Stand: 2000-09-10. Leicht gekürzte Fassung mit Stand vom 3. Februar 2000 erschienen als:
Marit Köhntopp, Kristian Köhntopp: Datenspuren im Internet; Computer und Recht (CR) 4/2000; 248-257.

Datenspuren im Internet

Marit Köhntopp / Kristian Köhntopp

Bei der Nutzung des Internet hinterlässt jeder Teilnehmer Spuren. Einige Nutzerinformationen werden bewusst und freiwillig im Internet zur Verfügung gestellt, über andere Daten wissen viele Teilnehmer nicht Bescheid. Es muss unterschieden werden, wer jeweils Zugriff auf die Datenspuren hat und welche Kenntnisse daraus erlangt werden können. Nicht immer sind die Informationen authentisch, denn teilweise können Datenspuren verwischt oder gefälscht werden.

I. Funktionsweise des Internet

Das Internet ist ein Zusammenschluss von Rechnern, die über einen gemeinsamen Kommunikationsstandard, TCP/IP (Transmission Control Protocol/Internet Protocol) Daten austauschen können. Jeder Rechner im Internet erhält zu diesem Zweck eine eindeutige Adressierung, die IP-Adresse. Eine IP-Adresse ist eine 32 Bit lange Zahl[1], die meist – für eine bessere Lesbarkeit – durch vier durch Punkte getrennte Zahlen zwischen 0 und 255 geschrieben wird, z.B. 195.247.68.5.

1. Statische und dynamische IP-Adressen

Man unterscheidet die statischen von den dynamischen IP-Adressen:

- Eine **statische IP-Adresse** wird für längere Dauer an einen bestimmten Rechner gebunden. Statische Adressen sind typisch für Institutionen oder Einzelpersonen, die sich frühzeitig diese Adressen bei den Vergabestellen, den Network Information Centern (NIC), haben sichern können.

- **Dynamische IP-Adressen** werden dem Teilnehmer erst bei der Nutzung zugewiesen und können pro Sitzung oder sogar während Sitzungen wechseln. Sie werden meist aus einem Pool von IP-Adressen genommen, über die Internet-Service-Providern oder Online-Dienst-Anbietern verfügen. Meist stehen sehr viel weniger IP-Adressen zur Verfügung, als potenzielle Teilnehmer angeschlossen sind, z.B. nur ein Zehntel, da diese Adressen lediglich für die Zahl der gleichzeitigen Nutzer reichen müssen.

Während statische IP-Adressen immer denselben Rechner (und damit oft auch dieselbe Person, die darüber das Internet nutzt) kennzeichnen und prinzipiell verkettbar sind, macht dies bei den dynamischen IP-Adressen nur für diejenigen Sinn, die die dynamische Zuordnung zu den Teilnehmern bzw. ihren Rechnern beim Anbieter kennen.

[1] Diese Darstellung bezieht sich auf das zur Zeit eingesetzte Internet-Protokoll IPv4. Im künftigen Protokoll IPv6 werden die IP-Adressen eine Länge von 128 Bit haben. Dadurch lassen sich ca. 10^{29} (genau 2^{96})mal so viele Internet-Adressen vergeben. Rechnerisch könnte jeder Erdenbürger mit 10^{32} IP-Adressen (eine 1 mit 32 Nullen) versorgt werden. Das reicht für individuelle IP-Adressen für jedes Elektrogerät im Haushalt auf absehbare Zeit aus.

2. Proxy

Oft identifiziert eine IP-Adresse nicht unmittelbar den abrufenden Rechner, sondern einen vorgeschalteten **Proxy**-Rechner, der stellvertretend für andere Computer auftritt und die Abrufe vornimmt. Proxies werden beispielsweise verwendet, um durch Zwischenspeichern der Abrufergebnisse Bandbreite bei gleichartigen Anfragen zu sparen oder um die sich dahinter befindenden Rechner gegen direkte Angriffe zu schützen, z.B. bei einer Kombination mit einer Firewall.

3. Domain Name Service

Da sich Menschen normalerweise Zahlen schlecht merken, können die IP-Adressen von Rechnern in einen Namen umgesetzt werden. Zum Beispiel verbirgt sich hinter dem Rechnernamen www.koehntopp.de die IP-Adresse 195.244.241.123. Diese Aufgabe übernimmt der Domain Name Service (DNS). Die Domains werden ebenfalls von den zuständigen Network Information Centern gegen monatliche Zahlungen vergeben. Die Zuordnung von Domainnamen und IP-Adressen wird in so genannten DNS-Servern gespeichert und zum Abruf bereitgehalten. Bei jeder Anfrage nach einer Internet-Adresse, z.B. beim World Wide Web nach einer Serverkennung wie www.koehntopp.de, leistet zunächst der DNS die Auflösung des Namens in die zugehörige IP-Adresse, mit der dann die Verbindung über die Wegewahleinheiten (Router) im Internet aufgebaut wird.

4. Zugangsvermittlung

Vorgeschaltet vor die eigentliche Nutzung des Internet ist die Telekommunikation mit dem Zugangsanbieter: Um die Dienste eines Providers nutzen zu können, muss sich der Rechner des Teilnehmers dort über Telekommunikationsleitungen einwählen. Im Standardfall überträgt der Rechner dann die zum vereinbarten Benutzerkonto (Account) gehörigen Daten, einen Login-Namen und ein Passwort.

Abhängig von den genutzten Diensten fallen weitere Informationen an (siehe Abschnitt III.).

II. Rollen und Akteure[2]

Prinzipiell hängen mit der Nutzung des Internet verschiedene Rollen zusammen, die diverse Aufgaben wahrnehmen und damit verbunden auch unterschiedliche Informationen über den Teilnehmer zur Kenntnis nehmen können. Die wichtigsten Rollen sind in Abb. 1 dargestellt.

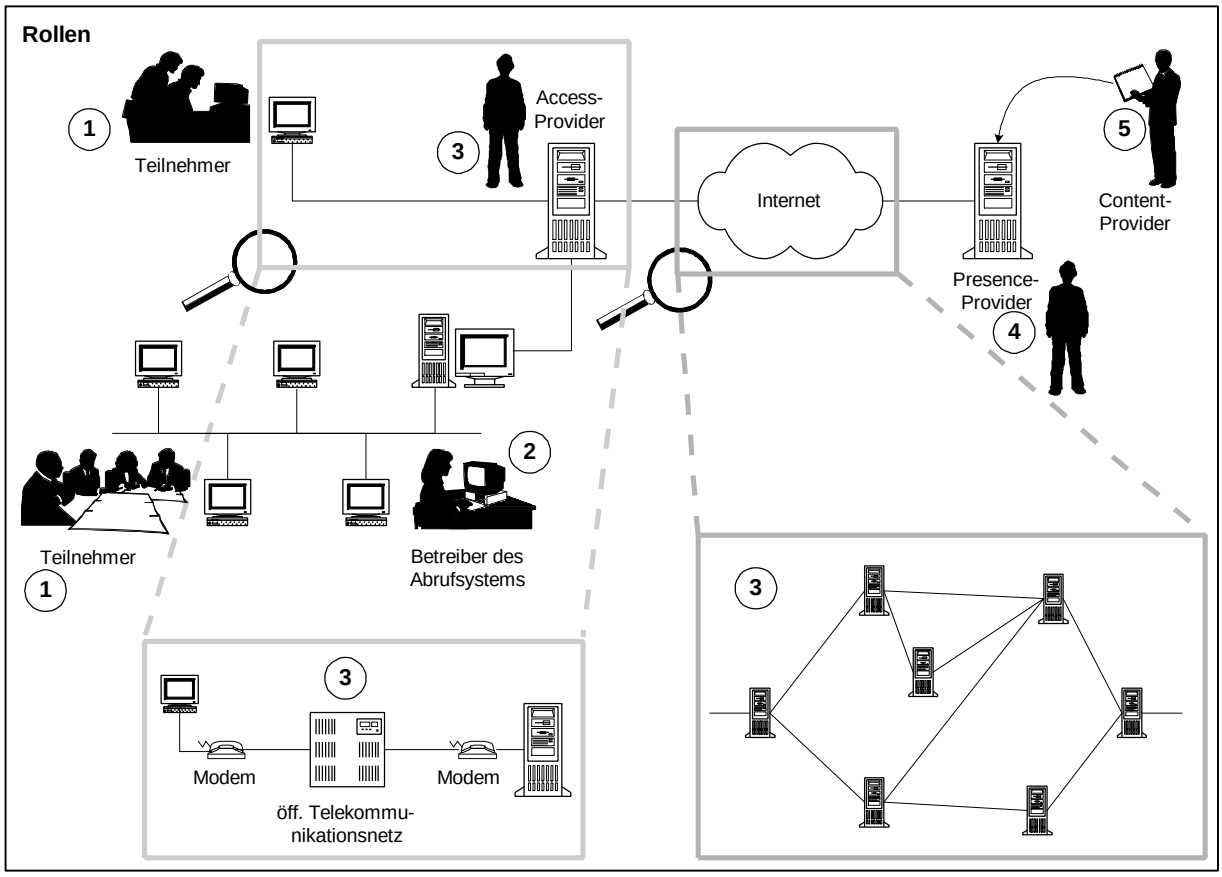

Abb. 1: Rollen im Internet

1. Teilnehmer

Der Teilnehmer nutzt verschiedene Dienste des Internet von einem lokalen Rechner aus. Insbesondere tritt der Teilnehmer an dieser Stelle als Rezipient der abgerufenen Inhalte in Erscheinung. Wenn er selbst Inhalte anbietet, erfüllt er in dieser Funktion die Rolle eines Inhaltsanbieters (siehe 5.).

2. Betreiber des lokalen Rechners und andere Nutzer

Häufig haben andere Personen ebenfalls Zugriff auf den Rechner, von denen aus der Teilnehmer die Internet-Dienste nutzt. Dies ist beispielsweise der Fall in lokalen Netzen von Firmen oder Institutionen oder auch im Internet-Café. Hier kann man unterscheiden, ob diese weiteren Nutzer mit eingeschränkten Berechtigungen arbeiten oder die vollständigen Zugriffsrechte haben, wie dies für den Betreiber des Systems typisch ist.

3. Zugangsvermittler (Access-Provider)

Zu den Zugangsvermittlern gehören aus technischer Sicht mehrere Beteiligte: der Internet-Service-Provider oder Online-Dienst-Anbieter, der die Schnittstelle zur Nutzung der

[2] Vgl. *Federrath*, Zur Kontrollierbarkeit des Internet, Zeitschrift für Urheber- und Medienrecht ZUM 43/3 (1999), S. 177-180.

Intnernet-Dienste zur Verfügung stellt, und ggf. zusätzlich Zugangsvermittler, die die Schnittstelle aus einem lokalen Netz zu weiteren Providern betreiben einschließlich etwaiger Proxy-Betreiber. Hinzu kommen die Betreiber der nötigen Internet-spezifischen Infrastruktur, z.B. Router, DNS-Server o.Ä. Auf einer tieferen Ebene im Schichtenmodell[3] liegt die Dienstleistung der Telekommunikationsanbieter, derer sich der Teilnehmer bedient, indem die Verbindung zu den Zugangsvermittlern darüber aufgebaut wird.

4. Diensteanbieter (Presence-Provider, Service-Provider)
Die verschiedenen Internet-Dienste werden von unterschiedlichen Beteiligten erbracht. Ein Beispiel ist das Bereitstellen von Festplattenplatz und Bandbreite auf einem Web-Server, um Inhalte über das World Wide Web zur Verfügung stellen zu können (Webhosting).

5. Inhaltsanbieter (Content-Provider)
Die Content-Provider sind für die eigentlichen Inhalte verantwortlich, die sie mit Hilfe anderer Provider zur Verfügung stellen.

III. Spuren

Im Folgenden wird für die wichtigsten Internet-Dienste dargestellt, welche Informationen an welchen Stellen typischerweise anfallen. Entscheidend ist die Art der Daten, bei denen unterschieden werden kann nach

- Bestandsdaten, die bei den Diensteanbietern (Telekommunikationsanbieter, Access-Provider, Service-Provider) meist im Rahmen eines Vertrags gespeichert sind (z.B. Name, Adresse, Bankverbindung),
- Verbindungsdaten, die Informationen über die Umstände der Telekommunikation geben (z.B. Absender, Empfänger, Datum, Dienst), und
- Inhaltsdaten, die die eigentlichen Nachrichten (E-Mail, News-Artikel, WWW-Anfrage o.Ä.) beinhalten.

Darüber hinaus ist zu betrachten, wie die reguläre Lebensdauer der Daten aussieht, wer welche Möglichkeiten eines Zugriffs darauf hat[4] und wie zuverlässig die Informationen sind (Integrität, Authentizität).

[3] Das standardisierte OSI-Schichtenmodell (Open Systems Interconnection) beschreibt eine Protokollhierarchie zur Datenübertragung in sieben Ebenen. Zur juristischen Abgrenzung von Telediensten und Telekommunikation vgl. *Spindler* in Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Kommentierung zu § 2 TDG Rn. 36 ff., Stand: 1999-01-01.

[4] Generell haben die jeweiligen Betreiber der Systeme aus technischer Sicht Vollzugriff (Lesen, Schreiben, Ändern, Löschen) auf die Daten in ihrem Bereich.

1. World Wide Web (WWW)

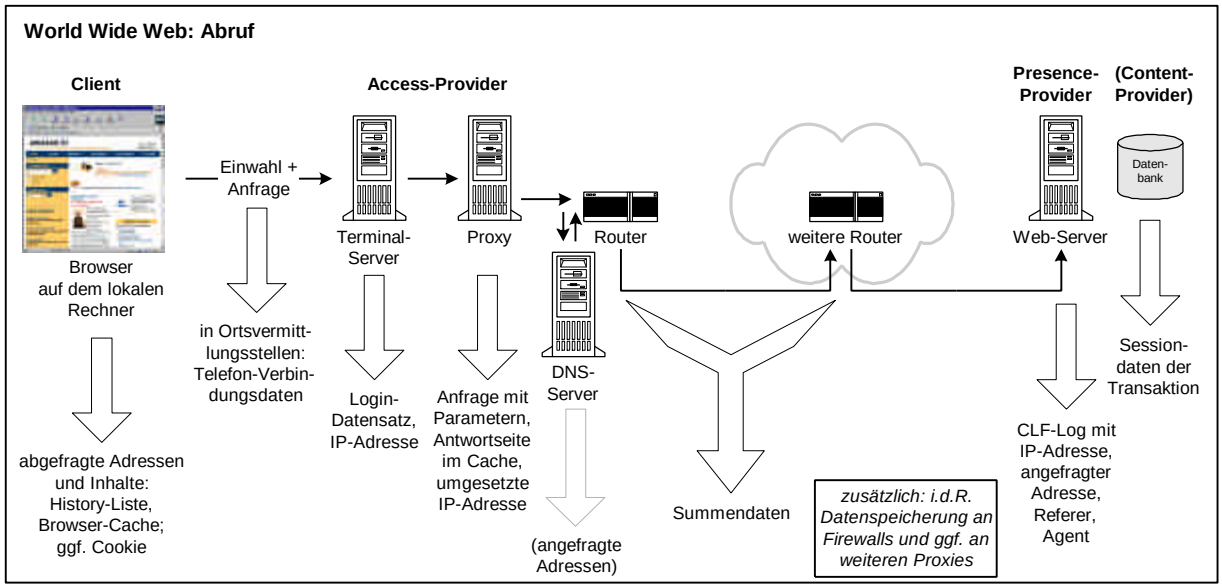

Abb. 2: Datenspuren beim WWW-Abruf

Der Datenfluss beim Abruf von Informationen im World Wide Web wird schematisch in Abb. 2 dargestellt. Exemplarisch für andere Dienste ist dort zusätzlich eingezeichnet, welche Daten für die Einwahl erhoben werden, um Zugang zum Internet zu erlangen.

a) Datenfluss

Auf der Client-Seite arbeitet der Teilnehmer mit einem Internet-Browser, mit dessen Hilfe die WWW-Informationen visualisiert werden. Der Browser ist auf einem Rechnersystem (Einzelplatz- oder vernetztes System) installiert. Für den Internet-Zugang muss sich der Rechner des Nutzers zunächst über die Ortsvermittlungsstellen der Telekommunikations-anbieter bei dem Zugangsrechner (Terminal-Server) seines Access-Provider einwählen und dort mit Hilfe seines Passwortes anmelden. Hierdurch entstehen sowohl Daten bei dem **TK-Provider**[5] als auch Einträge in der Logdatei des **Terminal-Servers** (Login-Name, Datum, Uhrzeit, IP-Adresse). Sofern die Information über die Zuordnung dynamischer IP-Adressen nicht von den Abrechnungsdaten getrennt wird, bleibt sie ebenso lange gespeichert, d.h. in der Regel mehrere Monate lang.

Für die WWW-Anfrage schickt der Browser des Teilnehmers eine Anfrage (Request[6]) an den Proxy (sofern vorhanden), der den Request weiterleitet. Am **Proxy** wird der Request vollständig gespeichert, später beantwortet mit der zugehörigen Antwort des Web-Servers. Ebenso wird hier zwischengespeichert, welche ankommende IP-Adresse durch welche neue IP-Adresse[7] ersetzt wird, um die spätere Antwort an den richtigen Client weiterzuleiten.

[5] Bei ISDN enthält ein Kommunikationsdatensatz u.a. eine Versions- und Satzkennung, die Nummer des anrufenden Anschlusses, die Zielrufnummer, Datum und Uhrzeit von Beginn und Ende der Verbindung, Kennungen über das verwendete Kommunikationsprotokoll, Dienstemerkmale, Transaktionen und Tarife. Näheres siehe AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Arbeitspapier Datenschutzfreundliche Technologien in der Telekommunikation, 1997, http://www.datenschutz-berlin.de/to/tk/ds_tk123.htm.

[6] Der Request enthält die Adresse der Webseite (Uniform Resource Locator, URL).

[7] Hier kann es sich um die eigene IP-Adresse des Proxies handeln, oder es wird eine differenziertere Adressumsetzung (Network Address Translation) vorgenommen. Der angefragte Web-Server sieht nur die neue IP-Adresse und erfährt nichts über die Original-IP-Adresse des Clients.

Sofern eine Auflösung der angegebenen Adresse in eine IP-Adresse notwendig ist, wird diese Information von einem DNS-Server bezogen. An dieser Stelle wird in der Regel nichts außer der Zuordnung von IP-Adressen und Domain-Namen gespeichert. Die Anfrage des Teilnehmers wird über Router an den Web-Server gesandt. Die Router speichern meist Summendaten über die transferierten Datenmengen, anhand derer eine Abrechnung erfolgt.

Am **Web-Server** wird die Anfrage mit weiteren Daten in einer Logdatei gespeichert.[8] Der gängige Minimalstandard für die zu speichernden Informationen wird durch das Common Logfile Format (CLF)[9] definiert, das folgende Datenfelder vorsieht:

- Name oder IP-Adresse des anfragenden Clients
- Logname des Teilnehmers (sofern vom Client aktiviert)
- Username des Teilnehmers bei eingestellter Authentisierung (mit Passwort)
- Request
- Status der Anfrage, der an den Client übermittelt wird
- Länge der übertragenen Webseite

Beispiel:
jay.bird.com - fred [14/Mar/1996:17:45:35 +0000] "GET /~sret1/ HTTP/1.0" 200 1243

Auch erweiterte Logfiles, z.B. mit Informationen über den Referer (Angabe der URL der Webseite, über deren Link der Zugriff erfolgte) und den User-Agent (Browser-Version, oft auch Information über Sprache und Betriebssystem), sind gängig.[10] Hinzu kommen Daten über die Konfiguration des Rechners, z.B. Bildschirmauflösung, installierte Plug-Ins, Akzeptanz von Cookies sowie Aktivierung von ActiveX, Java oder JavaScript.[11] Logfiles an Web-Servern werden oft monatlich aggregiert ausgewertet. Meist werden erst dann die Logfile-Rohdaten gelöscht.

Einige Web-Servern werten das Referer-Feld zu dem Zweck aus, um solche Zugriffe abzulehnen, die über gesetzte Links auf Webseiten der Konkurrenz zum eigenen Angebot

---

[8] Die Protokollierung eingehender Requests durch das World Wide Web Consortium (W3C) sieht verschiedene mögliche Logfiles vor für alle Zugriffe (AccessLog), für Proxy-Zugriffe (ProxyAccessLog), für Cache-Zugriffe (CacheAccessLog) sowie für Fehlerfälle (ErrorLog), siehe "Logging Control In W3C httpd", http://www.w3.org/Daemon/User/Config/Logging.html, Juli 1995. Hinzu kommen CookieLogs o.Ä., siehe beispielsweise Dokumentation des Apache-Web-Servers, http://www.apache.org/docs/mod/mod_log_config.html.

[9] http://www.w3.org/Daemon/User/Config/Logging.html#common-logfile-format.

[10] Beispiele von der "Webserver Logfile Technical Reference", http://www.openwebscope.com/help/logfiletechsheet.html:
Common Logfile Format Extended (NCSA combined):
jay.bird.com - [14/Mar/1996:17:45:35 +0000] "GET /~sret1/ HTTP/1.0" 200 1243
"http://www.statslab.cam.ac.uk/"; "Mozilla/2.0 (X11; I; HP-UX A.09.05 9000/735)"
Microsoft IIS Common:
207.111.105.145, -, 6/8/98, 10:03:20, W3SVC1, WINDOG, 207.111.105.145,
130, 343, 182, 304, 0, GET, /hcsweb/index.html, -,
W3C Standard - Extended Logfile Format (ELF),
Hallam-Baker/Behlendorf, W3C Working Draft WD-logfile-960323, 1996, http://www.w3.org/TR/WD-logfile.html:
#Fields: date time c-ip cs-username s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken s-port cs(User-Agent) cs(Cookie) cs(Referer)
1997-12-01 08:29:50 129.20.88.11 - W3SVC1 PC-BOB 139.30.18.11 GET /Web/UMR653.htm - 200 0 7824 340 11457 80 Mozilla/4.0+(compatible;+MSIE+4.0;+Windows+NT) - -

[11] Man kann selbst überprüfen, welche Daten vom Browser übertragen werden oder unmittelbar vom Server ermittelbar sind, z.B. bei der Privacy-Analyse unter http://privacy.net/analyze/.

erfolgen.[12] Dass die Information des Referer-Feldes an den Web-Server übertragen wird, ist kritisch zu beurteilen:

- Der Server-Betreiber gewinnt Informationen über Interessen und Nutzungsverhalten des Teilnehmers über den Bereich des eigenen Web-Servers hinaus. So wird bei der Verwendung von Suchmaschinen, von denen aus auf die gefundenen Seiten zugegriffen wird, auch die Anfrage selbst durch die Referer-Angabe übermittelt. In dem folgenden Beispiel sind die Suchwörter "Pizza" und "Kiel" und die verwendete Suchmaschine www.google.com im Klartext zu erkennen, die zur Webseite www.pizza-kiel.de geführt haben:

  valiant.koehntopp.de - - [17/Oct/1999:18:42:29 +0200] "GET /www.pizza-kiel.de/pages/ HTTP/1.0" 200 3522 **http://www.google.com/search?q=pizza+kiel** "Mozilla/4.61 [en] (X11; U; Linux 2.2.10 i586)"

  Tatsächlich wurden schon Pläne diskutiert, eigene Webseiten mit verfänglichen Schlüsselwörtern (beispielsweise "Porno"), die gar nicht Inhalt des Angebots sind, in Suchmaschinen eintragen zu lassen und dann die Rechneradressen der dadurch "angelockten" Teilnehmer zu speichern.

- Verwandt ist das Problem, dass sicherheitsrelevante Informationen übertragen werden, z.B. die Kreditkartennummer, wenn aus dem Referer-Eintrag Folgendes hervorgeht:

  https://blah.com/cgi/buy-cd?creditcard=2034872398472340[13]

- Außerdem wird beim Folgen eines externen Links von einer internen Webseite, deren Adresse oder Existenz geheim bleiben soll, die URL im Referer übertragen.[14]

Zwar sieht der Internet-Standard zum Web-Protokoll HTTP (Hypertext Transfer Protocol) vor, dass Informationen wie der Referer-Eintrag optional sein sollen:

"Note: Because the source of a link may be private information or may reveal an otherwise private information source, it is strongly recommended that the user be able to select whether or not the Referer field is sent. For example, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and From information."[15]

Jedoch bieten die heutigen Standard-Browser keine komfortable Möglichkeit, die Übertragung des Referer-Feldes fallweise zu unterbinden oder zuzulassen.[16] Dies bleibt zur Zeit Zusatzsoftware mit Filterfunktionalität vorbehalten.[17]

---

[12] Mailinglist-Beitrag von *Patterson*, Betreff: "Re: confidentiality and the referer field", 1997-06-26, http://www.ics.uci.edu/pub/ietf/http/hypermail/1997q2/0626.html.
[13] Mailinglist-Beitrag von *Holtman*, Betreff: "Re: confidentiality and the referer field", 1997-07-01, http://www.ics.uci.edu/pub/ietf/http/hypermail/1997q3/0004.html.
[14] Mailinglist-Beitrag von *Hallam-Baker*, Betreff: "confidentiality and the referer field", 1997-06-26, http://www.ics.uci.edu/pub/ietf/http/hypermail/1997q2/0616.html.
[15] *Fielding/Gettys/Mogul/Frystyk/Berners-Lee*, Hypertext Transfer Protocol -- HTTP/1.1, RFC 2068, Abschnitt 14.37, 1997, http://ietf.org/rfc/rfc2068.txt.
[16] Beispielsweise ist es im Netscape-Communicator ab Version 4 zum Unterdrücken der Referer-Angabe notwendig, in der Konfigurationsdatei prefs.js den Eintrag "user_pref("network.sendRefererHeader", false);" hinzuzufügen.
[17] Z.B. Internet Junkbuster (FAQ siehe unter http://www.junkbusters.com/ht/en/ijbfaq.html) oder diverse PC-Firewalls.

Sofern die Daten für die Webseite dynamisch aus Datenbankinhalten generiert werden, wie dies im Bereich der Webshops, Newsticker und Suchmaschinen gängig ist, können Transaktionsdaten von der **Datenbank** mitprotokolliert werden. Hier ein Beispiel eines Datensatzes mit Authentisierungs- und Adressinformationen:

```
$this->in = "";
$this->pt = array();
$this->pt["auth"] = "1";
$this->pt["order"] = "1";
$this->pt["challenge"] = "1";
$GLOBALS["auth"] = new Poe_Challenge_Auth;
$GLOBALS["auth"]->auth = array();
$GLOBALS["auth"]->auth["uid"] = "fb89048f1bff2d27b759158708848bc3";
$GLOBALS["auth"]->auth["uname"] = "kris";
$GLOBALS["auth"]->auth["perm"] = "admin";
$GLOBALS["auth"]->auth["exp"] = "940179155";
$GLOBALS["challenge"] = "7301d4eae4ae2657c794b69f78e33718";
$GLOBALS["order"]["name"] = "Kristian Köhntopp";
$GLOBALS["order"]["street"] = "Knooper Weg 46";
$GLOBALS["order"]["city"] = "24103 Kiel";
$GLOBALS["order"]["email"] = "kk@netuse.de";
```

Nachdem der Request bei dem Web-Server angekommen ist, wird die angefragte Seite über die Router und den Proxy an den Client zurückgeschickt. Auf dem Proxy-Rechner wird die Antwortseite im Cache zwischengespeichert, um weitere Anfragen danach schneller bedienen zu können.

Weitere Daten fallen auf dem **Client-System** an, bei denen ebenfalls die abgerufenen Informationen nicht nur kurzfristig im Arbeitsspeicher, sondern auch im Browser-Cache (meist ein Bereich auf der lokalen Festplatte) zwischengespeichert werden. Außerdem wird eine Liste mit den zuletzt besuchten Adressen geführt ("History"). Zusätzlich bleiben oft Spuren in dem Verzeichnis, das vom Betriebssystem für temporäre Dateien vorgesehen ist.[18] Wenn dort nicht besondere Zugriffsbeschränkungen implementiert sind, können Unberechtigte auf die Daten zugreifen.[19] Aus diesem Grund wird Vorsichtigen empfohlen, zum einen Browser- und Arbeitsspeicher-Cache auszuschalten, zum anderen die Daten aktiv vor Beenden des Programms zu löschen.[20]

b) Cookies, Session-IDs und Web-Bugs

Um feststellen zu können, welchen Weg Teilnehmer durch die Webseiten auf dem eigenen Server nehmen, werden verschiedene Mechanismen eingesetzt:

---

[18] Z.B. Bericht über einen Browserfehler, dass Formulardaten im TEMP-Verzeichnis verbleiben: Netscape's Form-Handling in Communicator 4.5 Compromises Security, 1999-02-02, http://www.skylab.org/netscape/index.html.

[19] Beispielsweise Zugriff auf im Browser-Cache hinterlegte Webseiten aus passwortgeschützten Bereichen: *Rapoza/Kerstetter*: Security bug in IE 5.0 uncovered, PC Week Online, 1999-05-04, http://www.zdnet.com/pcweek/stories/news/0,4153,1014586,00.html.

[20] *Perske*, Mangelnde Sicherheit von WWW-Programmen, 1999-10-12, http://www.uni-muenster.de/WWW/Sicherheit.html. Weitere Fehler und Sicherheitsrisiken von Browsern hat *Kubaitis* dokumentiert: WWW Browser Security & Privacy Flaws, http://www.cen.uiuc.edu/~ejk/browser-security.html.

Cookies[21] sind Einträge in der Datei COOKIES.TXT oder im Verzeichnis COOKIES auf dem Rechner des Teilnehmers, die von dem Server generiert und beim nächsten Zugriff wieder an ihn übermittelt werden. Sie enthalten die folgenden Informationen:

- Domain, die den Cookie gesetzt hat und lesen kann
- Information, ob alle Computer der Domain Zugriff auf den Cookie haben
- Pfad der Domain, in der der Cookie gültig ist
- Information, ob ein Cookie-Zugriff nur bei SSL-Verbindung (verschlüsselt) möglich ist
- Zeitangabe für die Lebensdauer des Cookies
- Name des Cookies
- Wert des Cookies (oft eine Identifikationsnummer)

Beispiele:

```
nike.rz.uni-konstanz.de  FALSE  /  FALSE  915148800  BEISPIELTEXT  Das_ist_bei_Ihnen_gespeichert
.microsoft.com           TRUE   /  FALSE  947433000  MC1           GUID=30853a5de5b61d08b60802b
```

Cookies können persistent (auf Dauer) angelegt sein, oder aber sie können sich gleich nach Beenden des Browsers wieder löschen[22]. Die persistenten Cookies sind aus Datenschutzsicht aus verschiedenen Gründen kritisch:[23]

- Der Cookie-Mechanismus ist bei der Standardkonfiguration der gängigen Browser wenig transparent. Der Teilnehmer wird nicht über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Datei informiert.

- Cookies können dazu dienen, Profile über Teilnehmer anzufertigen, um z.B. gezielte Werbung einzublenden. Sofern sich ein Nutzer beispielsweise im Rahmen einer Bestellung irgendwann einmal auf den Webseiten identifiziert, kann man diese Personendaten dem Abrufprofil zuordnen.

- Da Cookies lokal auf der Festplatte ohne besonderen Zugriffsschutz abgespeichert sind, sollte man vermeiden, dort Personendaten oder Passwörter abzulegen.

Der Teilnehmer kann Cookies in den meisten Browsern deaktivieren oder sich eine Warnung vor dem Annehmen von Cookies anzeigen lassen. Außerdem lassen sich die Cookie-Dateien schreibschützen oder die Inhalte manuell oder mit Hilfe spezieller Zusatzprogramme löschen.

---

[21] FAQs zu Cookies: http://www.cookiecentral.com/faq.htm; Setzen eines Cookies: http://privacy.net/cookies/.
[22] Ein Beispiel für temporäre Cookies findet sich auf den Seiten des Bundesministeriums für Wirtschaft und Technologie: http://www.bmwi.de/cookie.html.
[23] Vgl. *Moore/Freed*, Use of HTTP State Management, Network Working Group Internet Draft, Dezember 1999, http://www.ietf.org/internet-drafts/draft-iesg-http-cookies-02.txt.

Session-IDs[24] in URLs sind in ihrer Funktionsweise mit temporären Cookies vergleichbar. Beim Zugriff auf eine Webseite erhält der Teilnehmer eine bestimmte Nummer zugewiesen, die als Teil der Adresse beim Verfolgen von Links im eigenen Angebot mitgeführt und auch in der Anzeige der Adresse im Browser dargestellt wird. Im folgenden Beispiel ist die Session-ID als der Teil nach dem Fragezeichen im Request zu erkennen:

200.39.96.149 - - [17/Oct/1999:18:45:16 +0200] "GET
/index.php3?**Poe_Session=a8a796174d6771432c57aa346012b949** HTTP/1.0" 200 5105
"http://www.php.net/links.php3" "Mozilla/4.61 [en] (X11; I; Linux 2.2.13-7mdk i686)"
200.39.96.149 - - [17/Oct/1999:18:45:19 +0200] "GET /phpower.jpg HTTP/1.0" 200 2351
"http://phplib.netuse.de/index.php3?Poe_Session=a8a796174d6771432c57aa346012b949" "Mozilla/4.61 [en]
(X11; I; Linux 2.2.13-7mdk i686)"
200.39.96.149 - - [17/Oct/1999:18:45:19 +0200] "GET /mysqlpower.gif HTTP/1.0" 200 708
"http://phplib.netuse.de/index.php3?Poe_Session=a8a796174d6771432c57aa346012b949" "Mozilla/4.61 [en]
(X11; I; Linux 2.2.13-7mdk i686)"
200.39.96.149 - - [17/Oct/1999:18:45:19 +0200] "GET /shopower.jpg HTTP/1.0" 200 1395
"http://phplib.netuse.de/index.php3?Poe_Session=a8a796174d6771432c57aa346012b949" "Mozilla/4.61 [en]
(X11; I; Linux 2.2.13-7mdk i686)"

Die Gültigkeit dieser Nummern wird zeitlich begrenzt, indem bei der Generierung ein Zeitstempel einfließt. Durch Verwenden einer Hashfunktion (z.B. MD5) mit einer Zufallszahl sind die Nummern nicht ratbar.

Hinter den **Web-Bugs**[25] oder **Clear GIFs** stecken transparente GIF-Bilder, die normalerweise 1x1 Pixel groß sind. So ein Web-Bug wird von einem dritten Server geladen, also weder vom Rechner des Abrufers noch dem des Anbieters. Der Anbieter www.anbieter.de baut dazu in seine Seite http://www.anbieter.de/zaehlwas.html das folgende HTML-Kommando ein:

<img src="http://www.dritter.de/bug-www.anbieter.de-code-17.gif" width=1 height=1 border=0>

Bei jedem Zugriff auf die Seite zaehlwas.html von www.anbieter.de wird nun auch das angegebene Bild von www.dritter.de geladen, wodurch ein Eintrag in der Logdatei von www.dritter.de, komplett mit Referer, User-Agent, IP-Adresse, Uhrzeit und Cookies, generiert wird. Der Web-Bug kann ebenfalls selbst Cookies setzen, die dann – da ausgehend von dem Dritten – auch nur an www.dritter.de zurückgesandt werden.

Web-Bugs sind von dem Abrufer nicht zu erkennen, es sei denn, er untersucht den Quelltext der HTML-Seite. Man kann HTML auch in E-Mails verwenden – tatsächlich wurden insbesondere in Werbe-E-Mails bereits Web-Bugs eingesetzt. Mit ihrer Hilfe lässt sich erkennen, ob und wann die Nachricht geöffnet wurde, sofern eine Online-Verbindung zum Internet besteht.

c) Lesezeichen beim Internet Explorer

Im Microsoft-Browser Internet Explorer 5.0 wurde eine Funktion eingeführt, damit die Web-Server in der Bookmark-Liste (Favoriten) des Teilnehmers neben den Eintrag der URL automatisch ein Piktogramm setzen können.[26] Damit lässt sich standardmäßig durch den

---

[24] *Hallam-Baker/Connolly*, Session Identification URI, W3C Working Draft WD-session-id-960221, 1996, http://www.w3.org/TR/WD-session-id.

[25] *Smith*, The Web Bug FAQ, Version 1.0, 1999-11-11, http://www.tiac.net/users/smiths/privacy/wbfaq.htm; *Rötzer*, Nach den Cookies die Web Bugs, Telepolis, 1999-11-14, http://www.heise.de/tp/deutsch/inhalt/te/5482/1.html.

[26] Hierfür nur die Datei Favicon.ico ins Hauptverzeichnis des Web-Servers stellen. Näheres bei *Oakes*, Another Privacy Hole in IE 5.0?, Wired, 1999-04-16, http://www.wired.com/news/news/technology/story/19160.html.

Web-Server abfragen, ob ein solcher Nutzer die Seite in der Liste der Lesezeichen hat, und damit auf das besondere Interesse des Teilnehmers an der Site schließen. Der Nutzer kann diese Funktion nicht deaktivieren.

d) "Neben der Spur"

Neben der eigentlich angefragten Seite bei einem Betreiber können auch andere Provider eine Rolle spielen:

Viele Webseiten finanzieren sich über **Bannerwerbung**. Der Abrufer einer solchen Seite erhält die Banner, indem sein Browser zusätzlich zu dem Werbeanbieter eine HTTP-Verbindung aufbaut. Dem Anbieter stehen damit über den Referer und über mit den Bannern verteilte Cookies weitere Informationen zur Verfügung, aus denen er Abruf- und Interessensprofile gewinnen kann.[27] Da die Angebote großer Bannerwerbefirmen wie z.B. DoubleClick auf sehr vielen Websites vertreten sind, bekommen diese Anbieter siteübergreifend umfassende Profile über Teilnehmer.[28]

Einige Webseiten funktionieren über eine Umleitung (**Redirect**). Dies ist praktisch, wenn beispielsweise die Site physisch umgezogen ist. Allerdings muss man sich bewusst sein, dass auch der Betreiber der ursprünglich angewählten Seite Zugriffsinformationen protokollieren kann.

Bei Aktivieren der **Smart-Browsing**-Funktion "What's Related" des Netscape Communicators (ab Version 4.06) werden die angegebenen Webadressen an einen zentralen Server übermittelt, der mit Vorschlägen verwandter Websites reagiert. Zusätzlich kommen Cookies zum Einsatz. So lassen sich ebenfalls Interessensprofile anlegen.[29]

In der Diskussion um den Einsatz von Filtermechanismen für mehr Jugendschutz im Internet gibt es Pläne, Webinhalte durch Einstufungen in bestimmten Kategorien zu klassifizieren (Rating). Einige Ansätze beinhalten Pläne für "**Labeling Bureaus**", bei denen die Einstufungen dritter Parteien (Third-Party-Rating) abrufbar sein sollen. An diesen Stellen könnte ebenfalls – ggf. sogar mit Authentisierungsinformationen, damit Jugendliche das System an dieser Stelle schwerer umgehen können – eine Vielzahl von Webadressen bezogen auf einzelne Teilnehmer gesammelt werden.[30]

Um die eigenen Systeme gegen Angriffe aus dem Internet zu schützen, haben die meisten Provider **Firewalls** installiert, die unerwünschte Kommunikation herausfiltern sollen. Damit Angriffe erkennbar sind, ist die Protokollierungsfunktion der Firewalls von großer Bedeutung. Auf den Firewalls werden also weitere Informationen zu dem Zweck gespeichert, um die

---

[27] Gegen solche "Third Party Cookies" kann man sich durch entsprechende Konfiguration seines Browser schützen, z.B. im Netscape Communicator durch die Einstellung "Nur an den ursprünglichen Server zurückgesendete Cookies akzeptieren".

[28] Nach Berichten der Zeitung USA Today (*Rodger*, Activists charge DoubleClick double cross, 2000-01-25, http://www.usatoday.com/life/cyber/tech/cth211.htm) befinden sich die Cookie-setzenden Banner von DoubleClick auf 11.500 Websites. Demnach plant die Firma eine Verkettung der Cookie-Informationen mit den Datensätzen der Direktmarketingfirma Abacus Direct Corp., die von DoubleClick übernommen wurde. Die Datenbank von Abacus soll Namen, Adressen und Informationen über das Kaufverhalten von 90 % der US-amerikanischen Haushalte umfassen. So lässt sich für die Cookies in vielen Fällen der Personenbezug herstellen.

[29] *Curtin/Ellison/Monroe*, What's Related? – Everything But Your Privacy, Version 1.5, 1998-10-07, http://www.interhack.net/pubs/whatsrelated/.

[30] *K. Köhntopp/M. Köhntopp*, Why Internet Content Rating and Selection does not work, Version 1.2, 1999-09-26, http://www.koehntopp.de/kris/artikel/rating_does_not_work/.

Datensicherheit zu gewährleisten.[31] Teilweise wird an diesen Systemen temporär die gesamte Kommunikation mitgeschnitten, bis entschieden werden kann, dass die übertragenen Daten nicht Teil eines Angriffes sind. Ebenso können weitere Proxies (auch Anonymisierungsdienste mit Adressumsetzung) verwendet werden, an denen ebenfalls Daten anfallen.

2. E-Mail

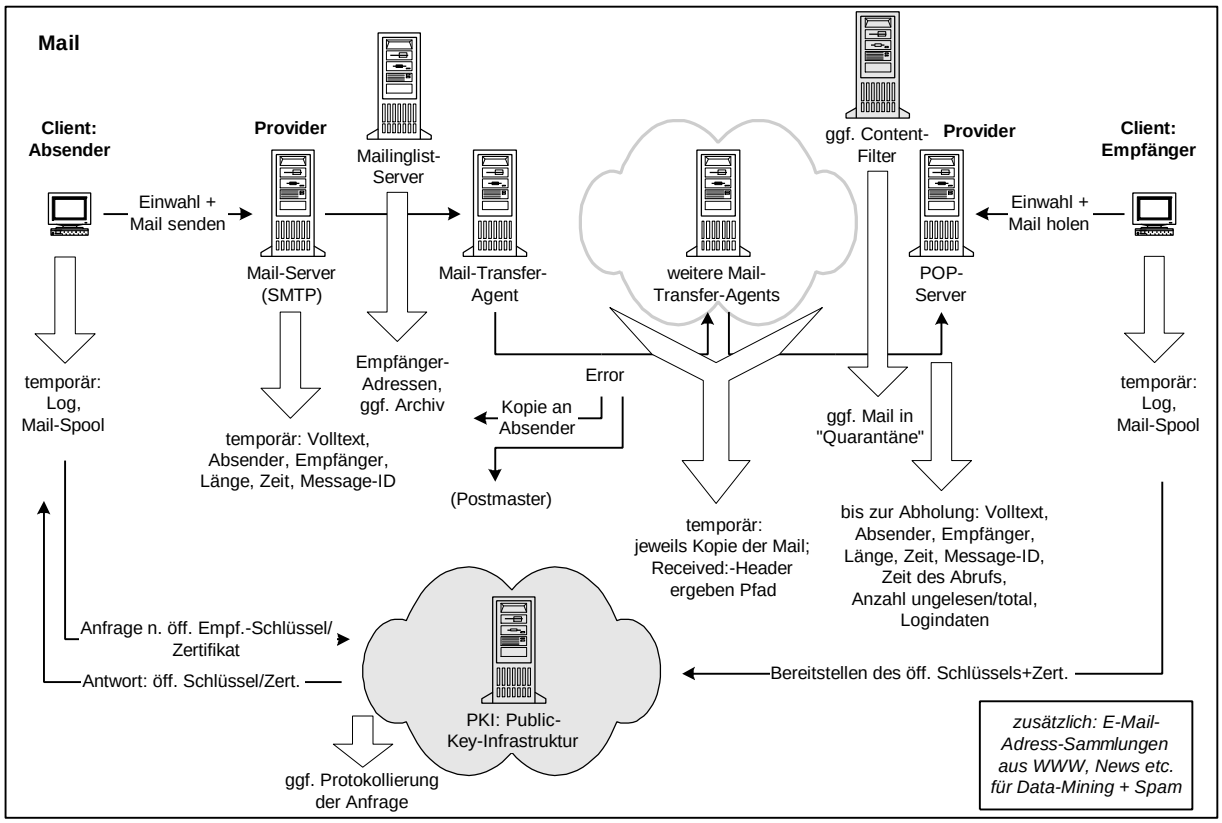

Abb. 3: Datenspuren beim Austausch von E-Mails

E-Mails durchlaufen beim Transport durch das Internet viele Stationen, bei denen unterschiedliche Daten gespeichert werden (siehe Abb. 3).

a) Datenfluss

Auf dem Client-System des Absenders liegt die Nachricht als Ganzes vor. Beim Versand gelangt sie über ein spezielles Mail-Verzeichnis (Mail-Spool) zum Mail-Server, der die Nachricht an den nächsten Mail-Transfer-Agent (MTA) schickt. Von dort gelangt sie über weitere MTAs, die jeweils die Mail für eine kurze Zeit zwischenpuffern und den Kopf (Header) der Nachricht um einen Received-Eintrag ergänzen, zu einem weiteren Server (POP: Post Office Protocol), von dem sie der Empfänger aus einem für ihn vorbereiteten Speicherbereich abholen kann. Der POP-Server speichert bis zum Abholen der E-Mail (oder je nach Vertragsgestaltung auch länger) den Volltext der Nachricht einschließlich dem Kopf, der Informationen enthält über Absender- und Empfängeradressen, Betrefftext, Länge der Nachricht, Datum und Uhrzeit der Erstellung, eine eindeutige Kennzeichnung sowie den Pfad, den die Mail zurückgelegt hat. Außerdem protokolliert er die Logindaten (das Passwort wird

[31] *M. Köhntopp/M. Seeger/L. Gundermann*, Firewalls – Konzept, Design und Aufbau, Verlag Computerwoche, 1998, S. 75 ff.

oft im Klartext übertragen) des Empfängers, die Zeit des Mailabrufs sowie die Anzahl der ungelesenen und insgesamt vorhandenen Nachrichten für den Empfänger.

Falls die Mail nicht zustellbar war, z.B. wegen eines Fehlers bei der Adressierung, bekommt der Sender in der Regel eine Fehlermeldung sowie eine Kopie seiner Nachricht zurückgesandt. Der für die E-Mail zuständige Betreiber (Postmaster) des Systems, das den Fehler festgestellt hat, kann ebenfalls darüber informiert werden. Aufgrund der Vielzahl von Meldungen ist dies jedoch meist nicht der Fall, oder er erhält lediglich die Header-Informationen der betroffenen Mail, um ggf. den Fehler beseitigen zu können.

Einige Empfänger-Systeme verwenden einen vorgeschalteten Inhaltsfilter, der insbesondere verhindern soll, dass E-Mails mit Viren oder Trojanischen Pferden in das System gelangen. Statt dessen können die Nachrichten zunächst in ein Quarantäne-Verzeichnis gestellt werden, wo versucht werden kann, den bösartigen Code zu entfernen, wenn die Mail nicht gelöscht werden soll. Es lassen sich auch Fehlermeldungen an Absender, Empfänger oder Postmaster generieren.[32]

Künftig wird es vermutlich zu einem vermehrten Einsatz von Verschlüsselung und digitalen Signaturen bei E-Mails kommen. Hierfür werden zur Zeit Public-Key-Infrastrukturen (PKI) aufgebaut. An den Servern solcher Institutionen fallen Daten darüber an, wer welche öffentlichen Empfänger-Schlüssel(zertifikate) abruft oder nachprüft, so dass hier die potentiellen Kommunikationspartner ermittelbar sind.

b) Mailinglists

Eher öffentlichen Charakter haben Mailinglists, bei denen E-Mails an einen Verteiler von Interessierten geschickt werden. Zu diesem Zweck gibt es besondere Mailinglist-Server mit eigenen Betreibern. Die Nachrichten an die Mailinglist werden an den Server adressiert, der sie anschließend an seinen Verteiler weiterschickt. Mit der Digest-Funktion werden die Nachrichten eine gewisse Zeit zwischengespeichert, um dann aus den Einzelmails eine Sammelmail an die Empfänger zu generieren. Auf den Mailinglist-Servern ist das Verteiler der eingetragenen Empfänger gespeichert. Darüber hinaus bieten einige Listen ein Archiv der bisher versandten Nachrichten, ggf. auch mit einem Web-Gateway, an.

c) Mail-Adressen

E-Mail-Adressen werden auch außerhalb des eigentlichen Mail-Austausches gesammelt, weil sie als Absenderkennung in News-Artikeln eingetragen sind oder bei Webseiten angegeben werden. Dadurch sind sie oft mit zusätzlichen Daten über die Person verbunden und werden beispielsweise nach Interessensgebieten geordnet an Werbetreibende vermarktet.

Ähnlich den Web-Proxies, die für eine Adressumsetzung genutzt werden, gibt es für den Mail- und News-Dienst Remailer, die die Absenderadresse durch eine neue Adresse ersetzen können. Einige Remailer pseudonymisieren die Information über den Absender, in dem sie eine Datenbank mit der Zuordnung zwischen angegebener und neuer Adresse führen, so dass Rückantworten über den Remailer zugestellt werden können. Andere anonymisieren die Nachrichten, ohne dass sie Informationen über eine Zuordnung speichern.[33]

[32] Zur Problematik von Content-Filtern für E-Mail siehe auch *Köhntopp/Seeger/Gundermann*, S. 81 ff. (FN 23).
[33] Eine Übersicht findet sich unter http://www.iks-jena.de/mitarb/lutz/anon/.

3. News

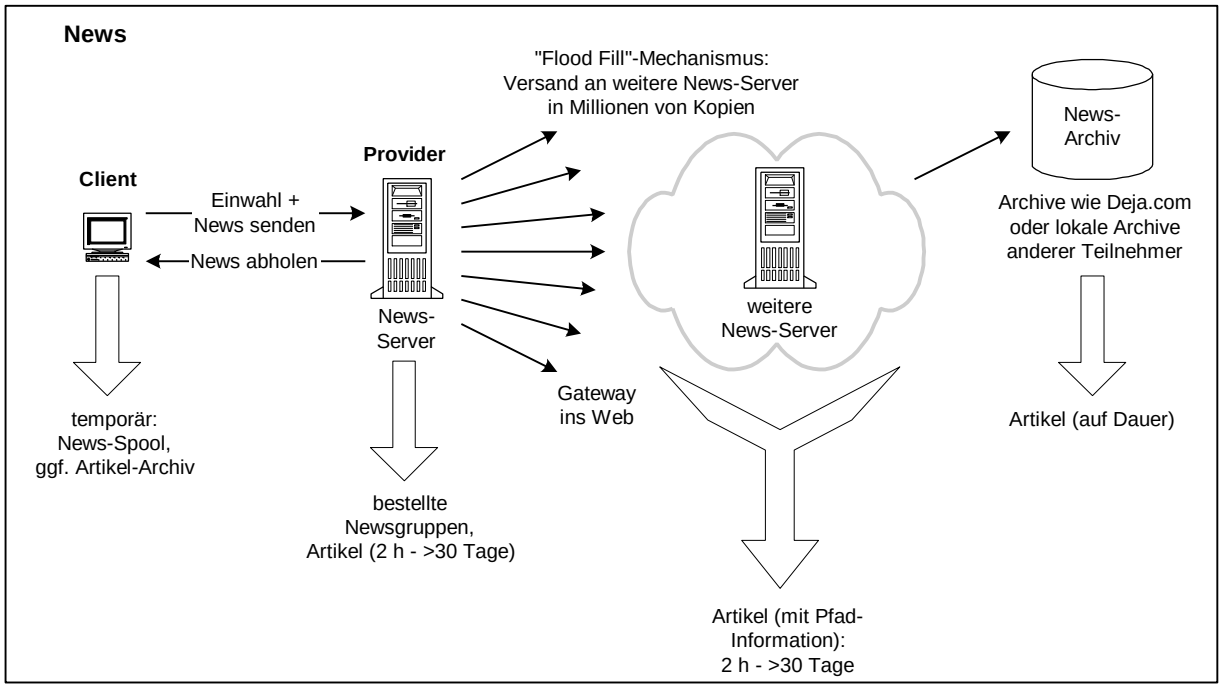

Abb. 4: Datenspuren beim Austausch von News

a) Datenfluss

Der News-Dienst betrifft im Gegensatz zur privaten E-Mail öffentliche Artikel (Postings), die in bestimmten, fachlich unterschiedenen Foren (Newsgroups) zum Abruf bereitgestellt werden (siehe Abb. 4). Auf dem lokalen System können Nachrichten temporär (zum Versand) zwischengespeichert oder auch in einem Archiv für längere Zeit abgelegt werden. Da News-Postings im Gegensatz zu Mails keine Empfängerangabe haben, werden sie ungerichtet verteilt.

Der Provider führt auf dem News-Server eine Liste mit den Newsgruppen, die der Teilnehmer bestellt hat. Ebenso ist dort vermerkt, welche Artikel bereits abgeholt bzw. als gelesen markiert sind. Die eigentlichen Postings werden in der Regel wegen der großen Datenmengen nicht dauerhaft gespeichert, sondern haben eine konfigurierbare Lebensdauer, häufig im Bereich von etwa 2 Stunden bis 30 Tagen. Jeder eingelieferte Artikel wird durch den "Flood Fill"-Mechanimus an eine Vielzahl von anderen News-Servern weitergesandt, die jeweils eine Kopie davon bei sich speichern und zum Abruf bereithalten.

b) Archive

Zusätzlich gibt es News-Archive wie Deja.com, die es mit Hilfe einer großen Datenbank ermöglichen, per WWW auch nach länger zurückliegenden Postings zu recherchieren. Wenn man im Header oder in der ersten Zeile eines Artikels "X-No-Archive: Yes" angibt, nehmen "höfliche" Archivdienste das so gekennzeichnete Posting nicht in ihre Datenbank auf.

Aus dem Header eines News-Artikels gehen die folgenden Informationen hervor: Absenderadresse, Newsgroups, Betrefftext, Erstellungsdatum und –zeit, Organisation, Länge des Artikels und Daten über den Rechner, auf dem das Posting eingespeist wurde, sowie über den Übertragungsweg.

4. Internet Relay Chat (IRC)

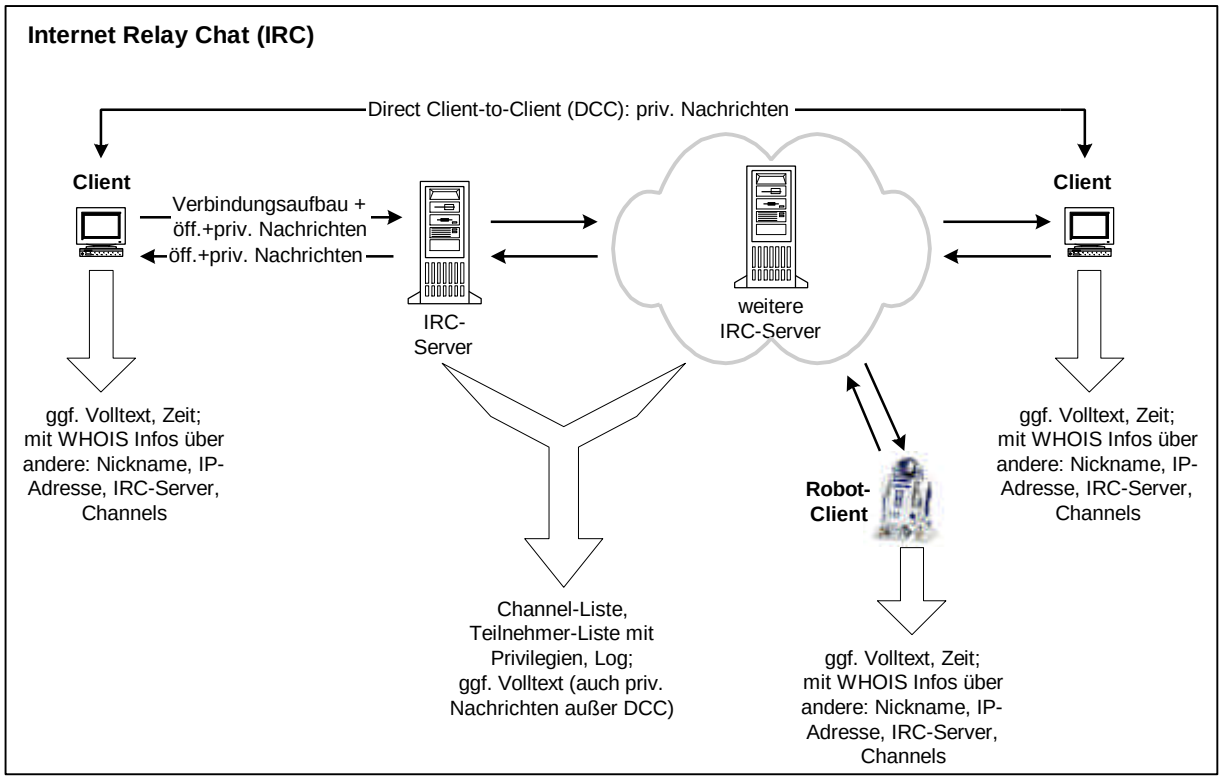

Abb. 5: Datenspuren im Internet Relay Chat

Verschiedene Chatdienste werden im Internet oder in Online-Diensten genutzt, z.B. ICQ ("I seek you") oder AIM (AOL Instant Messenger). Der ursprüngliche und immer noch weit verbreitete Chatdienst im Internet ist IRC (Internet Relay Chat). Bezüglich der Datenspuren (siehe Abb. 5) ähneln sich die Dienste.

a) Datenfluss

Typisch für das Auftreten in Chatrooms (in IRC-Terminologie: Channel) ist die Wahl eines Pseudonyms (Nickname) durch den Nutzer. Mit dem /whois-Kommando kann man sich von anderen Teilnehmern die IP-Adresse, den Nutzernamen (oft konfigurierbar, z.B. in der Umgebungsvariable IRCMORPH) und den Rechnernamen, von dem aus der Zugriff erfolgt, anzeigen lassen. Allerdings sind auch IP-Adresse und Rechnername nicht unbedingt authentisch, z.B. wenn der Dienst über ein Webinterface (wie http://www.chatsystems.com) genutzt wird.

Es gibt zwei verschiedene Möglichkeiten, die Nachrichten im IRC zu adressieren:

- über den IRC-Server: Hier werden öffentliche (an alle Teilnehmer des Channels) und private Nachrichten (an einen ausgezeichneten Teilnehmer mit Hilfe des /msg-Kommandos) über den IRC-Server geschickt. Damit sind diese Nachrichten prinzipiell immer für den Betreiber des Servers und die IRC-Operator sichtbar.

- direkt: Mit dem /dcc-Kommando (Direct Client-to-Client) kann man unabhängig vom IRC-Server eine Verbindung zu einem anderen Teilnehmer über den üblichen Weg im

Internet etablieren und so private Nachrichten versenden, die dem Betreiber und den IRC-Operatorn verborgen bleiben.

Auf dem IRC-Server können Betreiber und IRC-Operator neben der normalen öffentlichen und privaten (ausgenommen: /dcc) Kommunikation auch die angebotenen Channels und die Teilnehmerkennungen mit den ihnen zugewiesenen Berechtigungen sehen.

b) Robots

Außer menschlichen Teilnehmern sind Programme, sog. IRC-Robots, im Einsatz, die z.B. dazu dienen, automatisch Berechtigungen an Teilnehmer zu vergeben und einen Channel auch bei Abwesenheit des Operators aufrechtzuerhalten. Ebenso wie diese können sie den gesamten Volltext der ausgetauschten Nachrichten gemäß ihren Berechtigungen (d.h. ggf. mit erweiterten Rechten auch die private Kommunikation zwischen anderen Teilnehmern, die über den IRC-Server per /msg abgewickelt wird) speichern.

5. Globally Unique Identifier (GUID)

Bereits bei den Cookies findet sich der Wunsch, die Teilnehmer (bzw. ihre Rechner) über (weltweit) eindeutige Kennungen, Globally Unique Identifiers (GUID), zu identifizieren. Solche Kennungen können in Hardware, in Software oder in Diensten implementiert sein:

- Im Januar 1999 wurde bekannt, dass Intel im Prozessor Pentium III eine eindeutige Seriennummer, die PSN (Processor Serial Number), eingebaut hat, die sich per Software abfragen lässt.

- Die Firma Microsoft verwendet GUIDs, die Informationen über die pro Netzkarte eindeutige MAC-Adresse (Media Access Control) beinhalten. So wird dem Nutzer beispielsweise bei der Online-Registrierung von Windows 98 eine GUID zugeteilt, die in der Registry-Datenbank des Systems abgelegt wird. Auch in Office-Dokumenten ist eine GUID wie Word, Excel oder Powerpoint enthalten, in einigen Fällen wurde sie ebenfalls über das Mail-Programm Outlook verbreitet.[34]

- GUIDs kommen außerdem bei der Abspielsoftware (Media-Player) von Microsoft und RealNetworks[35] sowie bei der Software der Firma Comet Systems, mit deren Hilfe man das Cursor-Aussehen verändern kann[36], zum Einsatz.

- Das neue IP-Protokoll IPv6 sieht im jetzigen Planungsstadium vor, dass in allen Datenpaketen Informationen über die eindeutigen Netzkarten-Adressen (MAC) eingebaut werden. Dann würden alle Teilnehmer, die das Internet über ein lokales Netz nutzen, entsprechende Spuren hinterlassen.[37] Ende 1999 wurde diskutiert, inwieweit das internationale Gremium für Internet-Standards IETF (Internet Engineering Task Force)

---

[34] *Persson/Siering*, Big Brother Bill, c't 6/99, 16, http://www.ix.de/ct/99/06/016/; *Oakes*, Sniffing Out MS Security Glitch, Wired, 1999-05-08, http://www.wired.com/news/news/technology/story/18331.html.
[35] *Anderson*, GUID Vibrations, Kommentar in ABCNEWS, 1999-04-16, http://abcnews.go.com/sections/tech/NextFiles/nextfiles990419.html.
[36] Associated Press, Cursor Software Monitors Customers, 1999-11-29, http://www.nytimes.com/aponline/f/AP-Internet-Privacy.html.
[37] *Krempl*, Aus dem Nebel ins Glashaus, Spiegel Online 30/1999, 1999-07-29, http://www.spiegel.de/netzwelt/technologie/0,1518,33327,00.html.

darüber hinaus auch Abhörmöglichkeiten in die Protokolle integrieren soll.[38] Zumindest die Einführung von Standards, die ausschließlich dem Abhören dienen, wurde inzwischen abgelehnt, doch ist fraglich, ob dieser Beschluss der Techniker auf Dauer zu halten ist.[39]

IV. Zusammenfassung und Ausblick

Der Nutzer im Internet hinterlässt im Normalfall eine breite Datenspur.[40] Diese vielfältigen Informationen sind in der Regel auf diverse Betreiber und Rechner verteilt, so dass nicht jeder die Daten zu einem Profil verdichten oder gar einer Person zuordnen kann. Allerdings gibt es für jemand, der Zugriff darauf erlangt, diverse Möglichkeiten, diese Daten zu verketten. Dazu können z.B. Marketing-Firmen, Geheimdienste oder auch Hacker, die Sicherheitslücken ausnutzen, gehören. Da die hinterlassenen Daten nicht in jedem Fall authentisch sein müssen, wird von einigen Firmen versucht, über zusätzliche Mechanismen wie GUIDs Teilnehmer bzw. Rechner eindeutig zu kennzeichnen.

Wegen der riesigen Menge an anfallenden Protokolldaten gilt für die meisten Provider, dass sie nur diejenigen Informationen zwischenspeichern, die notwendig sind, um den jeweiligen Dienst erbringen und abrechnen zu können. Eine undifferenzierte Speicherung auf Vorrat, wie sie teilweise von Sicherheitsbehörden gewünscht wird, können die Provider schon wegen fehlender Kapazitäten nicht für die Masse der Teilnehmer realisieren. Darüber hinaus widerspräche es den elementaren Anforderungen des Datenschutzes.

Danksagung

Die Autoren danken Hannes Federrath, Lukas Gundermann und Andreas Pfitzmann für eine kritische Durchsicht des Textes und konstruktive Anmerkungen. Außerdem haben wir uns sehr über die Verbesserungsvorschläge von Clemens Fuchslocher gefreut.

[38] *Rötzer*, Die IETF überlegt, ob sie Abhörmöglichkeiten in Standards integrieren soll, Telepolis, 1999-10-13, http://www.heise.de/tp/deutsch/inhalt/te/5373/1.html.
[39] *Rötzer*, Standardisierungsgremium für das Internet sagt Nein zu Abhörprotokollen, Telepolis, 1999-11-13, http://www.heise.de/tp/deutsch/inhalt/te/5481/1.html.
[40] Es gibt allerdings Möglichkeiten, weniger Datenspuren zu hinterlassen. Selbstschutzmechanismen werden beispielsweise dargestellt in *Federrath/Pfitzmann*, Neue Anonymitätstechniken, Datenschutz und Datensicherheit DuD 22/11 (1998), S. 628-632.