In diesem Kapitel:

- Verräterische Daten
- Abhörbarkeit von Kommunikationsinhalten
- Proxies
- Provider
- Juristische Aspekte und staatliche Abhörsysteme

KAPITEL 9

Anonymität

Je intensiver Sie sich mit dem Internet beschäftigen, desto häufiger werden Sie auf den Begriff *Anonymität* treffen. Warum ist dieser Begriff im Internet von so zentraler Bedeutung? Ist man im riesigen, unstrukturierten Netz nicht ohnehin anonym? Wie Sie in diesem Kapitel sehen werden, ist das nur auf den ersten Blick der Fall.

Jede Einwahl, jede E-Mail und jeder Besuch einer Webseite hinterlässt für lange Zeit eindeutige Spuren. Neben den Crackern sind aber noch andere Instanzen damit beschäftigt, persönliche Daten zu sammeln und auszuwerten. Im Einzelnen handelt es sich dabei um Betreiber von Diensten (WWW, E-Mail, FTP etc.), Internetprovider, aber auch um staatliche Institutionen sowie fremde Staaten. Seit dem 11. September 2001 ist gerade Letzteres zu einem ernsthaften Problem im Hinblick auf unsere vermeintliche Informationsfreiheit und den Datenschutz geworden.

Wir wollen uns zunächst mit der Frage beschäftigen, welche Daten überhaupt gesammelt werden können und faktisch gesammelt werden. Anschließend werden wir uns genauer mit dem Einsatz von Proxies als Schutzmöglichkeit und des Weiteren mit dem Staat als Akteur der Überwachung befassen.

Verräterische Daten

In diesem Abschnitt wollen wir uns zum einen mit der Frage auseinander setzen, welche Daten überhaupt abgehört werden können, und zum anderen damit, welche Rückschlüsse diese übertragenen Daten auf Sie und Ihr Verhalten zulassen. Dabei ist es wichtig, immer im Hinterkopf zu behalten, welche Akteure beteiligt sind. Einem Mailprovider stehen beispielsweise viel weniger Daten zur Verfügung als dem Internetprovider oder dem Staat. Allen Informationen ist aber gemeinsam, dass sie, gespeichert und richtig ausgewertet, wichtige Informationen über den Surfer preisgeben. Natürlich stellt sich dabei sofort die Frage, wer überhaupt an diesen Daten interessiert ist.

Es gibt verschiedene Gründe, warum jemand versuchen könnte, Daten aus dem Internet zu sammeln: Zunächst existieren rechtliche Vorgaben, denen zufolge z.B. Provider die Zuordnung von dynamischen IP-Adressen zu konkreten Benutzern eine gewisse Zeit lang archivieren müssen. Online-Shops hingegen interessieren sich vor allem für die Möglichkeit, anhand des Surfverhaltens der User Benutzerprofile zu erstellen, um beispielsweise Werbung flexibler und individueller gestalten zu können. Ein Cracker wiederum braucht Angaben, die ihm der Browser oder das Mailtool liefern, als Ansatzpunkt für einen erfolgreichen Hack. Zu diesen Angaben zählen z.B. Informationen über die verwendete Software, das Betriebssystem des Rechners, die Browser-Plugins, die eingestellte Sprache und die Auflösung des Bildschirms. Auch Wirtschaftsspionage ist ein wichtiges Motiv der Datenjäger und -sammler. Dieser Punkt wird zurzeit besonders heiß diskutiert, da sich die Gerüchte verdichten, dass der Datenverkehr europäischer Unternehmen aus Übersee eifrig mitgelesen wird und daraus enorme Nachteile für die hiesige Wirtschaft entstehen. Mit diesen staatlichen Abhörmaßnahmen werden wir uns in einem späteren Abschnitt beschäftigen.

Manch einem wird das Ausspähen sensibler Inhalte an sich schon unangenehm erscheinen, richtig problematisch wird es aber erst dadurch, dass durch die IP-Adresse ein Bezug zwischen den Daten und einer Person hergestellt werden kann. Dies ließe sich wohl am besten mit dem Verlust des Hausschlüssels vergleichen. Wenn Sie Ihren Schlüssel irgendwo in einer fremden Stadt verlieren, ist das natürlich ärgerlich. Sie müssen aber nicht mit einem Einbruch rechnen, da der Finder des Schlüssels Ihren Wohnort nicht kennt. Verlieren Sie hingegen Ihre Aktentasche samt Schlüssel und Papieren, sieht die Situation anders aus, denn jetzt kann dem Schlüssel ein Wohnort zugeordnet werden und ein Einbruch wird möglich. Genauso verhält es sich mit den Daten im Netz: Sind sie mit keiner Adresse und mit keinem Namen in Verbindung zu bringen, sind sie wertlos, egal zu welchem Zweck sie gesammelt wurden. Interessant wird die Datensammlerei dann, wenn sich ein Profil erstellen lässt, d.h., wenn ein konkretes Surfverhalten entweder mit Besuchen auf anderen Webseiten oder gar mit einem Namen verbunden werden kann.

Allen angesprochenen Akteuren ist daher gemeinsam, dass sie im Zuge der Aufzeichnung als Erstes versuchen, Ihre IP-Adresse auszulesen und somit Ihren Computer eindeutig zu identifizieren. Sind Sie über eine feste IP-Adresse mit dem Internet verbunden, reicht bereits diese Information aus, um alle gesammelten Daten mit Ihnen in Verbindung zu bringen. Wählen Sie sich hingegen bei einem Provider ein, der Ihnen eine dynamische Adresse zuweist,[1] gestaltet sich die Zuordnung der IP-Adresse zum Benutzer wesentlich schwieriger. In diesem Fall können Ihre Handlungen nur bis zum Einwahl-Provider zurückverfolgt werden. Der Beobachter kann also nur eine Aussage in der folgenden Form erhalten: Jemand, der bei T-Online Kunde ist, war auf einer bestimmten Webseite oder hat eine E-Mail geschrieben.

1 Dies ist bei den meisten Modem-, ISDN- und DSL-Benutzern der Fall.

Wer sich jetzt in trügerischer Sicherheit wiegt, sei jedoch gewarnt, denn mittels geschickter Analyse gelangt ein ernsthaft interessierter Spion oder Shopbetreiber meistens trotzdem ans Ziel. Dazu kann z.B. ein Online-Shop, der Benutzerprofile erstellen möchte, die IP-Adresse eines Surfers mit einem Cookie auf dessen Festplatte abspeichern. Beim nächsten Besuch des Users (mit einer anderen IP-Adresse) wird der Cookie ausgelesen, und so kann festgestellt werden, dass dieser Benutzer bereits einmal auf der Webseite gewesen ist. Setzt der Shopbetreiber nun diese alte Adresse mit der Aktivitätentabelle der eigenen Datenbank in Bezug, kann er die jetzigen Handlungen des Surfers mit den vorherigen in Verbindung bringen. Auf den ersten Blick ist zwar ersichtlich, dass man damit eine sehr genaue Verhaltensdatenbank eines Benutzers erstellen kann, aber die Verknüpfung zur eigentlichen Person fehlt immer noch.

Da man aber davon ausgehen kann, dass ein Surfer, der eine Webseite häufiger besucht, auf Dauer persönliche Spuren hinterlässt, ist das Verfahren dennoch äußerst wirksam. Irgendwann einmal wird der User eine Bestellung auf der Internetseite vornehmen oder einen Gästebucheintrag mit seinem Namen unterschreiben. Selbst eine E-Mail an den Webmaster oder die Teilnahme am Chat mit einem Spitznamen verrät die nun noch nötigen persönlichen Daten. Hat man erst einmal eine Verknüpfung zwischen der fraglichen IP-Adresse und einer konkreten Person hergestellt, braucht man nur noch mittels der Cookies und der eigenen Datenbank die gesammelten Erkenntnisse mit der Person zu verbinden, und das Profil ist fertig. In Kombination mit weiteren Taktiken wie z.B. Mail-Maulwürfen kann man auf diese Weise sehr schnell zu zuverlässigen und vor allem detaillierten Benutzerinformationen kommen. Da die IP-Adresse aber nach wie vor von zentraler Bedeutung ist, wollen wir uns im Abschnitt »Proxies« eingehend mit ihrer Tarnung beschäftigen.

Wie Sie sehen, ist also auch eine dynamische IP-Adresse kein Garant für Ihre Anonymität. Zudem dürfen Sie nicht vergessen, dass es mit Hilfe zahlreicher fortgeschrittener Lösungen sehr wohl möglich ist, innerhalb einer einzigen Online-Sitzung genug Daten über den Surfer zusammenzutragen. Neben der IP-Adresse als Basis werden auch andere Daten genutzt. Dazu zählen die Informationen, die Ihr Browser oder das E-Mail-Tool sowohl über sich selbst als auch über das Betriebssystem preisgibt (siehe dazu den Abschnitt »Browserkonfiguration prüfen« in Kapitel 5, *Browser – einer für alles*) sowie die eigentlichen Übertragungsinhalte. Hierzu zählen im Einzelnen Informationen über die Art des Browsers oder Mailtools, die an Ihrem Computer eingestellte Auflösung, Farbtiefe und Sprache sowie das installierte Betriebssystem und die vorhandenen Browser-Plugins. Neben dem Effekt, dass diese Daten zur Erstellung eines Profils gebraucht werden können, sind sie für potenzielle Angreifer unerlässlich, um einen Ansatzpunkt für einen erfolgreichen Hack zu finden.

Abschließend wollen wir uns ein weniger bekanntes, aber sehr eindrucksvolles Beispiel anschauen, wie sich Benutzer im Internet eindeutig identifizieren lassen. Die IP-Adresse ist für die Adressierung im Internet und in lokalen TCP/IP Netzen

zuständig, doch dies ist nur die halbe Wahrheit. Wie Sie in Kapitel 2, *Technische Hintergründe*, gelesen haben, bauen Netzwerkstacks auf mehreren Schichten auf. Unterhalb der IP-Schicht gibt es ein weiteres Adressierungsverfahren, das sich auf so genannte MAC-Adressen (Media Access Control) stützt. Im Gegensatz zu den IP-Adressen, die softwareseitig durch den Benutzer, Administrator oder von einem zentralen Server auf Betriebsystem vergeben werden und nur im öffentlichen Bereich eindeutig sind, sind die 48 Bit großen MAC-Adressen hardwareseitig und eindeutig jeder einzelnen Netzwerkkomponente[2] auf der Welt zugeordnet. Jede MAC-Adresse kommt also nur einmal vor und verrät zugleich etwas über den Hersteller des Produkts. Die Netzwerkhardware von Asus beginnt beispielsweise immer mit »00-11-D8«.

Um Ihre eigene MAC-Adresse herauszufinden (wenn Sie über mehr als eine Netzwerkkomponente verfügen, werden für jede Komponente alle Daten aufgelistet), brauchen Sie unter Windows nur den Befehl `ipconfig /all` in die Eingabeaufforderung einzugeben.[3] Möchten Sie anschließend den Hersteller ermitteln, genügt es, die ersten sechs Stellen der Adresse unter *http://standards.ieee.org/regauth/oui/* einzutippen.

Eigentlich spielt die MAC-Adresse nur im lokalen Netz eine Rolle und dürfte daher im Internet gar nicht auftauchen. Ein Internetserver, dessen Webangebot Sie besuchen, kann zwar Ihre IP-Adresse ermitteln (diese braucht er ja, um mit Ihrem PC zu kommunizieren), er bekommt die weltweit eindeutige MAC-Adresse jedoch nicht zu Gesicht. Unverständlicherweise bietet die Standardkonfiguration von Windows dennoch eine Möglichkeit, an diese Daten zu gelangen. Wenn das so genannte NetBIOS-Protokoll über TCP/IP aktiviert ist, können Computer aus dem Internet über TCP/IP auf die NetBIOS-spezifischen Daten Ihres PCs zugreifen. Dazu gehört beispielsweise der Computername, die Arbeitsgruppe, aber eben auch die MAC-Adresse. Tatsächlich brauchen Sie in den meisten Fällen NetBIOS garnicht bzw. es liegt nicht in Ihrem Interesse, dass es nach außen kommunizieren kann.

Ist der Angreifer oder der Shopbetreiber in der Lage, diese eindeutige Adresse auszulesen, ist er in der Lage, Sie an jedem Ort der Welt und unter jedem Account zu erkennen. Da er das angeschlossene Netzwerkgerät eindeutig zuordnen kann, spielt es keine Rolle mehr, ob Sie sich aus dem Urlaub oder von zu Hause aus mit Ihrem Notebook ins Internet einwählen, und ob sie als Benutzer des Online-Shops angemeldet sind oder nicht. Es ist ein leichtes für den Shop-Betreiber, Sie zu identifizieren.

Wie Sie sich vorstellen können, bietet dies eine Unmenge weiterer Möglichkeiten zur Erstellung von Benutzerprofilen oder Vorbereitung von Angriffen. Mit spezieller

2 Dabei kann es sich um alle möglichen netzwerkfähigen Geräte wie etwa WirelessLAN-Stick, Bluetooth-Adapter, Netzwerkkarten oder Router handeln.

3 Geben Sie dazu unter `Start/Ausführen` den Befehlt `cmd` ein. Daraufhin öffnet sich eine Box mit der Windows-Eingabeaufforderung (Kommandozeile), in die Sie nun wiederum den Befehl `ipconfig /all` eintippen und mit Return bestätigen. Die MAC-Adresse trägt unter Windows den nicht ganz unpassenden Namen »Physikalische Adresse«.

Software ist es jedoch möglich, die eigene MAC-Adresse zu fälschen. Dies hat jedoch nur dann Sinn, wenn Sie die gefälschte Nummer immer und immer wieder aufs Neue in eine andere Nummer abändern, und ist daher unpraktikabel und zudem im heimischen Netzwerk problematisch.

Es empfiehlt sich daher vielmehr, NetBIOS über TCP/IP komplett zu deaktivieren. Dazu klicken Sie im Fall von Windows XP auf START → SYSTEMSTEUERUNG → EINSTELLUNGEN → NETZWERKVERBINDUNGEN auf die Netzwerkkomponente, mit der Sie ins Internet gelangen (siehe Abbildung 9-1) – bei DSL-Nutzern ist das meist die Netzwerkkarte oder das DSL-USB-Modem. Öffnen Sie per Rechtsklick deren Eigenschaften. Wählen Sie nun im Dialogfenster EIGENSCHAFTEN den Reiter NETZWERK aus, markieren Sie die Checkbox INTERNETPROTOKOLL(TCP/IP) und klicken Sie dann auf den Button EIGENSCHAFTEN. Dort angelangt, müssen Sie zunächst ERWEITERT und anschließend den Reiter WINS wählen. Haben Sie sich durch all diese Menüs durchgehangelt, ist noch der Radiobutton auf NETBIOS ÜBER TCP/IP DEAKTIVIEREN zu setzen. Nach dem Bestätigen durch OK sind Sie auf der sicheren Seite.

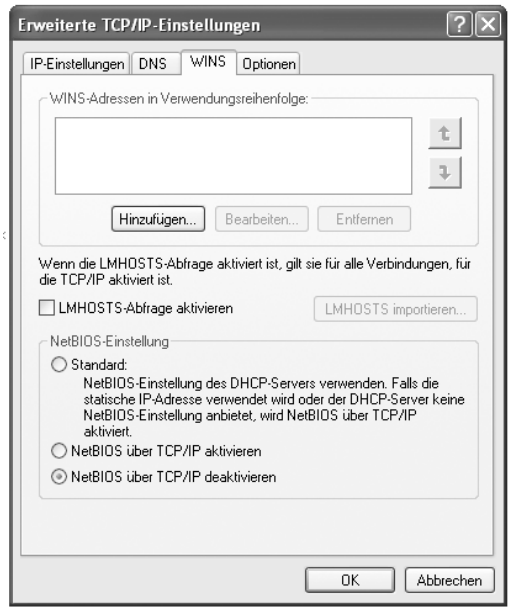

Abbildung 9-1: NetBIOS über TCP/IP deaktivieren

Wenn Sie nun den Test durchführen, den wir im Abschnitt »Shields Up!« in Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, vorgestellt haben, werden diese Einstellungen geprüft. Dort sollten nun weder der Rechnername noch die MAC-Adresse zu sehen sein. Erstaunlicherweise blocken einige Firewalls NetBIOS-Anfra-

gen nicht, und selbst Router sind nicht zwangsläufig sicher, wenn sie beispielsweise von Spielern im DMZ-Modus betrieben werden.[4]

Abhörbarkeit von Kommunikationsinhalten

Wie Sie in Kapitel 2, *Technische Hintergründe*, und speziell im Hinblick auf E-Mails in Kapitel 6, *E-Mail – wer liest mit?*, gelesen haben, gelangen Informationen nicht direkt von einem Computer zum anderen, sondern werden über mehrere, zum Teil dutzende Zwischenstationen transportiert. Dabei müssen Sie sich immer vor Augen halten, dass theoretisch jede dieser Stationen die Daten kopieren und somit auch auswerten könnte, ohne dass Sie es bemerken. Das Prinzip des Internets beruht darauf, dass die Server und Router auf dem Weg des Datenpakets als vertrauenswürdig eingestuft werden können. Dem ist aber definitiv nicht so, da ja im Prinzip jede Person einen Server betreiben kann, der als eine solche Zwischenstation dient. Gerade im Fall von E-Mail wird hier das ganze Ausmaß der Gefahr ersichtlich, da der ganze Inhalt auf einigen Servern zwischengelagert wird.

Ein anderes häufig zitiertes Beispiel ist der bereits in Kapitel 8, *Weitere Internetdienste*, beschriebene Dienst *Telnet*. Da im Fall des unsicheren Telnet die Account-Daten auch noch im Klartext übertragen werden, kann jede der Zwischenstationen nicht nur in den Besitz Ihrer Zugangsdaten gelangen, sondern auch noch die ganze Sitzung mitlesen. Dies wird als *Man-in-the-Middle-Angriff* bezeichnet und ist prinzipiell für jegliche Kommunikationssituation im Internet denkbar. Der Name rührt daher, dass der Angreifer an einer Position zwischen der Quelle und dem Ziel, also in der Mitte des Kommunikationswegs, sitzt. So ließe sich beispielsweise auch ein Chat, eine Passwortabfrage auf einer Webseite oder ein verschicktes MS Word-Dokument mitprotokollieren. Wie Sie sehen, sind Ihre Daten im Internet also keinesfalls sicher, sondern auf einer bestimmten Anzahl von Rechnern stets zugänglich.[5]

Die Abhörmöglichkeiten beschränken sich jedoch keineswegs auf Aktivitäten im WWW oder andere Zugriffe auf entfernte Rechner. Wie bereits mehrfach angedeutet, stellen »Angriffe« von Mitmenschen aus dem direkten räumlichen Umfeld zahlenmäßig die größte Gefahr da. Wenn Sie z.B. beruflich in einem Netzwerk arbeiten, haben auch Ihre Kollegen die Möglichkeit, Ihren gesamten Datenverkehr mitzulesen und dadurch an wichtige persönliche Informationen zu gelangen. Unterschätzen Sie die Neugier von Systemadministratoren nicht!

4 Ein kleines Experiment mit ca. 20 verschiedenen Windows-Rechnern in unterschiedlichen Konfigurationen und Umgebungen (sowohl Privat- als auch Firmencomputer) lieferte jedoch das Ergebnis, dass die Mehrheit der gängigen Sicherheitsmaßnamen die Anzeige der MAC-Adresse und des Computernamens wirkungsvoll unterdrückt (also keine NetBIOS-Anfragen nach außen hin beantwortet).

5 Ein Ausweg wäre es, sämtliche Daten nur über verschlüsselte VPN-Verbindungen zu verschicken.

Schauen wir uns dies anhand eines kurzen Beispiels an. Nehmen wir an, dass die Computer in dem Netzwerk über einen so genannten *Hub* miteinander verbunden sind. Das entspricht der Situation, wie man sie gewöhnlich in kleineren Firmen- oder Heimnetzwerken vorfindet, in größeren Netzen ist der Aufbau aber vergleichbar. Stark vereinfacht könnte man sagen, dass es sich bei einem Hub um ein Gerät handelt, an das alle Computer per Kabel angeschlossen sind und das die Nachrichten im Netz verteilt. Das Problem des Hubs liegt nun genau in dieser Funktion als Verteiler, denn tatsächlich verschickt der Hub alle ankommenden Datenpakete an alle Netzteilnehmer, unabhängig davon, ob sie überhaupt Ziel der Nachricht waren. Die einzelnen PCs prüfen das Datenpaket anschließend und verwerfen es, wenn es nicht für sie bestimmt ist. Jede Netzwerkkarte lässt sich nun aber auch in den so genannten *Promiscuous Mode* setzen, in dem sie die ankommenden Pakete nicht verwirft, sondern an die oberen Netzwerk-Layer weiterleitet. Mit einem der vielen frei im Internet verfügbaren Analyse-Tools kann man die so ankommenden, eigentlich nicht für den eigenen PC bestimmten Datenpakete in Echtzeit mitlesen und auf diese Weise Informationen aus dem ganzen Netzwerk sammeln. Wenn nun beispielsweise ein Kollege in der Mittagspause eine Internetseite ansurft, landet eine Kopie sowohl der Anfrage des Browsers als auch der Antwort des Webservers auf Ihrem Rechner. Einige Tools sind sogar darauf spezialisiert, diese Daten direkt an den eigenen Browser zu schicken, so dass man wirklich das Gleiche sieht wie der Kollege nebenan. So genannte *Switches* können in solchen Fällen die Sicherheit erhöhen. Im Gegensatz zu Hubs senden sie die Daten jeweils nur an den Zielrechner, doch auch hier lassen sich mit einigen Tricks (*ARP-Spoofing*) und den richtigen Programmen die Daten zu einem Angreifer umleiten.

Nachdem wir nun die Abhörmöglichkeiten im globalen und lokalen Netz beleuchtet haben, müssen wir noch einen abschließenden Blick auf den eigenen Rechner werfen. Das sicherste Passwort und die stärkste Verschlüsselung bringen nichts, wenn ein Keylogger auf Ihrem Computer still und heimlich jeden Tastendruck protokolliert. Inzwischen setzen Würmer und Trojaner daher verstärkt auf diese Logger und gelangen so viel einfacher an die gewünschten Daten. Um die so aufgezeichneten Protokolle dem Angreifer verfügbar zu machen, kann ein Schädling sie per E-Mail versenden oder an einen speziellen Chatroom leiten. Wir werden uns in Kapitel 10, *Viren, Würmer und Trojaner*, eingehender mit solchen Taktiken befassen.

Ein weiteres Beispiel für die nahezu unbegrenzten Abhörmöglichkeiten kommt aus dem Gebiet der Funkkomponenten. So konnte in der Zeitschrift *c't* gezeigt werden, dass es möglich ist, die Tastatureingaben von Funktastaturen auch noch in einigen Metern Entfernung aufzuzeichnen und auf diese Weise an wichtige Informationen zu gelangen. Ein wirksames Tool, um sich vor dem Ausspionieren des eigenen Rechners zu schützen, haben wir mit GnuPG bereits kennen gelernt; in Kapitel 7, *E-Commerce und Online-Banking*, haben wir zudem mit HTTPS eine Möglichkeit kennen gelernt, mit der man Webinhalte sicher übermitteln kann.[6]

6 Gegen Keylogger sind beide Ansätze jedoch machtlos.

Als Fazit bleibt zu sagen, dass man – wenn man das Mitlesen der Kommunikationsinhalte nicht mittels Verschlüsselung verhindern kann – wenigstens versuchen muss, die Verknüpfung von Daten und Benutzern zu verschleiern. Was uns zum Thema Proxies bringt.

Proxies

Das Wort *Proxy* bedeutet »Stellvertreter« und trifft eine der Hauptaufgabe eines Proxyservers sehr gut. Dieser versucht nämlich, den User zu tarnen, indem er an dessen Stelle auftritt.[7] Proxies sind meist dienstspezifisch, d.h. nicht jeder Proxy ist für das Vertreten eines beliebigen Dienstes geeignet. Sie werden also einen expliziten Web-Proxy nicht dazu bewegen können, Ihre SMTP-Daten zu übertragen. Auch sind nicht alle Proxies für das anonyme Surfen geeignet, sondern nur diejenigen, die sich nicht transparent verhalten. Es gibt auch generische Proxies, die alle Protokolle verstehen; diese sind jedoch sehr fehleranfällig und daher aus Sicherheitssicht nicht zu empfehlen. Schauen wir uns zunächst die grundsätzliche Funktionsweise eines Proxys an.

Möchte ein Benutzer nicht direkt mit einem Dienst in Kontakt stehen, wendet er sich an einen Proxy. Diesem teilt er nun einerseits mit, wer er selbst ist, und andererseits, mit wem er gern Kontakt aufnehmen möchte. Der Proxy baut nun eine Verbindung zu dem gewünschten Dienst auf und liefert die von dort erhaltenen Informationen an den Benutzer zurück. Dem angefragten Dienst scheint es aber so, als ob der Proxy der eigentliche Endpunkt der Kommunikation wäre. Er weiß also gar nicht, dass dieser nur als Stellvertreter auftritt. Die Daten, die der Dienst über den anfragenden PC einholen kann, sind demzufolge auch nur die des Proxys und nicht die des wirklichen Benutzers. Dies lässt sich besonders gut an der IP-Adresse demonstrieren.

Eine Person möchte unbemerkt auf einer Webseite surfen. Sie wendet sich an einen Web-Proxy, der an ihrer Stelle die Verbindung zu dem Webserver aufbaut und die gewünschten Daten anfordert. Da diese Anforderung vom Proxy ausgeht, wird an den Server auch nur dessen IP-Adresse übermittelt, und er wird auch nur diese in seinen Protokolldateien vermerken. Sind die Daten auf dem Proxy angekommen, leitet er diese wiederum an die IP-Adresse des Surfers weiter. Zwischen dem Client des Besuchers und dem Webserver besteht also zu keinem Zeitpunkt eine direkte Verbindung. Vielmehr gibt es jetzt zwei einzelne, voneinander unabhängige Kommunikationswege: Zum einen der Weg vom Benutzer zum Proxy, zum anderen die Verbindung vom Proxy zum Webserver. Wenn der Betreiber einer Webseite nun

7 Dies ist nicht die einzige und möglicherweise auch nicht die wichtigste Aufgabe eines Proxys, jedoch die für uns hier relevante. Ein Proxy ist eine (Sicherheits-) Komponente, die außer der User-Tarnung auch noch weitere Aufgabe erfüllt: Er kann z.B. als Paketfilter dienen oder als Dokumenten-Cache, um den eigentlichen Server durch die Bereitstellung häufig angefragter Daten zu entlasten.

versucht, einen Besucher anhand seiner IP-Adresse zu identifizieren, wird er nur auf die Adresse des Proxyservers stoßen.

Ein weiteres typisches Beispiel für den Einsatz eines Proxys ist das anonyme Versenden von E-Mails via SMTP. Da bei SMTP-Servern die eigene IP-Adresse in der Mail übertragen wird, können die Spuren der E-Mail im Normalfall bis zum Absender zurückverfolgt werden. Greift dieser aber über einen Proxy auf den SMTP-Server zu, wird in der verschickten Nachricht auch nur die IP-Adresse des Proxys auftauchen. Ein Rückschluss auf den Absender ist dann nicht mehr möglich. Die beiden Übertragungswege sind in Abbildung 9-2 dargestellt.

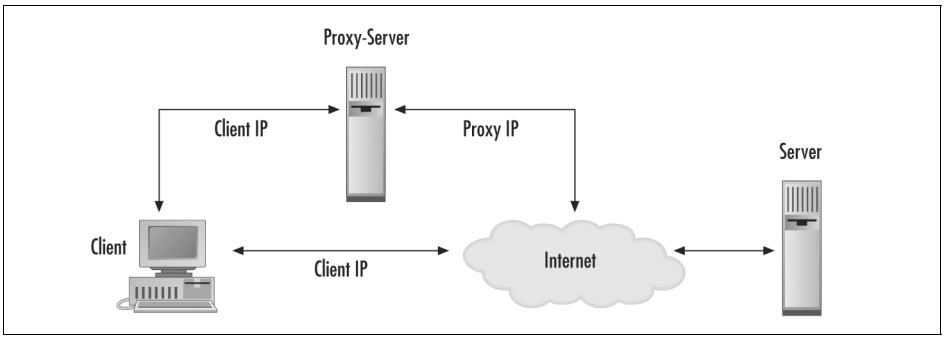

Abbildung 9-2: Die Übertragung der IP-Adresse, mit und ohne Proxy

Der mögliche Schwachpunkt dieses Systems liegt nun darin, dass es Proxies geben könnte, die unseriös oder kompromittiert sind und vom Betreiber benutzt werden, um Daten über den Benutzer zu sammeln. Prinzipiell muss man sich klar machen, dass einem Proxy alle Daten des Benutzers vorliegen (jede besuchte Webseite, jedes dort eingegebene Passwort), so dass sich z.B. aus der Analyse der besuchten Webseiten brauchbare Benutzerprofile erstellen lassen. Sie sollten sich also sicher sein, dass der von Ihnen benutzte Proxy wirklich vertrauenswürdig ist. Darüber hinaus sollten Sie sich aber hinter einem Proxy nicht zu sicher fühlen und bedenken, dass es mit einigen Tricks dennoch möglich ist, an Ihre IP-Adresse zu gelangen, und dass somit den Anonymitätsfunktionen von Proxies – wie allen Sicherheitsvorkehrungen – Grenzen gesetzt sind.

Nachdem wir nun grob die Funktionsweise von Proxies betrachtet haben, werden wir uns im nächsten Abschnitt einem interessanten Programm widmen, das uns das Benutzen wechselnder Proxyserver erlaubt und auf diese Weise das Problem der nicht vertrauenswürdigen Proxies entschärft. Eine Liste interessanter Proxies finden Sie beispielsweise unter *http://www.atomintersoft.com/products/alive-proxy/proxy-list/* oder *http://www.publicproxyservers.com*.[8]

8 Denken Sie bitte daran, einen anonymen Proxyserver auszuwählen, und seien Sie nicht enttäuscht, wenn ein großer Teil der Proxies nicht auf Anhieb mit Ihnen kommunizieren möchte, offline oder sehr langsam ist. Mit etwas Suchen findet sich immer der eine oder andere passende Server.

Proxomitron

Bei dem Tool *Proxomitron* handelt es sich um einen Webfilter mit einigen interessanten Zusatzfunktionen. Im Vordergrund steht hier die Möglichkeit, mittels Proxomitron eine Reihe wechselnder Proxyserver zu benutzen. Das Programm ist Freeware und kann unter *http://www.proxomitron.info/* aus dem Internet heruntergeladen werden; der Download ist mit etwa einem MByte angenehm klein. Eine deutschsprachige Seite mit Tipps und Tricks finden Sie unter *http://www.buerschgens.de/Prox/*. Beide Portale bieten zudem eigene kleine Testwebseiten, mit denen Sie die Einstellungen von Proxomitron testen können.

Neben der Funktion als lokales Proxy-Relais ist Proxomitron auch ein leistungsstarker Filter für Werbebanner und Cookies und kann sogar den HTTP-Header manipulieren. Um den Umfang dieses Kapitels nicht zu sprengen, wollen wir uns hier jedoch nur mit den Proxyfunktionen vertraut machen; schauen Sie sich aber bei Gelegenheit auch die anderen Nutzungsmöglichkeiten an.

Nach der Installation von Proxomitron erscheint in der rechten Ecke der Taskleiste ein grünes Pyramidensymbol, das sich per Doppelklick öffnen lässt. Auf der linken Seite des Hauptfensters, im Fenster ACTIVE FILTER, aktivieren Sie zunächst die Option EXTERNEN PROXY BENUTZEN und klicken dann rechts auf den Button PROXY (siehe Abbildung 9-3). Nun müssen Sie einen oder mehrere Proxies (samt Portnummer z.B: 148.244.150.58:80) auswählen und eintragen (siehe Abbildung 9-4). Es empfiehlt sich jedoch, mittels TEST vorher zu prüfen, ob der Proxy überhaupt ansprechbar und schnell genug ist.

Abbildung 9-3: Das Hauptfenster von Proxomitron

Die Proxyliste muss insgesamt nicht mehr als vier oder fünf Server beinhalten,[9] sollte aber auch nicht zu kurz geraten. Nachdem Sie einige Proxies eingetragen

9 Natürlich erhöht es Ihre Anonymität schon um ein Vielfaches, wenn Sie nur einen festen Proxy nutzen; wir wollen uns hier aber die rotierende Konfiguration ansehen.

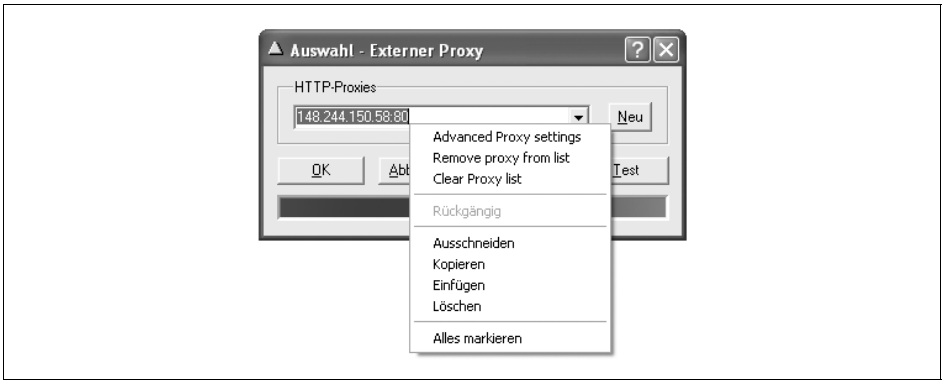

Abbildung 9-4: Die Proxyliste mit Wechselintervall

haben, geht es per Klick auf die rechte Maustaste in das Feld mit den Proxynamen zu den ADVANCED PROXY SETTINGS. Dort können Sie das Zeitintervall (gemessen in Verbindungen) einstellen, in dem Proxomitron automatisch den benutzten Server ändert. Schließen Sie dieses Fenster und verlassen Sie die Proxyliste mit OK, um wieder ins Hauptfenster zu gelangen. Nach dem Schließen und Abspeichern (über das grüne Diskettensymbol) der Konfiguration rutscht Proxomitron wieder als Pyramidensymbol in die Taskleiste zurück und ist einsatzbereit. Bevor es jedoch losgehen kann, müssen Sie Ihrem Browser mitteilen, dass Sie nun über einen Proxyserver surfen möchten.

Internet Explorer

Zu den nötigen Einstellungen für den Internet Explorer gelangen Sie über das Menü EXTRAS und den Befehl INTERNETOPTIONEN. Dort wählen Sie die Registerkarte VERBINDUNGEN und klicken auf die Schaltfläche für die LAN-EINSTELLUNGEN. In dem daraufhin erscheinenden Dialogfeld setzen Sie ein Häkchen bei PROXYSERVER und tragen in das darunter liegende Feld LOCALHOST und als Port 8080 ein. Über die Schaltfläche ERWEITERT könnten Sie zudem noch Internetseiten bestimmen, die direkt (also ohne den Weg über den Proxy) besucht werden sollen. Nachdem Sie dem Browser auf diesem Weg mitgeteilt haben, an wen er sich mit seinen HTTP-Requests wenden soll, können Sie mit dem Surfen beginnen. Stellt sich einer der verwendeten Proxies als besonders langsam heraus, kann es passieren, dass eine Anfrage ausläuft und der Browser eine Fehlermeldung liefert. In diesem Fall sollten Sie diesen Proxy einfach aus der Liste löschen und einen anderen auswählen.

Firefox

Um bei Firefox zu den entsprechenden Einstellungen zu gelangen, wählen Sie im Menü EXTRAS den Befehl EINSTELLUNGEN (siehe Abbildung 9-5). In dem daraufhin erscheinenden Konfigurationsfenster wählen Sie auf der linken Seite die Schaltfläche ALLGEMEIN und anschließend (unten rechts) VERBINDUNGS-EIN-

STELLUNGEN. Darüber hinaus gestaltet sich die Eingabe ähnlich wie im Internet Explorer, zuvor ist noch der Radiobutton für manuelle Proxyeinstellungen zu aktivieren.

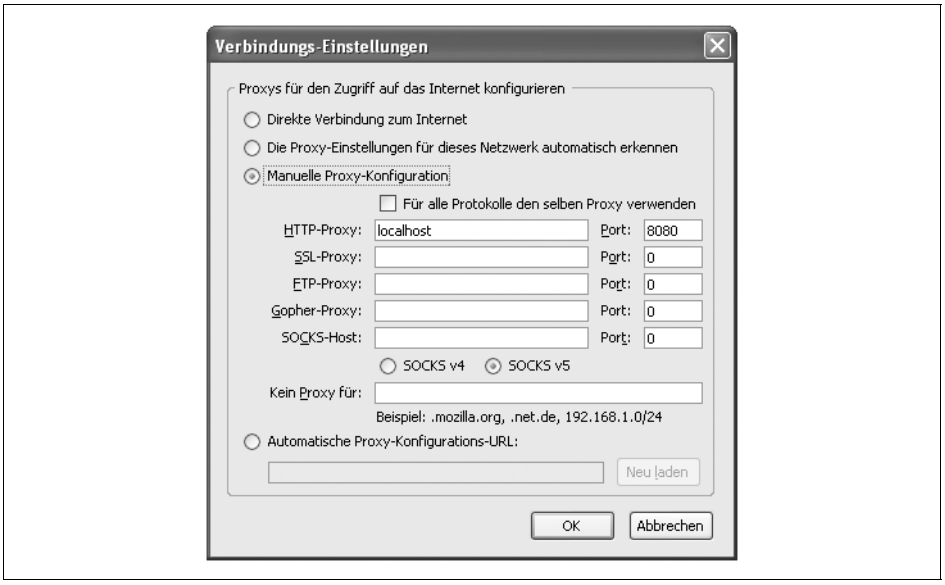

Abbildung 9-5: Proxyeinstellungen bei Firefox

Opera

Für Opera genügt im Prinzip der Druck auf die Taste F12 und das Setzen des Häkchens bei PROXY-SERVER AKTIVIEREN, die restlichen Einstellungen dürften automatisch richtig gesetzt sein (siehe Abbildung 9-6). Wir schauen uns dennoch den Weg an, falls einmal irgendwo etwas klemmen sollte. Wählen Sie den Menübefehl EINSTELLUNGEN im Menü EXTRAS und klicken Sie anschließend im Konfigurationsfenster auf den Reiter ERWEITERT. Dort wechseln Sie in den Abschnitt NETZWERK und klicken auf die Schaltfläche PROXY-SERVER. Auch hier gestaltet sich der Eintrag des lokalen Proxys ähnlich wie oben beschrieben.

Wenn Sie nun beispielsweise auf die Seite *http://www.wieistmeineip.de/* besuchen, werden Sie sehen, dass nun anstatt Ihrer IP-Adresse die des benutzten Proxyservers übertragen wird. Auch die Angaben zur Region und eingesetzten Software entsprechen jetzt nicht mehr Ihren eigenen Daten. Im hier gezeigten Fall stammen sie plötzlich aus Mexiko.

JAP

Bei dem Programm *JAP* handelt es sich um eine Lösung der Technischen Universität Dresden. Damit soll es in Zukunft möglich sein, wirklich anonym zu surfen. Dazu

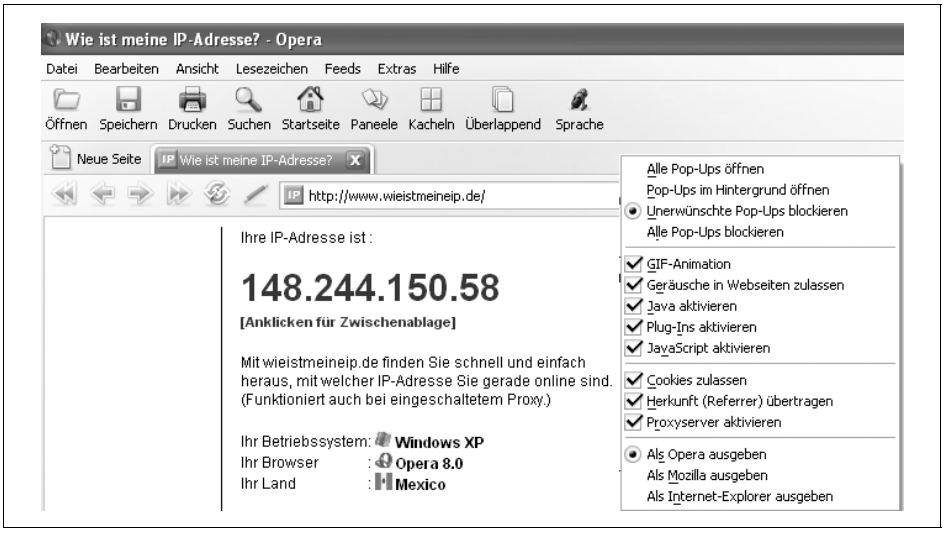

Abbildung 9-6: Die erkannte IP-Adresse ist nun die des Proxies.

soll laut JAP-Webseite eine so genannte *Mix Proxy Kaskade* benutzt werden, die bewirken soll, dass weder der angefragte Webserver noch ein Lauscher im Netz erkennen kann, welcher User welches Angebot besucht.

JAP basiert im Prinzip darauf, dass der gesamte Datenverkehr sämtlicher JAP-Benutzer an eine Kette verschiedener Proxies geschickt wird, von denen nur einer wirklich sicher sein muss. Diese Proxies verschlüsseln den Datenstrom und schicken ihn in einer anderen Reihenfolge weiter. Dadurch soll es in Zukunft nicht mehr möglich sein, die Nutzerdaten eines einzelnen Surfers aus der Gesamtmenge zu extrahieren. Man verschwindet sozusagen in der Anfrageflut der Server. Da sich JAP zurzeit in der Probephase befindet, kann noch nicht bewertet werden, wie sicher die endgültige Version sein wird. Es handelt sich aber um eines der interessantesten Projekte dieser Art. Ein Besuch der Webseite unter *http://anon.inf.tu-dresden.de/* (inklusive Möglichkeit zum Download der Probeversion) lohnt daher auf jeden Fall.

Provider

Provider spielen bei der Aufzeichnung von Kommunikationsinhalten eine besondere und immer gewichtigere Rolle. Wenn Sie sich in das Internet einwählen, passiert im Grunde genommen Folgendes: Sie bauen eine Verbindung zu Ihrem Internetprovider auf, dieser prüft die übergebenen Benutzerdaten und gewährt Ihnen über seine Router und Firewalls Zugriff auf seine Standleitung ins Internet. Die EDV-Systeme des Providers sind also der erste Punkt, den all Ihre Daten unabhängig von Protokoll, Ziel oder Dienst vollständig passieren müssen. Daher verfügt ein Provider natürlich über sämtliche Kommunikationsdaten zwischen Ihnen und

dem Rest des Internets. Zwar würde ein seriöser Provider diese Daten nicht missbrauchen, er ist jedoch potenziell in der Lage, die von Ihnen übertragenen Inhalte auszuwerten und abzuspeichern. Der größte deutsche Provider, T-Online, hat im Sommer 2005 einen wichtigen Prozess verloren, in dem es um seine Weigerung ging, von einem Nutzer unnötig erhobene und abgespeicherte Verbindungsdaten zu löschen. Das Amtsgericht Darmstadt hat diese Speicherung bei Flatrate-Kunden für unzulässig erklärt, da sie den Datenschutzbestimmungen wiederspricht.

Wenn ein Internetuser versucht, Schaden bei einem Online-Shop anzurichten, im Chat sehr negativ auffällt oder Spam-Mails verschickt, kann es vorkommen, dass sich der verantwortliche Systemadministrator oder Webmaster mit der auffällig gewordenen IP-Adresse an den Provider wendet und um eine Verwarnung des betreffenden Users bittet. Der Provider kann zurzeit (noch) anhand seiner Datenbank nachvollziehen, welcher User wann welche IP-Adresse benutzt hat, und sich dann an die betreffende Person wenden. Je nach Schwere des Vorfalls kann das zu einer Verwarnung oder sogar der Sperrung des Accounts führen. Ist zudem die Polizei durch eine mögliche Anzeige in den Fall involviert, wird der Provider alle Personendaten an die Beamten weitergeben. Zwar speichert der Provider die Zuordnungsdaten zwischen IP-Adresse und Benutzer nicht für alle Zeiten, mit einer Dauer von 80 Tagen sollten Sie jedoch rechnen.

Wie Sie oben gelesen haben, wird diese Speicherung einerseits (in vielen Fällen) als unzulässig gebrandmarkt, der Gesetzgeber würde hingegen seit dem 11.9.2001 gern jegliche Verbindungsdaten (und Inhalte) über Jahre hinweg speichern. Daher wollen wir uns im Folgenden kurz mit dem Staat als Datenakteur näher befassen.

Juristische Aspekte und staatliche Abhörsysteme

Da das Internet ein sehr junges Medium ist, stecken die rechtlichen Grundlagen noch in den Kinderschuhen. In vielen Ländern gibt es noch keine konkrete Gesetzgebung für den Umgang mit diesem neuen Medium. Auch die Gesetzesentwürfe der EU sowie speziell auf der deutschen Ebene sind zum Teil noch sehr unausgereift und werden kontrovers diskutiert. Im Gegensatz zu Europa spielen die USA eine Art Vorreiterrolle, wenn auch oft im negativen Sinn. Bei der Entwicklung der Rechtsgrundlagen gibt es zwei Hauptaspekte, die immer wieder für Konfliktstoff sorgen. Erstens bemängeln sowohl Benutzer als auch Experten das mangelnde Fachwissen der gesetzgebenden Instanzen. Zweitens gehen die neuen Entwürfe und Gesetze sehr stark in Richtung eines pauschalen Abhörens des gesamten Datenstroms. Dabei scheinen vor allem die Anschläge des 11.9.2001 und die daraus resultierenden weiteren Enwicklungen der letzten Jahre an der wichtigsten Grundlage unserer westlichen, freiheitlichen Ordnung zu rütteln – der Unschuldsvermutung. Im harten Kurs beim Kampf gegen den Terror bleibt Letzere allzu oft auf der Strecke, was

sich insbesondere in der aktuellen und aufkommenden Internet- und Datenschutzgesetzgebung wiederspiegelt.

Der erste Punkt ist deshalb wichtig, weil in den vergangenen Jahren bei der Bewertung von juristischen Problemen im Zusammenhang mit Internetangeboten, aufgrund der fachlichen Inkompetenz der Beteiligten, häufig gravierende Fehlurteile gefällt wurden. Als extremes Beispiel gilt die Anzeige gegen Compuserve Deutschland, einen der Mitte der 90er Jahre größten deutschen Internetprovider. Dabei wurde dem Geschäftsleiter vorgeworfen, »kinderpornographische Schriften« zu verbreiten. Da es den Fachleuten und Anwälten zunächst nicht gelang, Richter und Staatsanwaltschaft davon zu überzeugen, dass ein Provider nicht ohne Weiteres die Nachrichten, die über seinen Newsserver ausgetauscht werden, kontrollieren kann, wurde der damalige Geschäftsführer von Compuserve Deutschland, Felix Somm, zu einer zweijährigen Bewährungsstrafe und 100.000 DM Geldbuße verurteilt. Erst im November 1999 sprach das Landgericht München Herrn Somm nach zwei Jahren Rechtsstreit frei.

Aber auch aktuell gibt es immer wieder Fälle, in denen sich zeigt, dass die rechtsprechenden Instanzen versuchen, die herkömmliche Rechtsprechung unmodifiziert auf das Internet zu übertragen. Auch der an sich harmlose Internetlink wurde zum Thema zahlreicher Debatten und Fehlurteile. So waren einige Juristen der Ansicht, dass man sich den Inhalt einer Seite, zu der man auf der eigenen Website einen Link setzt, zu eigen mache und deshalb auch für die dortigen Inhalte verantwortlich sei. Dies führte natürlich zu hitzigen Diskussionen, denn Hyperlinks sind nun einmal *das* Strukturmerkmal des WWW. Stellen Sie sich vor, Sie wären als Betreiber einer privaten Homepage für die von Ihnen verlinkten Webseiten verantwortlich. Sie müssten rund um die Uhr darüber wachen, welche Inhalte sich auf diesen fremden Seiten ändern und ob nicht zufällig jemand etwas Verbotenes in einem Chat oder in einem Forum schreibt. Zudem stellt sich dann zurecht die Frage, ob Sie auch für die Links auf der von Ihnen verlinkten Webseite verantwortlich sind, was die Sache ad absurdum führen würde. Nimmt man es genau, ist nämlich jede Seite im Internet mit jeder anderen durch eine bestimmte Zahl an Hyperlinks verbunden.

Gerade in Deutschland zeichnet sich innerhalb der letzten Jahre und zunehmend seit 2004 eine beunruhigende Entwicklung ab: Betreiber von Blogs, Foren, Chats und anderer Internetcommunities laufen zunehmend Gefahr, abgemahnt oder verklagt zu werden. Dazu reicht es schon, einen Songtext zu zitieren, sich in einem Forum Luft über einen Händler oder ein großes Warenhaus zu machen oder das CD-Cover seiner Lieblingsband als Avatar[10] zu benutzen. Die Streitsummen werden dabei in unnatürliche Höhen getrieben, und man vergisst anscheinend, dass es sich bei den Verklagten nicht nur um Fans besagter Musikgruppen, sondern vor allem um unbe-

10 Damit bezeichnet man ein kleines Bildchen, das in Chat- und Forensystemen neben einem Spitznamen als Identitätsmerkmal benutzt wird.

darfte Internetnutzer handelt. Fünfstellige Streitsummen oder Abmahnkosten in Höhe einiger tausend Euro (Massenabmahnungen von dubiosen Anwaltskanzleien sind im deutschen Teil des Internets zu einem echten Problem geworden und befassen inzwischen auch den Gesetzgeber) verderben vielen privaten Betreibern schnell den Spaß an der Community. Deutschland gerät daher im internationalen Vergleich im Bereich der innovativen Online-Projekte und Plattformen zunehmend ins Hintertreffen.

Der zweite wichtige Aspekt, den wir einleitend erwähnten, ist der Versuch, die Kommunikation des Individuums umfassend und auch ohne besondere Verdachtsmomente abzuhören. Es soll also zuerst einmal flächendeckend abgehört und schließlich bei Bedarf geprüft werden, ob dies überhaupt nötig war. Es mag verständlich sein, dass der Staat eine Möglichkeit finden muss, die Kommunikationsinhalte, die zur Aufklärung von Verbrechen und Terrorismus beitragen können, im äußersten Notfall mitzuprotokollieren. Ein pauschales Abhören verstößt jedoch gegen verschiedene Grundrechte oder zumindest gegen die Vorstellungen von einer freien Gesellschaft. Zurzeit lassen sich in Europa gleich mehrere, zum Teil aber miteinander verflochtene Abhörpläne voneinander unterscheiden. Auf nationaler Ebene sei hier die deutsche Telekommunikations-Überwachungsverordnung (TKÜV) genannt. Es würde den Rahmen dieses Kapitels sprengen, sich zu all diesen Angriffen gegen die Privatsphäre zu äußern. In einer Presseerklärung des Bundesbeauftragten für Datenschutz vom 10.5.2001 zur TKÜV heißt es:

> Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße »Surfen« zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.
>
> Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen. (Quelle: *http://www.bfd.bund.de*).

Auch von Seiten der Wirtschaft, der Internetgemeinde und zahlreicher Menschenrechtsorganisationen hagelt es starke Kritik. Auslöser für diese heftigen Reaktionen sind die oben genannten Pläne zum Abhören sämtlicher Kommunikationsmittel. Dabei sollen nicht nur kriminelle Personen (laut früherer Gesetzgebung nur Terro-

risten) abgehört werden, sondern jeder Bürger, der Fax, Telefon, Internet oder Handy benutzt. Ein Enfopol-Papier fordert sogar, »Telekommunikationsanbieter dazu [zu] verpflichten, jedes Telefongespräch, jedes Fax und jede E-Mail »für mindestens sieben Jahre« lang zu archivieren« (Quelle: *http://www.heise.de*, Auszug aus: *Harsche Kritik an Enfopol-Arbeitsgruppe*, 23.5.2001).

Wie Sie sicherlich bemerkt haben, stammen diese Zitate aus dem Jahre 2001, inzwischen ist das TKÜV nach langem Tauziehen und Protesten in Kraft getreten und soll gegen den massiven Widerstand der Datenschutzbeauftragten weiter ausgebaut werden. Das europäische Pendant steht ebenfalls kurz vor der Fertigstellung, wird aber noch heftig diskutiert und möglicherweise an entscheidenden Stellen abgeschwächt.

In einem Buch über Computer und Datensicherheit können staatliche Datenabhörvorrichtungen und Sicherheitspolitik nicht fehlen, es wäre jedoch falsch, hier zu tief in die politische Situation einzutauchen und würde dem Ernst der Lage (sowohl im Hinblick auf den weltweiten Terrorismus als auch unserer eigenen westlichen Werte) nicht gerecht werden. Daher wollen wir uns nun nur kurz mit einem der bekanntesten Überwachungssysteme beschäftigen, um die allgemeinen Möglichkeiten an einem Beispiel aufzuzeigen.

Das Echelon-System

Bei dem Geheimdienstprojekt *Echelon* handelt es sich aller Wahrscheinlichkeit nach[11] um ein weltumspannendes Abhör- und Spionagesystem, an dem neben den USA auch Großbritannien, Australien und Neuseeland aktiv beteiligt sein dürften. Verantwortlich für das Projekt ist die amerikanische *National Security Agency* (NSA) sowie das britische *Gouvernment Communications Headquarters* (GCHQ).

Echelon verfügt weltweit über zahlreiche Abhöreinrichtungen, so zum Beispiel in den Niederlanden und in Bad Aibling (Deutschland). Mit diesen Einrichtungen ist es theoretisch möglich, einen Großteil der modernen Kommunikation über Telefon, Handy, Fax oder E-Mails in Echtzeit zu filtern und möglicherweise sogar Personalisierungen durchzuführen. Insgesamt ist das Wissen um Echelon aber sehr vage und basiert oft auch nur auf Verdachtsfällen. Da sich aber inzwischen sogar ein nichtständiger Ausschuss des Europäischen Parlaments mit dem Geheimprojekt beschäftigt, kann man zumindest davon ausgehen, dass es Echelon wirklich gibt und es auch im Einsatz ist.

Zurzeit wird besonders der Verdacht der Wirtschaftsspionage diskutiert. Dabei verdichten sich die Informationen, dass Echelon bewusst Wirtschaftsspionage betrieben hat oder immer noch betreibt. Der EU-Ausschuss rät daher sowohl Privatpersonen als auch Unternehmen, ihre sensiblen Daten unbedingt zu verschlüsseln. Die

11 Diese Formulierung zeigt bereits, wie geheim das Projekt tatsächlich ist.

Angst der Wirtschaft vor einer gezielten Bespitzelung durch die USA wurde im Juni 2001 sogar zu einem Hauptthema beim Spitzengespräch zwischen dem Bundeswirtschaftministerium und der Internetbranche. Inzwischen hat auch die NSA auf die schweren Vorwürfe seitens der EU reagiert und versprochen, die Abhörstation Bad Aibling bis zum 30.9.2002 zu schließen. Nach den Anschlägen auf das World Trade Center blieb die Anlage jedoch bis 2004 in Betrieb und wurde nun anscheinend durch eine andere, kleinere Überwachungsanlage bei Darmstadt ersetzt (siehe dazu *http://www.heise.de/tp/r4/artikel/17/17024/1.html*).

Besonders erwähnt sei hier noch der britische Journalist Duncan Campbell, der im Auftrag des Parlamentsausschusses zahlreiche Erkenntnisse zu Echelon gesammelt und veröffentlicht hat. Zumindest die neuesten Berichte deuten weiterhin auf eine starke Aktivität von Echelon, sowohl in Form einer Bespitzelung von Nicht-US-Bürgern als auch bei der Wirtschaftspionage. Erst im März 2001 hat die Organisation *Privacy International* der NSA bezüglich des Echelon-Projektes eine symbolische Auszeichnung im Bereich »Lebenslange Bedrohung« verliehen und somit die Diskussion wieder angeheizt. Aktuelle Informationen rund um Echelon sowie ein Artikelarchiv und Interviews mit Duncan Campbell finden Sie in der Netzzeitung *Telepolis* unter *http://www.heise.de/tp/*.

Schließen wollen wir dieses Kapitel mit einem Zitat, das dem berühmten amerikanischen Vordenker und Staatsmann Benjamin Franklin zugeschrieben wird und das den Nagel vielleicht besser auf den Kopf trifft, als man es von einem über 200 Jahre alten Ausspruch erwarten könnte: »Wer grundlegende Freiheiten aufgibt, um vorübergehend ein wenig Sicherheit zu gewinnen, verdient weder Freiheit noch Sicherheit.«