Patrick Hammer

Sicherheit und Datenschutz im Internet

Studienarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 1998 GRIN Verlag
ISBN: 9783638101462

Patrick Hammer

Sicherheit und Datenschutz im Internet

GRIN Verlag

Sicherheit und Datenschutz im Internet

Der Service-Provider

Jeder User läßt beim Surfen im Internet eine individuelle Datenspur zurück, die zu mehr oder weniger detaillierten Verhaltens- und Kommunikationsprofilen ausgewertet werden kann. Jedoch ist nicht jeder Mitwirkende im Internet dazu fähig, den Eigentümer der jeweiligen Datenspur zu ermitteln. Der Service-Provider kann den User in aller Regel ermitteln, während die Content-Provider (die eigentlichen Internet-Diensteanbieter) auf zusätzliche Informationen angewiesen sind, um die Identität ihrer Kunden ausfindig machen zu können. Über den Service-Provider (AOL, CompuServe usw.) wird im allgemeinen der Internet-Zugang hergestellt. Hierfür benötigt dieser den Namen und die Adresse des Kunden, sowie seine Bankverbindung. Der Service-Provider hat eine sehr detaillierte Kenntnis über die Online-Aktivitäten des Users, da man dort weitläufig personenbezogene Nutzungs- und Abrechnungsdaten verarbeitet, die während der Internet-Nutzung aufgezeichnet werden: Internet-Adressen, die besucht wurden, Inhalte von E-Mails, Nutzung von Diensten des Service-Providers, Nutzung und Inhalt von gelesenen oder geposteten Newsgroups, und Aussagen, die in Diskussionsforen gemacht werden. Hier besteht zum einen die große Gefahr, daß der Service-Provider die gespeicherten Daten zu detaillierten Kundenprofilen auswertet und diese an andere für Marketingzwecke weiterreicht, zum anderen können durch die Auswertung der Zeitpunkte der Online-Nutzung Gewohnheiten und Anwesenheitszeiten ermittelt werden. Durch die Internet-Nutzung wird es also immer schwieriger, sich unbeobachtet zu verhalten, die Privatsphäre wird immer weiter eingeschränkt. Dem User bleibt also nichts anderes übrig, als auf die Regelungen des Multimediagesetzes (s.u.) zu vertrauen und sollte sich darum beim Surfen im Internet immer im klaren sein, daß er nicht unbeobachtet bleibt und sein Nutzungsverhalten in Anbetracht dessen gegebenenfalls verändern.

Der Content-Provider

Beim Internet-Zugang über einen Service-Provider wird dem Internet-Nutzer bei jedem Einstieg ins Netz eine andere Netz(IP)-Adresse aus dem Kontingent des Provider zugewiesen. Durch diese Dynamik kann der jeweilige User wenigstens gegenüber der Content-Provider eine gewisse Anonymität vorweisen. Über die IP-Adresse allein können diese nicht den Internetbenutzer identifizieren, sie können nur den Service-Provider ermitteln, den der jeweilige User nutzt. So gibt es auf vielen Seiten von Diensteanbietern die Möglichkeit, seine Anschrift oder E-Mail-Adresse zurückzulassen (bei Gewinnspielen oder Umfragen, die sich auf das Internetangebot beziehen).

Cookies

Individuelle Nutzungsdaten können jedoch nicht nur seitens der Content-Provider, sondern auch auf dem lokalen PC des Users gespeichert werden: Die Diensteanbieter verwenden hierfür sogenannte Cookies, die diese Daten beinhalten und auf dem PC des Nutzers gespeichert werden. Kommt der User dann irgendwann wieder auf die gleiche Internetseite, kann der Cookie vom Content-Provider ausgewertet werden und das Angebot auf die gespeicherten Daten hin (also dem Nutzungsverhalten des Users gemäß) ausgerichtet werden. Die neuen Daten können dann wieder im Cookie abgespeichert werden. Bei vielen Internet-Browsern kann man die Nutzung von Cookies deaktivieren,

oder man kann sich zumindest warnen lassen, bevor ein Cookie auf der Festplatte gespeichert wird. Andererseits kann man die Cookies (deren Dateiname mit "cookie" beginnt) auch selber immer wieder von Hand löschen.

Bezahlen im Netz

Auch beim Bezahlen im Internet wird die Identität des Users benötigt, hier erfährt erstens der Diensteanbieter den Namen seiner Kunden, zweitens kann die Bank (bei Bezahlung per Kreditkarte) sich ein Bild über die Online-Nutzung ihrer Kunden machen. Das Bezahlen per Kreditkarte ist ohnehin noch viel zu unsicher und nicht empfehlenswert. Hier wird sich statt dessen eventuell das elektronische Geld (Ecash) durchsetzen: Diese Zahlweise macht anonymes Zahlen möglich, das Geld wird auf der Festplatte des Users gespeichert. Die Echtheit wird durch eine verschlüsselte digitale Unterschrift der Ecash herausgebenden Bank gewährleistet. Die Ecash-Münzen sind nur mit einer Seriennummer versehen, somit können weder Content-Provider noch Kundenbank die Identität des Users ermitteln.

Das erhaltene elektronische Geld können die Diensteanbieter dann wieder bei einer Bank gegen Bargeld einlösen.

Rechtliche Bestimmungen

Die Internet-Angebote von Service- und Content-Providern werden im Telekommunikationsgesetz (TKG), im Informations- und Kommunikationsdienstegesetz (IuKDG, auch "Multimediagesetz") und im Mediendienste-Staatsvertrag der Länder geregelt. Das TKG regelt elektronische Post und Mobilfunk, während für alle anderen Dienste das Multimediagesetz und der Mediendienste-Staatsvertrag gelten. Das IuKDG regelt u.a. den Schutz personenbezogener Daten bei Telediensten (z.B. Homebanking, Suchmaschinen oder Telearbeit). Die Gestaltung und technische Ausrichtung von Telediensten soll so vonstatten gehen, daß so wenige persönliche Daten wie möglich erhoben und verarbeitet werden. Service- als auch Content-Provider sind hiernach verpflichtet, dem User die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder zumindest unter einem Pseudonym zu ermöglichen, insofern dies technisch machbar ist. Benutzerprofile sind nur bei der Verwendung eines Pseudonyms zulässig. Eine Zusammenführung von Nutzungsdaten aus verschieden Diensten ist ebenfalls nicht erlaubt. Des weiteren müssen Nutzungsdaten ungeachtet der Verwendung von Pseudonymen nach der jeweiligen Nutzung wieder gelöscht werden, sobald die Abrechnung beendet ist.

Diese Gesetze gelten jedoch nicht in vollem Umfang für AOL und CompuServe, da diese Provider den Großteil ihrer Daten in Rechenzentren in Nordamerika verarbeiten und auch die Internet-Verbindung über Amerika herstellen. Diese Daten sind nicht durch das bundesdeutsche Recht geschützt und können somit an Marketingfirmen weitergereicht werden.

Schutz lokaler Daten

Daten, die auf unvernetzten PCs gespeichert sind, sind vor dem mißbräuchlichen Zugriff von außen meist hinreichend geschützt. PCs mit Internetzugang oder solche, die mit Internet-PCs vernetzt sind, sind vor Zugriffen von außen nicht so einfach zu schützen.

Internet-Programme, wie z.B. Internet-Browser, enthalten relativ oft Software-Bugs (Programmfehler), die es außenstehenden Hackern ermöglichen, lokale Sicherheitsmaßnahmen zu umgehen und sich Zugriff auf lokale PCs und Netzwerke zu verschaffen. Beispielsweise enthalten die Versionen 3.0 und 3.1 des Microsoft Internet Explorer einen Fehler, der es Außenstehenden ermöglicht, Programme auf fremden Rechnern während einer Internetsitzung zu starten, mit Hilfe derer Daten kopiert, verändert oder gelöscht werden können. Gegen diese Bugs kann man von den meisten Softwareherstellern nach einiger Zeit kostenlos sogenannte Patches beziehen, also Programme, die diese Sicherheitslücken schließen.

Jedoch geht Gefahr auch von Funktionen in Programmen aus, die bewußt vom Hersteller eingebaut wurden. Microsofts Betriebssystem Windows95 war anfänglich mit der Funktion ausgestattet, daß bei der erstmaligen Online-Registrierung des Programms Lizenznummern von Microsoft-Produkten ausgelesen wurden und somit überprüft werden konnte, ob der User in Besitz illegaler Software ist. Erst nach öffentlichen Warnungen vor der Registrierung sah sich Microsoft veranlaßt, die Funktion zu entfernen. Auf die gleiche Weise hätten auch andere, persönliche Daten des Users an Microsoft übermittelt werden können. Auch das Browser-Plug-in (Zusatzprogramm) Shockwave der Firma Macromedia enthält eine ähnliche Funktion: Dieses Programm, das für die Darstellung von Spezial-Effekten im Browser notwendig ist, ist in der Lage, die E-Mail-Adresse des Nutzers an andere Rechner zu senden. Man sollte also zumindest darauf verzichten, Programme von Herstellern, die nicht als seriös gelten, zu verwenden. Am besten schützt der Anwender sich jedoch vor solchen Vorfällen, indem er sich regelmäßig in PC-Zeitschriften über Bugs und versteckte Funktionen erkundigt.

Computerviren

Computerviren sind Programmroutinen, die sich reproduzieren und Daten Schaden zufügen können. Sie kopieren sich selbständig in verschiedene Systembereiche und veranlassen oft die Löschung oder Beschädigung von gespeicherten Daten. Natürlich können sich Computerviren auch hervorragend über das Internet verbreiten. Der sogenannte "Internet-Wurm"-Virus nutzte einen Programmfehler des für das Versenden von elektronischer Post zuständigen Sendmail-Dienstes aus und konnte dadurch veranlassen, daß auf dem jeweiligen Computer verschiedenste Programme ausgeführt werden und somit die Hauptspeicherkapazität verbraucht wurde. Dies führte dazu , daß 1989 mehrere Tausend Rechner lahmgelegt wurden. Viren können jedoch auch veranlassen, daß geheime Daten, wie zum Beispiel Paßwörter, an andere Internet-Rechner weitergesendet werden.

Computerviren können sich an ausführbare Programme oder Dokumente heften, die per Diskette oder E-Mail übertragen werden. Durch den regelmäßigen Einsatz von (durch kostenlose Updates) aktuell gehaltenen Virenscannern kann man sich relativ wirksam vor Virenbefall schützen.

Java, Javascript und ActiveX X

Auf immer mehr Webseiten finden sich nicht nur Grafik und Text, sondern auch spezielle Programme: Java-Applets, Javascripts oder ActiveX-Controls. Diese Programme bieten unzählige Anwendungsmöglichkeiten, man kann durch sie Webseiten mit Spielen,

Grafikeffekten und vielen Funktionen zur Steigerung des Bedienungskomforts ausstatten. Das hier auftretende Sicherheitsproblem liegt darin, daß man nicht kontrollieren kann, welche Funktionen das angewandte Programm tatsächlich enthält. Oft bemerkt der User gar nicht, daß ein solches Programm ausgeführt wird. Mithilfe dieser Programme können auch unbemerkt persönliche Daten kopiert und an andere Rechner geschickt werden. Die Programme können aber nicht nur von WWW-Seiten aus gestartet werden, sondern auch von E-Mails und anderen HTML-Dokumenten. Bei Java-Applets wird jedoch meist von den Sicherheitsvorkehrungen des Browsers verhindert, daß das Programm ungehindert auf die gesamte Festplatte zugreifen kann. Jedoch können auch hier Sicherheitslücken in den Internet-Programmen vorliegen, die von den Java-Programmierern mißbräuchlich genutzt werden können. Außerdem werden von den meisten Usern in Unkenntnis möglicher Folgen Anfragen der Java-Programme auf Zugriffsrecht für die Festplatte gewöhnlich gewährt. Zum Beispiel müssen viele Java-Applets temporäre Dateien im "Temp"-Verzeichnis der Festplatte anlegen, wo der User keine sensiblen Daten vermutet, jedoch legen viele Texteditoren ebenso im "Temp"-Verzeichnis temporäre Dokumentversionen an, die dann ausgelesen werden können.

Javaskripten sind weitaus weniger gefährlich, bei diesen in den HTML-Code von Webseiten eingebetteten Programmen besteht lediglich die Gefahr, daß diese Konfigurationsdaten des Browsers auslesen und über das Internet verschicken können. Bei der Netscape-Version 2.0 sorgte beispielsweise der einfache Befehl <Body onLoad = "document.mailme.submit()"> dafür, daß eine E-Mail an den Betreiber der Webseite geschickt wurde, so daß der dann die E-Mail-Adresse des Absender herausfinden konnte. Hiervor kann man sich lediglich schützen, indem man im Browserprogramm keine Absender-E-Mail-Adresse einträgt.

Bei ActiveX-Controls gibt es keine solch einfachen Sicherheitsvorkehrungen, weswegen dieses ein weitaus gefährlicheres Werkzeug ist: Alles, was unter Windows mit Maus und Tastatur möglich ist, kann man auch mit Hilfe von ActiveX über das Netz steuern. Lokale Daten können problemlos kopiert und über das Internet verschickt werden. Man kann hier nur ein geringes Maß an Sicherheit erreichen: Es besteht lediglich die Möglichkeit, nur solche ActiveX-Controls zuzulassen, die mit dem sogenannten "Authenticode" zertifiziert sind. Dieser enthält eine digitale Unterschrift, die die Echtheit und Vollständigkeit des Zertifikats bestätigt, jedoch nicht die Programmqualität. Außerdem werden hier nicht die Programme auf Integrität und Sicherheitsrisiken überprüft, sondern nur auf den Hersteller. In der Fernsehsendung "PlusMinus" wurde beispielsweise gezeigt, wie man mit Hilfe eines auf einer Lockseite versteckten ActiveX-Controls Geld via Internet auf fremde Konten transferiert. Hier wurde ein Homebanking-Programm auf dem PC des Users so manipuliert, daß es bei der nächsten Homebanking-Sitzung unbemerkt bestimmte Überweisungen zusammen mit anderen ausführt. Beispielsweise kann aber auch durch solche Manipulationen veranlaßt werden, daß jede E-Mail eines Users unbemerkt kopiert und an eine bestimmte E-Mail-Adresse gesendet wird.

Man sollte hinsichtlich dieser Gefahren die Nutzung solcher Programme weitgehend einschränken. In den meisten Browsern läßt sich die Nutzung solcher Programme ausschalten.

Zugriff über TCP/IP

Über das Internet-Protokoll TCP/IP läuft nahezu der gesamte Datentransfer im World Wide Web ab. Um Zugriff auf lokale Systemressourcen von fremden Computern aus zu verhindern, werden zwischen lokalem PC und Internet Firewall-Systeme zwischengeschaltet. Firewalls schützen Computernetzwerke vor Zugriffen von außen. Spezielle Router lassen nur ganz bestimmte Datenpakete in das Netzwerk eindringen (durch Überprüfung des Headers), manche Router lassen nur E-Mail-Verkehr zu, je nach den Vorgaben des Systemadministrators. Da diese Systeme aber noch sehr teuer sind, werden sie noch relativ selten eingesetzt. Sollte der Internet-Zugang eines Unternehmens nicht durch Firewalls gesichert sein, ist es ratsam, auf das Internet von einem unvernetzten Rechner aus zuzugreifen, auf dem keine sensiblen Daten gespeichert sind.

Unverschlüsselter und verschlüsselter Datentransfer

Die meisten Daten, die im Internet verschickt werden, sind nicht verschlüsselt und können somit in den Netzwerkrechnern des Netzes abgehört werden. Datenpakete können auf ihrem Weg zum Empfänger von Hackern über bestimmte Rechner umgeleitet werden. Beispielsweise werden unverschlüsselte Kreditkartennummern häufig von Hackern abgefangen und zur kriminellen Abbuchung größerer Summen genutzt. Ebenso ist es aber auch möglich, vertrauliche E-Mails mitzulesen oder zu verändern. Auch können Daten beim Homebanking abgefangen werden und mit veränderter Kontonummer an die Bank weitergeleitet werden. Solche Vorgänge sind aber nur sehr schwer zu bewerkstelligen und setzt sehr große Sachkenntnisse voraus. Außerdem werden immer wieder neue Sicherheitsvorkehrungen geschaffen, die es dann erst wieder zu durchbrechen gilt.

Um Daten zu verschlüsseln, gibt es Verschlüsselungsprogramme, wie z.B. Pretty Good Privacy (www.pgp.com), die man kostenlos beziehen kann. Sie können beispielsweise beim Versenden von elektronischer Post verwendet werden und gewährleisten ein gewisses Maß an Privatsphäre und Sicherheit im Netz, da sie mit einem sehr guten Verschlüsselungsverfahren ausgestattet sind.

In mehreren Ländern bricht jetzt eine sehr kontroverse "Kryptodiskussion" an, auch in Deutschland wird seitens der Bundesregierung geprüft, ob der Einsatz sicherer Verschlüsselungsprogramme reglementiert oder ganz verboten werden sollte. Ein Verbot der Verschlüsselung wäre jedoch möglicherweise verfassungswidrig, da die vertrauliche und unbeobachtete Kommunikation gemäß Art. 10 als unverletzlich gilt. Auch würde eine solches Verbot staatlichen und wirtschaftlichen Interessen an einer vertraulichen Übertragung von Daten widersprechen. Außerdem wäre das Verbot auch technisch und finanziell kaum kontrollierbar, die Strafandrohung wäre für Kriminelle nur von Bedeutung, wenn sie höher wäre, als für das zu verschleiernde Delikt und es kann nur schwerlich überprüft werden, ob überhaupt verschlüsselte Daten vorliegen.

Autor: Patrick Hammer