Datenschutz und Datensicherheit DuD, BvD-Kolumne, 22/10 (1998) 608-609.

Selbstschutz im Internet

Hannes Federrath

Problemanalyse

Die Verbreitung des Internet als Kommunikationsmedium hat in den letzten Jahren deutlich zugenommen; nicht nur zum Austausch von Daten zwischen privaten Nutzern, auch im kommerziellen Bereich wird das Internet zunehmend zu einer Plattform für den Austausch von Waren und Dienstleistungen. Zwangsläufig wachsen damit die Risiken sowohl der Nutzer als auch der Anbieter und ebenfalls, aufgrund gegensätzlicher Interessen, das Spannungsfeld zwischen Privatheit und der Verbindlichkeit von Kommunikationsaktivitäten im Netz.

Normalerweise wird ein Anbieter zunächst einige Anstrengungen zur Senkung *seiner* Risiken unternehmen. Seine Schutzanforderungen beziehen sich insbesondere auf die Identifizierung und Authentizität der Benutzer seines Angebots. Ein technischer Mechanismus zur Sicherstellung der Authentizität ist bekanntlich die digitale Signatur. Deutschland war bei der Verabschiedung eines Rechtsrahmens für die digitale Signatur vorbildlich schnell, nicht zuletzt auch deswegen, weil für die Industrie der kommende Markt absehbar war.

Für die Benutzer neuer Kommunikationsmedien ist die Authentizität von Angeboten und die Identifizierung von Anbietern natürlich ebenso notwendig wie wichtig. Darüber hinaus haben die Endbenutzer ein berechtigtes Interesse daran, auch ihre Privatheit bei der Nutzung von Angeboten zu wahren. Leider tun sich hier jedoch sowohl die Industrie als auch der Gesetzgeber etwas schwer, die zunächst gezeigte Vorbildlichkeit aufrechtzuerhalten. Zwar predigen Datenschützer, daß auch für den Schutz der Nutzer etwas getan werden muß, ja haben sie sogar einiges erreicht (beispielsweise die Forderung nach Bereitstellung anonymer und pseudonymer Kommunikationsformen im Multimediagesetz), doch bisher fehlen umfassende und gezielte Lösungen oder Projekte zur Umsetzung der Privatheit der Endbenutzer. Vielmehr werden die gesetzlich vorgeschriebenen Überwachungsmöglichkeiten von den Netzbetreibern zähneknirschend implementiert. Es scheint so, als ob der Endbenutzer keine Lobby besitzt, obwohl sich alle Anstrengung des „Electronic Commerce“ doch auf ihn als Konsumenten beziehen müßte.

Nutzer brauchen Werkzeuge zum Selbstschutz

Ganz nüchtern betrachtet bleibt dem Nutzer des heutigen Internet nur übrig, sich selbst um seine Privatheit zu kümmern. Verläßt er sich darauf, daß ihm irgendwann die Anbieter entsprechende Schutzmöglichkeiten bereitstellen, läuft er Gefahr, bereits zuviele Daten über sich preisgegeben zu haben. Kein Anbieter muß in jedem Fall wissen, welche Angebote sich ein Nutzer beispielsweise angesehen hat, bevor er sich für eines entscheidet.

Je nach Schutzziel existieren im heutigen Internet bereits einige oder gar vielfältige Möglichkeiten, sich selbst zu schützen. Die Tabelle gibt zumindest eine kleine Auswahl an.

Anwendung	Beispielprogramm/Lösung
E-Mail-Verschlüsselung und Signatur	Pretty Good Privacy (PGP)
Senden und Empfang von E-Mail ohne Beobachtbarkeit	Mixmaster, Anonymous Remailer
Verschlüsselte Internet-Telefonie	PGPFone
Versteckte Kommunikation (Steganographie)	S-Tools, Jsteg, Stego
Unbeobachtbares Surfen im WWW	Anonymizer, Crowds, Onion Routing

Viele der Lösungen sind völlig kostenfrei zugänglich. Aus Sicherheitssicht ist das Positive an vielen Lösungen, daß sie meist gut dokumentiert und teilweise sogar im Quellcode zur Verfügung stehen und sich dadurch, im Gegensatz zu kommerzieller Software, keiner Überprüfung durch die „Netzgemeinde“ entziehen. Gegen die meisten Lösungen spricht, daß sie aufgrund der US-amerikanischen Exportrestriktionen nicht exportiert werden dürfen und wenn doch, dann nur mit reduzierter Sicherheit, z.B. reduzierter wirksamer Schlüssellänge.

Wer einige dieser Lösungen einmal ernsthaft ausprobiert hat, wird feststellen, daß deren Installation und Bedienung, gemessen an der Qualität professioneller Software, einige Wünsche offen läßt. Weiterhin unterscheiden sich die Sicherheitseigenschaften verschiedener Lösungen für die gleiche Anwendung oft erheblich von einander. Mit anderen Worten: Wo die eine Lösung noch gegen einen Angreifer schützt, ist die andere bereits unsicher.

Gerade im Hinblick auf die verstärkte Nutzung von Electronic Commerce sind die existierenden Selbstschutz-Werkzeuge leider nur sehr eingeschränkt nutzbar. Was nützt eine mit PGP verschlüsselte und digital signierte Bestell-E-Mail eines Endbenutzers, wenn der Anbieter nicht in der Lage ist, PGP-Nachrichten zu verarbeiten? Was nützt die anonyme Nutzung des Warenangebotes eines Softwareanbieters im World Wide Web, wenn man schließlich seine Kreditkartennummer unverschlüsselt über das Internet übertragen muß, damit der Anbieter zu seinem Geld kommt?

Fazit

Die Industrie sollte Selbstschutz-Werkzeuge wie PGP oder unbeobachtetes Surfen im Web auch als Chance sehen: Sicherheit gewinnt bei den Nutzern mehr und mehr an Bedeutung. Nach einer Umfrage des Georgia Institute of Technology setzten über 30 % von mehr als 10.000 Befragten den Schutz der Privatsphäre an die erste Stelle der Herausforderungen, die das Internet hervorbringt. Letzten Sommer waren es noch etwa 26 % (Chronicle of Higher Education 30. Januar 1998). Wir brauchen in der vernetzten Welt der Zukunft Möglichkeiten, mit denen die Nutzer sich schützen und selbst bestimmen können, welche Daten sie zu welcher Zeit über sich preisgeben. Die Aushandlung des Sicherheitsniveaus sollte dabei von einem Ausgleich des Machtgefälles zwischen Anbietern und Endbenutzern gekennzeichnet sein. Solange dieser Ausgleich nicht erfolgt ist, bleibt den Nutzern nur, ihren persönlichen Schutz in die eigenen Hände zu nehmen.

Adresse des Autors:
Hannes Federrath, TU Dresden, Fakultät Informatik, 01062 Dresden
E-Mail: federrath@inf.tu-dresden.de
WWW: http://www.inf.tu-dresden.de/~hf2
Hannes Federrath ist Referent für IT-Sicherheit im Vorstand des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.