenigen Personen möglich, die Kenntnis von dem passenden Schlüssel haben.

Viren, Würmer, trojanische Pferde

Schadprogramme, die insbesondere über das Internet zusätzliche Verbreitung finden. Bei Viren handelt es sich um Programm-Bestandteile, die nicht selbstständig auszuführen sind, sich jedoch in einem Wirtsprogramm aktivieren lassen und andere Programme infizieren. Würmer sind ausführbare Programme, die sich über verschiedene Mechanismen, insbesondere über Adressbücher von eMail-Programmen, vervielfältigen. Trojanische Pferde sind als nützliche Software getarnte Schadprogramme.

Web Bug

Winzige Grafikdatei, meist von der Größe von nur einem Pixel, die in Web-Seiten eingebaut werden, um damit eine versteckte Verbindung zu einem anderen Web-Server aufzubauen. Web bugs werden häufig in Verbindung mit *Cookies* verwendet.

Werbebanner

In eine Webseite eingeblendete "Anzeige". Werbebanner werden zum größten Teil von darauf spezialisierten Anbietern (Bannerserver) vermarktet. Durch Verwendung von Nutzungsprofilen streben die Anbieter an, die Banner entsprechend der individuellen Interessenlage der Nutzer auszusuchen und gezielt einzuspielen.

WWW

Abkürzung für World Wide Web. Das WWW („Web“) und bezeichnet den neben *eMail* am häufigsten genutzten Dienst im Internet. WWW kann nahezu alle anderen Dienste integrieren und ermöglicht den Zugriff auf weltweit verteilte Informationen, die für das Internet bereitgestellt werden. Alle im Web verfügbaren Informationen sind eindeutig durch eine Adresse (die *URL*) gekennzeichnet. Durch Einfügen von *Links* können verschiedene Dokumente miteinander verbunden werden (Hypertext). Bei der Kommunikation zwischen dem WWW-Client (dies ist der PC, der zum Surfen benutzt wird) und dem WWW-Server (der Computer, auf dem die Informationen bereitgestellt werden) verständigen sich die Computer auf Basis von gemeinsamen Konventionen, die im Hyper Text Transfer Protocol (HTTP) zusammengefasst sind.

Zugangs-Provider

Unternehmern, die die Nutzung des Internets ermöglichen. Es handelt sich dabei sowohl um reine Zugangsvermittler als auch um solche Anbieter, die zusätzlich eigene Inhalte im Netz zur Verfügung stellen (z.B. T-Online, Web, AOL).