Datenschutz ist Selbstschutz

Andreas Beck

Zusammenfassung

Das Internet zählt zu größten Erfindungen menschlicher Kommunikationstechnik. Gleichzeitig stellt es aber für jeden der sich darin unbedarft bewegt auch eine Gefahr für seine Privatsphäre dar. Anders als im realen Leben hinterläßt jeder unbemerkt irgendwelche permanenten Datenspuren, zusätzlich zu den Daten, die er aktiv preisgibt. Brisant wird es in dem Moment, wenn diese Daten zu einem Persönlichkeitsprofil zusammengeführt werden.

Dieser Artikel soll dem Benutzer Verhaltensvorschläge an die Hand geben, um sich vor den schlimmsten Auswüchsen ungehemmter Datensammelei zu schützen. Er soll in die Lage versetzt werden selbst zu entscheiden, wann wer welche Daten von ihm erhält. Die hier vorgeschlagenen Maßnahmen sind vollkommen technikunabhängig und daher sind zu ihrer Anwendung weder Änderungen am Betriebssystem des Computers, noch die Installation irgendwelcher Software notwendig. Dementsprechend findet sich hier auch *keine* Diskussion von Technik und Software.

Schlüsselwörter

Auktionen, Bankkonto, Datenschutz, Identität, Internet, Ebay, e-Mail, Kundenkarten, Lastschrift, WWW

Einleitung

Im vorliegenden Artikel geht es um konkrete Verhaltensvorschläge wie man seine Daten und damit sich selber im Kontakt mit anderen Teilnehmern schützen kann. Schwerpunkt ist hierbei zweifelsohne der „Lebensraum“ Internet, aber dennoch lassen sich viele Vorschläge auch problemlos auf andere Lebensbereiche übertragen. Rein technische Hinweise zu bestimmten Betriebssystemen oder Software wird man hier nicht finden. Dies bleibt den darauf spezialisierten Computerzeitschriften überlassen, die zu diesen Themen regelmäßig Testberichte veröffentlichen.[1-3] Zwar sind die hier gemachten Vorschläge unabhängig von der eingesetzten Technik, aber es wird davon ausgegangen, daß sich grundlegende Maßnahmen wie der Einsatz eines Anti-Virenprogrammes und einer Firewall auf Computern die mit dem Internet verbunden sind, inzwischen weitgehend herumgesprochen haben und zur Selbstverständlichkeit geworden sein. Hier geht es ausschließlich um das Verhalten im Umgang mit den eigenen Daten. Bei diesen Dingen hilft es nur sehr bedingt sich auf gesetzliche Rahmenbedingungen zu berufen oder gar zu verlassen. Das Internet ist ein globales Medium, bei dem man an keine offensichtlichen Grenzen wie in der realen Welt stößt. In vielen Fällen wird einem überhaupt nicht klar sein, in welchem Rechtsraum man sich bewegt. Auch wäre es sehr leichtsinnig sich allein darauf zu verlassen, daß die Gesetzte, sofern es überhaupt welche zum Datenschutz gibt, auch eingehalten werden. Wesentlich besser ist es, dort wo es möglich ist die Eigenverantwortung zu übernehmen um sich selber zu schützen. Dazu gehört aber auch, daß man wenigstens in groben Zügen über das Deutsche Bundesdatenschutzgesetz (BDSG) informiert ist.[4] Kürzlich ist hierzu eine sehr empfehlenswerte Broschüre mit vielen praktischen Fallbeispielen und Tipps beim Verbraucherzentrale Bundesverband e.V. (VZBV) erschienen.[5]

Oft wird der Standpunkt vertreten „*Ich habe nichts zu verbergen...*“, aber dies ist eine sehr kurzsichtige Einstellung und zeugt eher davon, daß derjenige sich nicht darüber im Klaren ist, welche Möglichkeiten die moderne Datenverarbeitung bietet. In einem hochgradig vernetzten System, in welchem die Daten quasi automatisch ausgetauscht werden, kann schon ein kleiner, vielleicht sogar falscher, Informationsbaustein fatale Folgen für den Betroffenen haben:

- Bei Bewerbungen um eine Wohnung kommen nur Absagen? Vielleicht sind Sie ja als schlechter Kreditnehmer bei der Schufa gebrandmarkt.
- Ihre Bestellungen werden, wenn überhaupt, grundsätzlich nur gegen Vorkasse angenommen? Nun, vielleicht wohnen in Ihrer unmittelbaren Umgebung zu viele potentielle Risikokandidaten („Sozialfälle“).
- Bewerbungen in sozialen Berufen bei kirchlichen Trägern werden abgelehnt? Sollte es an der Spende für den Verein „Hilfe für gleichgeschlechtliche Lebensgemeinschaften“ liegen?
- Ihre Lebensversicherung wird überraschend vom Versicherer gekündigt? Der privat bezahlte HIV-Test neulich kann ja eigentlich nichts damit zu tun haben, oder doch?

Realität oder Fiktion? Teils, teils. Aber in einer Welt ohne Datenschutz auf jeden Fall Realität. Entsprechende Dienstleister zur Bewertung der Wohnanschrift, Bonität und des möglichen Ausfallrisikos der Zahlung des potentiellen Kunden sind bereits im Einsatz.[6] Diese Prüfungen laufen bei Anmeldung und Bestellung vom Anwender unbemerkt im Hintergrund ab. Beliebt sind hier Abgleiche mit Datenbanken bei der Deuschen Post AG oder der Schufa.[7, 8] Allein die wenigen, genannten Beispiele zeigen wohl deutlich, daß es durchaus sinnvoll ist, nicht alles öffentlich verbreiten zu lassen und eine gewisse Kontrolle über seine Daten auszuüben. Jeder der schon einmal in die Fänge eines Inkassobüros wegen einer angeblich nicht bezahlten Rechnung geraten ist, kann sehr schnell die Auswirkungen einer ungehinderten Datenverbreitung zu spüren bekommen.

Auch geht es primär nicht darum, ob die Informationen falsch oder richtig sind, sondern nur darum, daß ohne Zutun des Betroffenen oder gar dessen Einverständnis Daten über ihn eingeholt, gespeichert und weitergegeben werden. Aus diesem Grunde erfüllt das BDSG auch zwei wesentliche Funktionen. Einerseits soll es die beliebige Datensammelei und das Austauschen der Daten begrenzen, andererseits gibt es dem Bürger das Recht Auskunft über die über ihn gespeicherten Daten zu verlangen.

Soweit zur Funktion gesetzlicher Regelungen. Besser jedoch ist es, die Verantwortung für sein Leben in die eigene Hand zu nehmen und bereits im Vorfeld die Datenmenge zu begrenzen die man über sich preisgibt.

Abgesehen von den genannten Punkten, muß man auch akzeptieren, daß *jeder* Mensch so etwas wie Privatsphäre

haben will. Was genau diese Privatsphäre ist, fällt von Mensch zu Mensch und von Kultur zu Kultur sehr unterschiedlich aus. Auch läßt sich die zukünftige Entwicklung nicht vorhersehen und was heute gedankenlos verbreitet wird, kann morgen schon zu massiven Problemen führen.

Datensammler

Man hat es mit zwei Gruppen von Datensammlern zu tun, gegen die man sich mit mehr oder weniger Erfolg zur Wehr setzen muss.

Auf der einen Seite gibt es die staatlichen Einrichtungen mit ihrem nahezu unbegrenzten Datenhunger alles über die Bürger in Erfahrung bringen zu wollen, vorgetragen immer mit dem Argument der Verbrechensbekämpfung und -vorbeugung. Das führt dann letztendlich soweit, das praktisch das ganze Volk unter Generalverdacht steht. Man denke bspw. an die seit 2002 geführte Diskussion und den kürzlichen Beschluss des Bundestages zur Reform des Telekommunikationsgesetzes alle Verbindungsdaten prophylaktisch — also ohne Verdachtsmomente — über längere Zeit zu speichern.[9-11] Verbindungsdaten bedeutet in diesem Falle sehr konkret u.a. folgendes:

- Wann wurde welche Nummer angewählt
- Die Gesprächsdauer
- Wem wurde wann eine SMS geschickt
- Welche Internet-Seiten wurden wie lange besucht
- Wann wurde eine E-Mail an wen geschrieben

Noch sind diese Vorschläge von der Regierung nicht abgesegnet, aber allein schon die Tatsache, daß ein vermeintlich demokratisch rechtsstaalicher Teil des Regierungssystems überhaupt solche Vorschläge auch nur in Erwägung zieht und dann auch noch beschließt, zeigt wie weit die Überwachungsmentalität bereits fortgeschritten ist. Auch ist es erstaunlich wie ruhig die Bevölkerung solche Ideen aufnimmt und ihnen teilweise sogar zustimmt. Vor gar nicht allzu langer Zeit wurde die DDR mit ihrem Überwachungssystem als Beispiel für ein Unrechtssystem drohend angeführt, immer mit dem Hinweis, daß es bei uns auf keinen Fall soweit kommen darf. Heute sind wir auf Grund der technischen Möglichkeiten in vielen Bereichen der Überwachung weiter als in der damaligen DDR und bauen diese mit immer weitergehenden Gesetzen aus, ohne das ein Aufschrei durch die Bevölkerung geht, der die politische Klasse endlich in ihre Schranken weist bevor es zu spät ist.

Ein weiteres Beispiel für staatliche Schnüffelei ist das einem totalitären Regime würdige Geldwäschegesetz.[12] Hierbei werden unter Anderen Banken dazu verpflichtet auffällige Geldbewegungen auf den Konten an behördliche Stellen zu melden. Bei Millionen von Konten ein hartes Stück Arbeit, gäbe es dafür nicht Computer, die dies vollautomatisch erledigen können. Das Prinzip ist dasselbe wie im ersten Beispiel, alle Bürger stehen von vornherein unter Generalverdacht – die Überwachung läuft auch hier permanent ohne Verdachtsmomente. Klar ist, daß der unschuldig Überwachte niemals davon erfährt, wann und welche Daten weitergleitet wurden.

Auf der anderen Seite betätigt sich die private Wirtschaft zunehmend als Datensammler. Die Techniken die unter dem Begriff des Dataminings — „Schürfen von Daten“ — zusammengefaßt werden, sind für die Auswertung großer Datenmengen entwickelt worden. Gemeint ist damit das effektive Suchen und Verknüpfen von Daten aller Art aus verschiedenen Quellen, um so bestimmte Querbeziehungen (Profile) oder deren Abwesenheit zu ermitteln. Erkenntnisgewinne die Wissenschaft und Forschung weiterbringen, führen bei Anwendung auf persönliche Daten zu einem massiven Verlust der Privatsphäre. [13, 14] Dementsprechend ist der Adresshandel ein einträgliches Geschäft. Selbst Unternehmen, die beim Durchschnittsbürger als vertrauenswürdig gelten, bspw. wie die Deutsche Post AG, handeln im großen Stil mit Adressen.[8] Problematisch dabei ist, daß im Zeitalter der Globalisierung immer mehr Daten über immer mehr Menschen in immer weniger, dafür aber größeren, Unternehmen zusammenkommen. Die Unternehmen begründen die Sammelleidenschaft oft mit schierer Notwendigkeit um optimale Produkte für die Kunden entwickeln zu können. Gemeint ist letztendlich damit nur, risikobehaftete Kunden vom Geschäftsverkehr auszuschließen und alle Übrigen mit möglichst starken, gezielten Kaufanreizen zu versorgen. Das Ergebnis beim Kunden ist aber ein fremdbestimmtes Handeln, dessen er sich noch nicht einmal bewußt ist. Ist der Kunde gut genug identifiziert, werden ihm beim Abruf bestimmter Internetseiten vom Unternehmen genau auf ihn zugeschnittene Inhalte auf den Seiten präsentiert. Dies betrifft dann nicht nur die inhaltsbegleitenden Werbebanner sondern auch die eigentlichen Inhalte, also Produktauswahlen, Texte, Meinungen usw. Somit wird langfristig für den Kunden eine unzensierte Informationsbeschaffung unmöglich gemacht. Der Kunde bekommt nur das zu sehen, was er sehen soll. Und genau dies gilt es zu vermeiden.

Zumindest in Deutschland hat man ein Recht auf Auskunft, welche Daten über einen bei einem Unternehmen gespeichert sind. In der Praxis dürfte es aber bereits zu spät sein, wenn man anfängt bei einem Unternehmen nachzufragen. Auch wenn das Beispiel der Schufa Schule machen sollte [7,15], daß man überall für die Selbstauskunft auch noch bezahlen soll (Schufa: 7,60 €), wird das Auskunftsrecht schnell eine teure Angelegenheit für den Bürger. Man muß sich klar machen, was hier passiert. Die Schufa sammelt persönliche Daten, *bewertet* sie und gibt sie gegen Entgelt an Dritte weiter. Für die Auskunft über die eigenen Daten wird dann frecherweise ebenfalls kassiert. Die Auskunft kann aber im Sinne des Bürgers auch noch als unvollständig bezeichnet werden, da zwar die gespeicherten, persönlichen Daten mitgeteilt werden, nicht aber die exakte Bewertung und wie sie zu Stande kam.

Anonymität

Oft wird angenommen, daß das Internet als anonymes Netz angelegt worden ist, was aber definitiv falsch ist. Das Internet, bzw. sein Vorgänger das Arpanet, ist als dezentrales, niemals aber anonymes Netz konzipiert worden. Alle am Internet angeschlossenen Computer sind logisch gleichwertig und eindeutig identifizierbar. Deshalb ist es auch bis heute nicht möglich, sich ohne größeren Aufwand wirklich anonym im Netz zu bewegen. In vielen Fällen bleibt dies rein prinzipiell unerreichbar, spätestens dann wenn man sich Waren schicken lassen will muß man aus der Anonymität hervortreten. Aber bis zu diesem Zeitpunkt sollte sie immer das angestrebte Ziel sein. In den meisten Fällen ist absolute Anonymität auch nicht unbedingt notwendig, Pseudonymität in Verbindung mit einem guten Datenschutz reicht vollkommen aus. Ein Beispiel soll dies vedeutlichen.

Jemand wählt sich mit seinem Computer in das Internet ein. Dabei teilt ihm der Zugangs-Provider, bei Privatpersonen also meist die Telefongesellschaft, eine weltweit einmalige IP-Adresse zu, d.h. der Computer ist von diesem Augenblick an eindeutig identifizierbar. Diese IP-Adresse wird benötigt damit sich die Computer untereinander ansprechen und Daten austauschen können. Gleichzeitig speichert der Provider die IP-Adresse in Verbindung mit der Telefonnummer um eine Leistungsabrechnung vornehmen zu können. Im Prinzip ist also der Anwender, besser gesagt der Anschlußinhaber, gegenüber dem Provider bekannt. Besucht jetzt der Anwender eine beliebige Homepage, erscheint dort im Logbuch u.a. die IP-Adresse mit der sich der Anwender z.Zt. im Internet bewegt. Über die IP-Adresse läßt sich also der Weg zum Anschlußinhaber zurückverfolgen, sofern der Provider nicht durch den Datenschutz davon abgehalten wird auf Nachfrage oder gar automatisch die Daten des Anschlußinhabers herauszugeben. Tut er dies nicht, ist der Anwender zwar definitionsgemäß nicht wirklich anonym, sondern nur pseudonym (in diesem Falle ist die IP-Adresse das Pseudonym), aber das Ergebnis ist durchaus vergleichbar. Werden die Daten nach der Rechnungsstellung wirklich gelöscht, so wandelt sich die anfängliche Pseudonymität in Anonymität, da jetzt der Weg nicht mehr zurückverfolgt werden kann. Für viele Zwecke ist dies auch ausreichend und wirksam. Daher versuchen viele Unternehmen ihr Ziel dem Kunden möglichst „nah“ zu kommen auf anderem Wege zu erreichen. Aber schon in dem Augenblick, wo der Zugangs-Provider, also das Unternehmen welches den Zugang zum Internet zur Verfügung stellt, gleichzeitig auch selbst Inhalte im Internet anbietet fallen alle Daten von vornherein in ein und demselben Unternehmen an. Unter diesen Bedingungen ist im Prinzip noch nicht mal Pseudonymität gewährleistet. Diese Konstellation ist so noch nicht der Regelfall, aber die Entwicklung geht eindeutig in diese Richtung. In solchen Fällen helfen wirklich nur Anonymisierungsdienste weiter, die durch verschiedene Maßnahmen die IP-Adresse verschleiern.[16, 17]

Kommunikation

Bei allen Bewegungen im Internet ist immer zu berücksichtigen, daß nicht nur die professionellen Datensammler ihre Datenbanken füttern wollen um anschließend manipulierend auf den Kunden einwirken zu können, sondern auch genügend Hacker unterwegs sind, die versuchen sich der Login-Daten von Anwendern zu bemächtigen um hinter deren Namen ihre eigenen Aktivitäten zu verbergen (Identitätsdiebstahl). Allein Letzteres ist ein hinreichender Grund niemals alle seine Aktivitäten unter *einem* Namen und *einem* Passwort zu bündeln.

Auch wenn man sich zur Benutzung von Anonymisierungsdiensten [16, 17] entschlossen hat, kommt man nicht umhin, die meisten der nachfolgenden Vorschläge zu beachten, denn was nützt der anonyme Besuch einer Webseite, wenn dort Name und Anschrift hinterlassen werden?

e-Mail

Jede e-Mailadresse ist weltweit einmalig. Ein kleine Feststellung, aber man muß sich die Bedeutung klar machen. Einmal mit persönlichen Daten verknüpft kommt das einer weltweit gültigen Personenkennzahl gleich. Was politisch mit Pässen und Personalausweisen nicht durchsetzbar sein würde, ist im Internet beinahe gang und gäbe. Insbesondere Personen die sich ihre eigene Domäne haben registrieren lassen, werden somit recht transparent, wenn sie alles darüber abwickeln, denn die Anschrift kann bei der jeweiligen Registratur nachgeschlagen werden. Für Deutschland — Domänen des Typs www.xyz.de — ist hier das DENIC zuständig.[18, 19] Der Unsicherheitsfaktor besteht eben nur noch darin, daß eine e-Mailadresse beliebig gewechselt werden kann.

Aber auch alle anderen sollten auf keinen Fall alle ihre Aktivitäten nur über *eine* e-Mailadresse abwickeln. Deutlich wird das Problem fehlenden Datenschutzes beim Problem des Werbemülls („Spam“). Hinterläßt man überall seine e-Mailadresse, bleibt es nicht aus, daß über kurz oder lang Unmengen an Werbemails eintreffen, aus denen die für einen wichtigen e-Mails heraussortiert werden müssen. In einigen Fällen werden in den Spam-Mails Links zum Abmelden angeboten — wie auch bei den Werbefaxen [20] für 0190 und den neueren 0900[1]-Nummern Telefonnummern dafür angeboten werden —, aber man sollte *niemals* darauf eingehen, denn damit bestätigt man die jeweilige Adresse und macht klar, daß deren Inhalt gelesen wird! Bei den Werbefaxen bezahlt man sogar noch das Telefongespräch für die vermeintliche Abbestellung. Es gibt inzwischen auch offizielle „Robinson-Listen“ für e-Mails [21], aber auch deren Wirkung ist zweifelhaft. Die eigentlichen Spammer werden sich sowieso nicht daran halten und wenn ihnen eine solche Liste einmal in die Hände fällt oder gar von ihnen betrieben wird, ist der Schaden nicht wieder zu beheben. Bei Adresshändlern erzielen Adressen von Robinsonlisten einen deutlich höheren Preis, da die Adressen nicht nur bestätigt sind, sondern die Personen auch erwartungsgemäß weniger Werbung erhalten und damit die Wahrscheinlichkeit des Gelesenswerdens höher ist.

Etliche Webseiten haben sich die Information über und Bekämpfung von Spam auf die Fahnen geschrieben [22, 23] und inzwischen beschäftigt das Problem Spam selbst die Politik, aber ob in naher Zukunft von dort tatsächlich eine wirkungsvolle Lösung kommt, darf bezweifelt werden. Hier muß man sich einfach klar machen warum es Spam in diesem Umfang überhaupt gibt. Das Sammeln von Adressen ist recht einfach, da dazu nur Webseiten und Newsgroups automatisch nach e-Mailadressen durchsucht werden müssen. Solche Sammlungen werden dann für wenige Euro pro Million Adressen verkauft. Das Versenden der Werbemails erfolgt dann über ungeschützte Mailserver. Die geringen Kosten für die Werbeaktion sind aber nicht der eigentliche Grund, sondern die Anwender selber! Jeder der auch nur einen einzigen Kauf auf Grund einer solchen Werbemail tätigt ist der Schuldige und alle anderen dürfen die Suppe dann ausbaden. Ändern wird sich dies nicht lassen, also müssen andere Maßnahmen zum Schutze herangezogen werden. Dies ist dadurch erreichbar, daß man sich ein regelrechtes Netzwerk aus e-Mailadressen zulegt. Um das zeitaufwendige Abfragen etlicher Postfächer zu vermeiden kann man hier auf die Weiterleitungsfunktion („forwarding“ und „redirect“) zurückgreifen, die viele e-Mail-Dienstleister anbieten. Einige Dienstleister bieten auch eine Abholfunktion für e-Mailpostfächer (POP3-Abruf) an, d.h. man hinterlegt bei einem Dienstleister Login und Paßwort für ein anderes Postfach, welches dann in regelmäßigen Abständen automatisch abgefragt wird. Ob man dieses Angebot wirklich annehmen sollte hängt im Wesentlichen vom Vertrauen ab, welches dem Unternehmen entgegengebracht wird. Vom sicherheitstechnischen Standpunkt aus ist die Weiterleitung vorzuziehen.

Am besten legt man sich für unterschiedliche Zwecke spezialisierte e-Mailadressen nach dem Zwiebelschalenmodell (Abb. 1) zu, beispielweise nach folgendem Schema:

- Newsletter von deutschen Unternehmen (pseudonym)
- Newsletter von anderen Unternehmen (pseudonym)
- Newsletter von Informationsdiensten (pseudonym)
- Einkäufe (personalisiert)
- rein private Kontakte
- sonstige Aktivitäten
- 2-3 Sammelkonten, als Weiterleitungsempfänger
- „Tote Postfächer“

Die „Toten Postfächer“ sollen überall dort angegeben werden, wo zwar eine e-Mailadresse verlangt wird, man aber eigentlich keinen e-Mailkontakt wünscht. Hierfür kann man sich ein spezielles Postfach einrichten oder auf die dazu eingerichteten Adressen von Privacy.net

[1] Die 0190-Servicenummern sollen bis Ende 2005 durch die international gültigen 0900-Nummern ersetzt worden sein. Neues Spiel, selbe Masche.

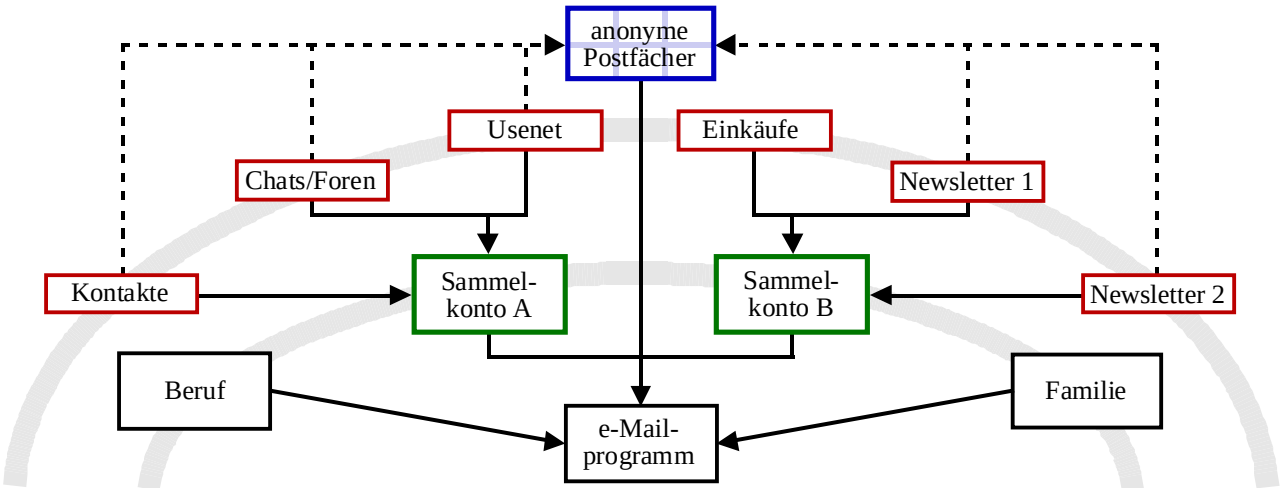

Abbildung 1: Schematische Darstellung eines halbwegs sicheren Netzes von Mailkonten nach dem Zwiebelschalenmodell. Die gezeigte Struktur gewährt einen effektiven Schutz der Privatspähre und verhindert eine allzu große Belästigung durch Werbemails. Laufen in einem der Weiterleitungskonten (rot) zuviele Werbemails ein, wird dieses einfach abgemeldet und durch ein Neues ersetzt, ohne das man allen seinen Kontakten eine neue e-Mailadresse mitteilen muß. Die Sammelkonten (grün) dienen dazu den Abfrageprozeß durch das e-Mailprogramm zu beschleunigen und erleichtern das Einrichten und Abmelden von e-Mailkonten, da das e-Mailprogramm nicht umkonfiguriert werden muß.
Echte anonyme Postfächer können nur durch direkte Abfragen über Anonymisierungsdienste aufrecht erhalten werden.

(me@privacy.net, me0@privacy.net, ..., me9@privacy.net) zurückgreifen.[24] Alles was bei diesen Postfächern eingeht wird mit einer kurzen automatischen e-Mail mit Hinweis auf die Privatsphäre und der Sinnlosigkeit weiterer Mails an diese Adresse beantwortet und dann gelöscht. Es wäre durchaus wünschenswert, wenn auch andere Domäneninhaber diese Idee des „Toten Postfaches“ für jedermann aufgreifen würden. Technisch ist es einfach zu realisieren und verursacht außer der einmaligen Einrichtung keine weitere Arbeit, da auf eingehende e-Mails nur durch eine kurze automatische Antwort reagiert werden muß bevor sie gelöscht werden.

Es kann nicht schaden, die personalisierten Postfächer durchaus mal zu wechseln. Domäneninhaber sollten darauf achten, daß nur die rein privaten Postfächer über die eigene Domäne laufen, alle anderen sollten an externe kostenlose e-Maildienstleister („freemailer“) ausgelagert werden [25-28], sofern diese gewisse Mindestanforderungen erfüllen:

- kostenlos
- Weiterleitungsfunktion
- POP3-Abruf
- Anonyme Nutzung möglich
- Spam-Schutz

Nach diesen Kriterien fallen bspw. zwei recht bekannte deutsche Dienstleister sofort durch das Raster, Web.DE und ePost.[27, 28] Es kann überaus lohnenswert und sinnvoll sein, sich auch unter ausländischen Maildienstleistern („freemail, webmail“) umszusehen. Das Internet ist ein globales Medium und sollte auch als solches behandelt werden.

Nicht zu vergessen bleibt der Hinweis, daß e-Mails als reiner Text durch das Internet geleitet werden. Jeder der Zugang auf eine Zwischenstation hat kann den Datenverkehr zwischen Sender und Empfänger unbemerkt lesen und weiterleiten, ja sogar verändern. In der realen Welt werden u.a. aus diesem Grunde Briefumschläge benutzt und niemand käme auf Idee jemandem daraus einen Vorwurf zu machen. Warum also in der virtuellen Welt alles für jedermann frei lesbar durch die Netze schicken?

Sensible und private Daten die per e-Mail versandt werden gehören daher in einen elektronischen Umschlag, d.h. verschlüsselt. Web.DE bietet zwar eine solche Möglichkeit standardmäßig an, aber der Nutzer wiegt sich in falscher Sicherheit („Verschlüsselung für Arme“). Der Anwender ist nicht Herr über seine Schlüssel, sie werden von Web.DE verwaltet. Einerseits praktisch, aber wer kann sagen was tatsächlich damit geschieht und bei der ersten staatlichen Anforderung wird sich das Unternehmen aller Wahrscheinlichkeit nach nicht schützend vor seinen Kunden stellen. Außerdem funktioniert das nur zwischen Web.DE-Benutzern, aber nicht zwischen beliebigen e-Mailadressen. Besser ist es auf die bewährte freie Software von PGP und Verwandten zurückzugreifen.[29-31] Standardisierung, Sicherheit, Betriebssystemunabhängigkeit und volle Kontrolle über die eigenen Schlüssel sind die unschätzbaren Vorteile vor allen anderen Lösungen.

Der konsequente Einsatz von PGP kann mit dazu beitragen den Spamversendern das Leben schwer zu machen. Wenn man auf seiner rein privaten e-Mailadresse nur PGP verschlüsselte e-Mails akzeptiert und alle anderen radikal löscht, bleibt zumindest dieses Postfach sauber.

Eine weitere häufig gemachte Unachtsamkeit — durchaus auch von professionellen Anwendern —, mit der e-Mailadressen unnötig verbreitet werden, ist mittels Rundschreiben. Werden die Empfänger in das „To“- oder „Cc“-Feld („Carbon copy“ = Kohledurchschlag) eingesetzt erhalten alle Empfänger auch die komplette Adressenliste. Dies ist nur in seltenen Fällen wirklich sinnvoll. Besser ist es, das in praktisch allen e-Mailprogrammen vorhandene Feld „Bcc“ („Blind carbon copy“) für die Empfängerliste zu verwenden. So erhält jeder Empfänger die e-Mail, aber ohne die e-Mailadressen aller Teilnehmer.

Pseudonyme

Der Umgang mit Pseudonymen erfordert im Grunde die gleiche Vorgehensweise wie bei den e-Mailadressen. Für jeden Zweck ein anderes Pseudonym, kombiniert mit einer anderen e-Mailadresse. Der eigene wahre Name sollte niemals in irgendwelchen Diskussionsforen auftauchen, weder als Login-Name, noch in der Signatur eines Beitrages. Sollten sich weitergehende persönliche Kontakte ergeben, ist immer noch Zeit genug seinem Gegenüber den Realnamen mitzuteilen.

Usenet (Newsgroups)

Das Usenet, gemeinhin als Newsgroups bezeichnet, ist mit der älteste und größte Teil des Internet. Leider geraten durch das WWW die Newsgroups gar nicht erst in das Blickfeld der meisten Anwender, obwohl es für viele Dinge besser geeignet ist. Gerade die verbreiteten Diskussionsforen sind im WWW eine äußerst langsame und unpraktische Angelegenheit.

Allerdings ist das Usenet auch eine beliebte Quelle für die e-Mailsammler. Einmal in eine „falsche“ Newsgroup gepostet und die Adresse ist einige Zeit später nicht mehr sinnvoll nutzbar. Dementsprechend kann nur dringend davon abgeraten werden seine wahre e-Mailadresse an irgendeiner Stelle dort anzugeben, allerhöchstens in verschleierter Art und Weise (IchKEINSPAM@Domain.DE für Ich@Domain.DE). Zu empfehlen ist aber definitiv die Verwendung eines „Toten Postfaches“. Im deutschen Usenet wird man sich hier dadurch sehr schnell einen Rüffel einiger selbsternannter Usenetpolizisten einhandeln, die man aber getrost ignorieren kann. Die Drohung von ihnen in den „Kill-File“ (Schwarze Liste) aufgenommen zu werden, kann man getrost ignorieren, vermutlich bekäme man von ihnen sowieso keine brauchbare Antwort. Allerdings sollte man wirklich darauf achten standardkonforme Usenetsoftware zu verwenden, wozu Outlook jedenfalls nicht gehört.

Die eigene Sicherheit geht vor, zumal auch jedes noch so kleine Posting auf unbestimmte Zeit archiviert wird. Dementsprechend sollte auch für Postings in verschiedenen Newsgroups unterschiedliche Pseudonyme verwendet werden. Die Ergebnisse einer Suche bei Google nach der eigenen Mailadresse oder dem eigenen Namen hat schon Manchen überrascht. Darüberhinaus steht es einem bei Bedarf frei, einzelnen Teilnehmern seine e-Mailadresse mitzuteilen.

Ein ebenfalls nicht zu unterschätzender Vorteil eines derart gestaffelten Verteidigungswalles ist ein gewisser Schutz vor Viren, Würmern und Trojanischen Pferden. Die zur Zeit herrschende Belastung des Netzes mit diesen Schädlingen wird sicherlich in der nächsten Zeit noch weiter drastisch zunehmen, da viele Anwender nicht Willens sind mal ein anderes Betriebssystem, ja nicht einmal ein anderes Mailprogramm anstelle von Outlook und Outlook Express, auszuprobieren und auch ihre Rechner nicht genügend abschotten. Inzwischen bieten aber viele Provider ihren Kunden kostenlosen oder kostenpflichtigen Virenschutz an. Laufen eingehende Mails über mehrere Provider, hat man eine gute Chance zumindest nicht mehr von den bekannten Schädlingen belästigt zu werden.

Geschwätzige Software

Eine ganze Reihe von Programmen kann nur dann in vollem Umfang genutzt werden, wenn eine Freischaltung erfolgt ist. Meist geschieht dies durch Eingabe einer Seriennummer. Oft werden dabei unnötigerweise auch gleich noch weitere Daten abgefragt. Um die Eingabe der Seriennummer kommt man nicht herum, aber bei allen anderen persönlichen Angaben sollte man äußerst fantasievolle Eingaben wählen. Der Grund dafür liegt in der Unvorhersehbarkeit für den Anwender was mit den Eingaben geschieht und wo diese gespeichert werden. Eine Reihe von Programmen schreibt diese Daten in jedes Dokument. Selbst bei e-Mailprogrammen wurden schon Name und Serienummer als spezielle Kopfzeilen („x-Header“) in den e-Mails gefunden. Immerhin geht es hier

nicht nur um die Privatsphäre allein, sondern auch um Investitionsschutz, denn die Serienummer dient oft als Grundlage für den Erwerb preiswerterer Updates. Dem Mißbrauch ist so Tür und Tor geöffnet.

Besonders geschwätzig zeigen sich in dieser und anderer Hinsicht die Programme aus dem Hause Microsoft.Hier gibt es zwei Probleme. Einerseits wird in einigen Versionen eine eindeutige Kennung (GUID, Global Unique Identifier) im Dokument abgespeichert (einfach mit einem Hex-Editor nach „PID-GUID“ suchen) [32-35], andererseits enthalten Textdokumente auch noch ältere, vermeintlich gelöschte Texteile aus dem Korrekurprozeß eines Dokumentes. Es besteht dadurch die Möglichkeit nachzuvollziehen wann durch wen welche Änderungen vorgenommen wurden. Das es sich hierbei nicht nur um eine Gedankenspielerei handelt hat der Vorfall des Word-Dokuments um Tony Blair zum Irakkrieg mehr als deutlich gezeigt.[36, 37]

Das Ergebnis kann nur sein, das man niemals irgendwelche Office-Dokumente außer Haus gibt, weder per e-Mail noch auf einem Webserver zum Runterladen. Die sichersten Dateiformate sind diesbezüglich reiner ASCII-Text und — zumindest bisher — das layouttreue PDF, in dem auch dieser Artikel vorliegt. Auch bei anderer Software sollte man ein gesundes Mißtrauen walten lassen, denn vielleich sind diverse Dinge nur noch nicht bekannt geworden. Übrigens stellen auch deutsche Behörden regelmäßig Word und Excel-Datein in das Netz.

World Wide Web (WWW)

Immer mehr Angebote im Internet gehen dazu über ihre Besucher wesentlich genauer unter die Lupe nehmen zu wollen, als es eigentlich für den Gebrauch des Angebotes notwendig wäre. Die Information kommt aus mehreren Quellen:

- Die Browser geben standardmäßig Daten preis. So unter anderem, von welcher Webseite der Anwender kommt („Referrer“). Dies läßt sich nur bei sehr wenigen Browsern ausschalten. Will man die so gelegte Spur unterbrechen, hilft nur die umständliche Methode, jeden Link den man ansurfen will auf der Ursprungsseite zu kopieren, um ihn dann in einer neuen separaten Browserseite in die Adressleiste einzusetzen und abzuschicken.
- Beim Abrufen der Webseite wird ein kleines Datenpaket („Cookie“) auf dem Rechner des Anwenders platziert. Der Dateninhalt ist vom Programmierer frei wählbar, aber er dient immer dazu, den Besucher zu identifizieren. Da die Cookies auf dem Rechner des Anwenders gespeichert sind, können sie so bei einem späteren Besuch der Webseite wieder ausgelesen werden. Der Besucher sieht das manchmal daran, daß er in irgendeiner Form persönlich begrüßt wird, ohne sich eingeloggt zu haben. Beim Anlegen eines Cookies ist zwar ein Verfallsdatum vorgesehen, aber dieses wird von den Webseitenbetreibern meistens auf Jahre in die Zukunft verlegt (typischerweise 2038). Für den Anwender heißt dies, daß er spätestens nach Abschluß seines Surftripps die Cookies selber löschen sollte, sofern er nicht einen der wenigen Browser verwendet, bei denen dies in den Einstellungen festgelegt werden kann.
- Speziell präparierte Webseiten können weitere Daten über den Computer und seine Software auslesen.

Eine vierte Quelle erfordert die aktive Mitarbeit des Anwender, die Anmeldung mit Benutzername (oft die e-Mailadresse) und -passwort, in vielen Fällen präsentiert mit einem mehr oder wenigen umfangreichen Fragebogen zu den Vorlieben des Anwenders. An dieser Stelle gilt es jetzt für den Anwender zu entscheiden, ob er nur einen einmaligen Besuch, vielleicht nur zur Probe, oder tatsächlich eine längerfristige Beziehung plant. Im ersten Fall sollte er einfach die Adresse eines „Toten Postfaches“ (vgl. Kapitel E-Mail) wählen. Passwort und Fragebogen können nach dem Zufallsprinzip ausgefüllt werden. Auch ansonsten sollte man mit wahren Angaben sehr sparsam umgehen. Bei sporadischen Besuchen von Webseiten die ein Login erfordern, sollte man sich jedesmal neu Anmelden. Das erscheint vielleicht etwas hinderlich, aber es zerstört recht effektiv den Versuch der Datengewinnung über den Besucher. Gleichzeitig erspart dieser sich aber auch die Arbeit, die durch die Verwaltung der jeweiligen Login-Daten entsteht.

Zu den am häufigsten erfragten Daten — im Internet wie außerhalb — ist das Geburtsdatum. An Hand dessen wird der Kunde in entsprechende Käufergruppen (Zielgruppen) eingeordnet. Besonders offensichtlich wird dies bei Telefonumfragen. Wird die entsprechende Frage bspw. mit 75 beantwortet hat der Anrufende Interviewer schlagartig kein Interesse an einer Weiterführung der Befragung.

Dieses Wissen kann man nutzen um sich bewußt einer nicht relevanten Gruppe zuzuordnen. Fast überall müssen die Unternehmen, insbesondere aber in den USA, sehr genau kontrollieren ob und welche Werbung Minderjährigen zugestellt werden darf. Jung bleiben heißt also oftmals die Devise.

Telefonnummern

Nach dem bisher gesagten eigentlich kaum noch erwähnenswert, aber private Telefonnummern sind ebenfalls keine geeignete Angabe in e-Mails, Forenbeiträgen, auf Webseiten oder gar in Formularen von Anbietern, sofern es nicht unbedingt notwendig ist, was allerdings nur in äußerst seltenen Fällen Vorkommen dürfte.

Darüberhinaus können die noch wenig verbreiteten persönlichen 0700-Rufnummern (Vanity-Nummern[2]) [38] als einzige Telefonnummer ohne Angabe der Kosten auf Webseiten als Folge eines Urteils [39] auch noch zu Abmahnungen führen.[40-42]

Noch ist Telefonmarketing, d.h. das Anrufen von Personen mit denen keine Geschäftsbeziehung besteht, in Deutschland verboten, aber niemand kann vorhersagen ob dies tatsächlich so bleibt. Voller Neid blicken die Firmen in die USA wo diese Art der abendlichen Belästigung gang und gäbe ist. Entsprechend stark ist auch der Druck den Lobbygruppen auf politischer Ebene ausüben um eine Aufhebung des Telefonmarketingverbots zu erreichen.

Auch ist in Deutschland die retrograde Telefonnummernsuche, d.h. die Ermittlung des Inhabers an Hand der Nummer, verboten, nur eben im Ausland nicht. Ein Unternehmen kann also im Ausland eine solche Dienstleistung anbieten. Für amerikanische Rufnummern geht dies einfach über die Suchmaschine Google.[43, 44] Hierfür muß man nur in das Suchfeld das Kommando

phonebook: (xxx) xxx-xxxx

eingeben. Google präsentiert daraufhin eine Ergebnisliste mit Namen und Anschrift.

Darüberhinaus können die noch wenig verbreiteten

Kaufen und Verkaufen

Bankkonto

Jeder der im Internet einkauft oder Waren feilbietet muß sich Gedanken über ein für ihn geeignetes Abrechnungsverfahren machen.[45-51] Privatleute und Kleinunternehmen werden hier aus Kostengründen auf das ganz normale Girokonto zurückgreifen. Jeder hat und kennt es, Überweisungen sind sehr preiswert und neuerdings sogar EU-weit ebenso problemlos und preiswert unter Verwendung der internationalen Bankleitzahl und Kontonummer durchführbar wie innerhalb Deutschlands.[52-55] Aber auch hier ist man nie ganz vor Missbrauch geschützt und je mehr Leute die Kontoverbindung kennen, desto größer wird die Wahrscheinlichkeit eines Tages selbst Betrugsopfer zu sein. Gerade Verkäufer sind oft darauf angewiesen ihre Bankverbindung einem sehr großen Personenkreis bekannt zu geben, oftmals direkt auf einer Internetseite.

Ohne auf illegalem Weg irgendwelche Daten ausspähen zu müssen bietet das Girokonto allein durch Kenntnis von Bankleitzahl und Kontonummer zwei Angriffspunkte für Betrügereien:

- *Lastschriften*

  Bei vielen Unternehmen besteht oft die Möglichkeit den fälligen Betrag durch das wirklich kundenfreundliche Verfahren der Lastschrift (Einziehungsauftrag) vom Konto abbuchen zu lassen.

  Im Internet erfolgt der Einkauf per Lastschrift nicht per Unterschrift, sondern einfach durch Angabe des Kontoinhabers, der Kontonummer und der Bankleitzahl. Der Kontoinhaber wird bei der automatischen Datenverarbeitung nicht immer standardmäßig geprüft, da nicht alle Banken Namenskonten führen. Abgesehen davon, das dies auch nicht viel Nützen würde. Das Unternehmen liefert die Ware oder Dienstleistung und einige Tage später erfolgt die Belastung des Kontos. Insbesondere bei Waren die auch über das Internet ausgeliefert werden können (Bilder, Filme, Musik, Software) ist dieses Verfahren für den Betrüger recht sicher.

  Bei ungerechtfertigten Abbuchungen hat man sechs Wochen Zeit um den abgebuchten Betrag ohne Begründung zurückbuchen zu lassen. Dies erfolgt einfach durch einen Anruf bei der kontoführenden Stelle. In der Regel ist das Geld 1-2 Tage später wieder auf dem Konto. Zum Problem kann das werden, wenn zum Monatsende oder -anfang weitere, gerechtfertigte Beträge (bspw. Miete) durch Lastschriften eingezogen werden sollen. Ist die Kontodeckung zu gering wird die Lastschrift nicht ausgeführt. Neben den Mahnungen über ausstehende Beträge werden einem hierbei auch noch die Gebühren der

[2] Hierbei werden anstelle der Nummern Buchstaben gewählt. Jeder Taste sind Buchstaben zugeornet (wie bei den SMS auf Mobiltelefonen).

Banken (ca. 10-20 €) für nicht ausgeführte Lastschriften von den betroffenen Unternehmen in Rechnung gestellt. Theoretisch könnte man den Verursacher, sofern er gefasst wird, auf Schadenersatz verklagen. In der Praxis dürfte man wohl auf diesem Schaden sitzen bleiben.

- *Überweisungen*
  Jeder kann ein Überweisungsformular ausfüllen und irgendeine Unterschrift darunter setzen. Ist der Betrag nicht allzu hoch, besteht eine gute Wahrscheinlichkeit, daß die Überweisung trotz falscher Unterschrift ausgeführt wird. Bei den gefälschten Überweisungen ist es etwas schwieriger sein Geld zurückzufordern, da man hier die Bank dazu bewegen muß, den Überweisungsträger herauszusuchen und explizit zu kontrollieren. Vom ökonomischen Standpunkt aus macht dieses Verhalten aus Sicht der Bank Sinn. Es ist preiswerter einige Betrugsversuche in Kauf zu nehmen und dem geprellten Kunden sein Geld zurückzuerstatten, als jede noch so kleine Überweisung zu kontrollieren.

In beiden Fällen kann man aber davon ausgehen, sein Geld zurückzubekommen und ohne größeren Schaden davonzukommen. Aber den Schrecken, die diversen Telefonate und den Gang zur Polizei für die Strafanzeige hat man in jedem Falle am Hals.

Übrigens sollte man es nach Entdeckung des Betruges nicht einfach beim Rückruf des Geldes und einer Strafanzeige belassen. Oft läßt sich dem Buchungstext auf dem Kontoauszug auch das abbuchende Unternehmen und eine Kundennummer entnehmen. Am besten man ruft dann sofort das abbuchende Unternehmen an, damit dieses selbst Schadensbegrenzung durch Sperrung des Kunden und Beweissicherung betreiben kann. Anschließend werden die Unternehmen auch eine Kopie (per Fax reicht) der Strafanzeige haben wollen.

Gerade Verkäufer, die eigentlich nur Geldeingänge auf ihrem Konto zu erwarten haben, können sich recht wirkungsvoll vor möglichen Betrugsversuchen schützen. Benötigt wird ein Konto auf das jedermann wie gewohnt Geld überweisen oder einzahlen kann, aber bei dem keine Überweisungen oder Lastschriften ausgeführt werden. Sparbücher und Tagesgeldkonten erfüllen genau diese Bedingungen. Sparbücher sind zwar prinzipiell brauchbar aber weniger geeignet, da sie meist nicht online geführt werden können und man Geld oft überhaupt nicht auf ein anderes Konto überweisen kann, sondern nur am Schalter abheben kann. Tagesgeldkonten mit ihrer kostenfreien Online-Kontoführung, der täglichen Verfügbarkeit des Geldes und der Möglichkeit ein Referenzkonto anzugeben, auf das *alle abgehenden* Zahlungen geleitet werden, machen sie zum idealen Werkzeug für Verkäufer.

Auf Grund des eingangs bereits erwähnten Überweisungsverfahrens per IBAN und BIC [54, 55] ist man nicht einmal darauf angewiesen, ein solch preiswertes Konto in Deutschland zu führen, was durchaus noch andere Vorteile haben kann.

Zum Abschluss des Themas Bankkonto noch zwei Tipps, die vollkommen unabhängig vom Internet sind.

Bei vielen Familien ist es immer noch üblich nur ein Girokonto zu führen, selbst dann, wenn sich das Familieneinkommen aus zwei Gehältern zusammensetzt. Eine auf den ersten Blick praktische Lösung, kann sich im Falle eines Problemes zu einer finanziellen Katastrophe ausdehnen. Nehmen wir einmal an, das Konto wird — aus welchen Gründen auch immer — vorübergehend gesperrt. Dies bedeutet, das Zahlungseingänge (bspw. Gehälter) weiter verbucht werden, aber keine Zahlungen (bspw. Lastschriften für Miete, Gas, Wasser, Abhebungen am Geldautomaten etc.) mehr geleistet werden. Nun könnte man meinen, das es kein Problem darstellt schnell ein anderes Konto bei einer anderen Bank zu eröffnen und dem Arbeitgeber die neue Kontoverbindung mitzuteilen. Bei Kontoeröffnungen erfolgt aber immer eine Abfrage bei der Schufa.[7] Sind dort entsprechende Negativmerkmale gespeichert, wird die Kontoeröffnung verweigert, unter Umständen mit fadenscheinigen Begründungen. Bis man die Ursache entdeckt und bereinigt hat, wird dies ohne Geld eine äußerst schwierige Lebensphase werden. Besitzt aber der Partner ein eigenes Konto, läßt sich eine gewisse, wenn vielleicht auch verminderte, Zahlungsfähigkeit aufrecht erhalten, da Geldflüsse noch steuerbar bleiben. Da es heute problemlos möglich ist gebührenfreie Girokonten zu führen, besteht auch kein Hinderungsgrund mehr, nicht für jeden ein separates eigenes Konto einzurichten und somit auch auf solche Fälle halbwegs vorbereitet zu sein.

Der zweite Tipp bezieht sich auf die allenthalben verbreiteten Gewinnspiele mit ihren Gewinnversprechungen. Abgesehen davon, daß es sich hierbei praktisch immer um Bauernfängerei handelt und man diese Schreiben getrost sofort dem Altpapiercontainer überlassen kann, sollte man, wenn man es denn gar nicht lassen kann, wenigstens niemals seine Girokontonummer für eventuelle Gewinnaus-

zahlungen angeben. Benutzen Sie hierfür grundsätzlich nur Kontonummer und Bankleitzahl eines (brachliegenden) Sparbuches. Wenn denn tatsächlich Geld eingehen sollte, muss man den Betrag schlimmstenfalls bei der Bank kündigen oder kommt erst in ein paar Monaten in den Genuss des Geldes. Aber man besitzt die Sicherheit, daß mit den Kontodaten kein Schindluder getrieben werden kann.

Identitätsprüfung

Einige Unternehmen verlangen inzwischen eine zweifelsfreie Feststellung der Identität eines Kunden, entweder um gesetzlichen Auflagen, wie bei der Volljährigkeitsprüfung für das Jugendschutzgesetz, nachzukommen oder einfach um sich selbst vor Betrug zu schützen. Zur Identitätsfeststellung wird je nach Unternehmen entweder eine Fotokopie der Personalpapiere oder auch „nur“ der EC-Karte verlangt. In Deutschland sind sowohl der Personalausweis als auch der Reisepass dafür geeignet seine Identität rechtsgültig nachzuweisen. Da man als Kunde keine Kontrollmöglichkeit über die angefertigten Kopien hat, sollte immer auch nur eine Fotokopie des Reisepasses, niemals des Personalausweises eingereicht werden. Dadurch bleibt man frei in der Angabe der Adresse und bei Weitergabe der Fotokopien an Dritte wird wenigstens vielleicht nicht sofort auch die Anschrift dazugeliefert. Diese läßt sich zwar recht einfach über die zuständige Meldebehörde in Erfahrung bringen, aber es ist eine — wenn auch kleine — Hürde mehr. Außerdem läßt sich dieser Prozeß nicht einfach automatisieren.

Zum Abschluss dieses Abschnittes auch wieder ein Tipp fern des Internets. Bei Reisen im Ausland wird oft bei Hoteleinbuchungen und anderen Gelegenheiten die Heimatadresse verlangt. Auch hier gilt es, niemals die wahre Adresse anzugeben. Vom Hausschlüsseldiebstahl aus dem Hotelzimmer bzw. dem Anfertigen von Kopien derselben bis zu Forderungen von Alimenten nach der Rückkehr sind hier viele Gelegenheiten für Gauner gegeben. Am besten man legt sich für diese Zwecke bereits vor der Abreise einige stimmige Adressen, d.h. Straße, Hausnummer und Postleitzahl müssen zusammen passen, zurecht.

Handelsplattformen (Versteigerungen)

Das Internet hat sich inzwischen auch als Handelsplatz für jedermann etabliert. Das Zusammenführen von Käufern und Verkäufern ist die Geschäftsgrundlage einiger Unternehmen, von denen Ebay allerdings die bekannteste Marke sein dürfte.[56-61]

Hinter den Webseiten mit den Angeboten stehen umfangreiche Datenbanksysteme zur Speicherung und Verwaltung der Kundendaten und der einzelnen Versteigerungen. Man muss immer davon ausgehen, daß die dort vorliegenden Daten sehr lange gespeichert bleiben (allein schon aus steuerlichen Gründen), auch wenn sie längst nicht mehr über die Internetseite abrufbar sind. Auch hier gilt es, darüber nachzudenken, was eigentlich mit diesen Daten tatsächlich geschieht, unabhängig von rechtlichen Vorschriften, die je nach Land sehr unterschiedlich ausfallen. Aber auch mit den über das Internet zugänglichen Kauf- und Verkaufsvorgängen, läßt sich ein recht gutes Interessenprofil über den Teilnehmer erstellen. Systembedingt läßt sich hier die unwillkürliche Datenanhäufung nicht vermeiden, aber man kann in gewissem Maße dazu beitragen, daß das Zusammenführen für Dritte nicht ganz so einfach wird. Die einfachste Maßnahme besteht darin, daß man sich für Kauf und Verkauf zwei unterschiedliche Benutzerkonten anlegt. Es ist nicht notwendig das Bankkonto für Käuferzahlungen sofort anzugeben. Erst nach dem Ende einer Auktion, ist der richtige Zeitpunkt dem Käufer per e-Mail die Bankverbindung mitzuteilen. Als Käufer werden wesentlich weniger Daten von einem eingefordert und Dritte können sich nicht so leicht einen Überblick über ihre gesamten Handelsaktivitäten verschaffen. Das Käuferkonto sollte in regelmäßigen Abständen gewechselt werden, d.h. das alte Kundenkonto wird gelöscht und man meldet sich als Neukunde an, inklusive neuer e-Mailadresse. Als Käufer hat man es hier besonders einfach, da man im Grunde nicht auf (positive) Bewertungen angewiesen ist und somit keine Nachteile zur befürchten hat. Einige Unternehmen verschärfen die Datensammlung derart, daß sich einmal eingegebene Daten wie Kreditkartennummer oder Bankkonto nachträglich nur mehr einfach ändern lassen.[58, 62]

Ansonsten sollte man auch trotz aller Begeisterung für die Möglichkeiten dieser Handelsplattformen nicht den gesunden Menschenverstand ausschalten.[63, 64] In keinem Laden der Welt würde man Waren für mehrere hundert Euro allein auf Grund des Versprechens später zu bezahlen einfach so ausgehändigt bekommen. Auch würde niemand auf dem Flohmarkt jemandem mit dem Hinweis „schicken Sie mir das mal“ Geld in die Hand drücken. Treuhanddienste sollen genau dieses Vertrauensproblem lösen, aber das funktioniert nur, wenn der Treuhanddienst selber vertrauenswürdig ist. Bloß weil eine Webseite diese Dienstleistung anbietet heißt das noch lange nicht, daß sie auch vertrauenswürdig ist. Auch solcherlei Webseiten sind

innerhalb weniger Minuten erstellt. Man sollte also nur dann einen Treuhanddienst benutzen, wenn man auf irgendwelche Referenzen die man auch nachvollziehen kann zurückgreifen kann.

Kundenbindungssysteme (Kundenkarten & Bonussysteme)

Immer mehr Unternehmen versuchen ihre Kunden zum Einsatz von Kundenkarten zu bewegen.[65-69] Dem Kunden werden Vorteile durch den regelmäßigen Einsatz bei jedem Einkauf versprochen, meist in Form eines wie auch immer gearteten Rabattes. Neben dem Ziel der Kundenbindung, also der Entscheidung des Kunden zurückzukehren, weil er dort seine Kundenkarte einsetzen kann, ist das eigentliche Ziel dieser Systeme das Sammeln von Kundendaten um das Konsumverhalten zu messen.

Normalerweise ist der Austausch von Daten zwischen unabhängigen juristischen Personen, auch wenn sie zum selben Konzern gehören, nach den BDSG nicht so ohne Weiteres möglich. Firmenübergreifend einsetzbare Kundenkarten lösen dieses Problem für die Unternehmen recht elegant und preiswert, da der Kunde freiwillig und aktiv seine Einkäufe an eine Stelle meldet. Die Vorteile für den Kunden sind äußerst mäßig und erfordern meist recht hohe Umsätze. Längerfristig besteht hier außerdem noch die Gefahr, daß, wenn erst der überwiegende Teil der Bevölkerung diese Karten einsetzt, die Nichtbenutzer durch höhere Preise abgestraft werden – z.B. Kartennutzer zahlen grundsätzlich 5% weniger. Das es bei den Kundenbindungsystemen um das Sammeln personenbezogener Daten geht, zeigt allein schon die Tatsache, daß der anonyme Einsatz der Karten praktisch unmöglich gemacht wird. Wozu müssen denn sonst Anträge mit Namen und Adresse ausgefüllt werden? Ginge es nur um die Messung des reinen Konsumverhaltens wäre dies wohl nicht notwendig. Schon seit einigen Jahren wird von mehreren Seiten im In- und Ausland auf das enorme Mißbrauchspotential der Kundenkarten hingewiesen.[70-72] Auch von den Verbraucherzentralen werden regelmäßig mehr als kritische Berichte und Gutachten zu den Kundenbindungssystemen veröffentlicht.[73-77]

Eine weitere Technologie die sich immer weiter verbreiten und auch auf nicht kommerzielle Dienste[3] übergreifen wird, ist die der sogenannten personalisierten Dienste. Was auf den ersten Blick als kundenfreundlich wirkt und zur Kundenbindung beitragen soll, ist aber im Grunde nichts weiter als eine gezielte Überwachung des Kunden. Immer mehr Internetläden blenden bei der Produktsuche oder — jedoch seltener zu diesem recht späten Zeitpunkt — bei der Bestellung einen oft bebilderten Text der Art „Personen die dieses Produkt gekauft haben, haben auch folgende Produkte gekauft“ ein. Der Text mag im Wortlaut variieren, was aber nichts an der Aussage ändert. Besonders beliebt ist diese Form der personalisierten Kaufanregung derzeit bei Internetbuchhändlern. Diese Angaben entstammen aus exakt ausgewerteten Kundenprofilen. Da diese Läden auch meist versuchen jeden Besucher bei Anwahl des Internetangebotes zu identifizieren (Auslesen von Cookies) bzw. den Kunden markieren (Session ID), kann man ebenfalls davon ausgehen, daß nicht nur das konkrete Kaufverhalten, sondern bereits im Vorfeld das Surfverhalten des portzentiellen Käufers beobachtet und ausgewertet wird. Gegen die Ausspähung des Interessenprofiles vor dem Kauf kann man sich zwar wehren, aber dies ist im Grunde zeitaufwändig:

- Angebot ansurfen und umschauen
- Produktseite, -nummer o.ä. merken (nicht den Link, da er die Session ID enthält !).
- Cookies löschen
- Verlauf im Browser löschen
- Modembenutzer können sich neu einwählen um eine andere IP-Adresse zu erhalten.
- Angebot neu über die Startseite anwählen und über die Produktsuche gezielt das Produkt bestellen.

Die Auswertung des Kaufverhaltens hingegen läßt sich nicht verhindern, da die Daten des Kaufes gespeichert bleiben.

Passwörter

Hält man sich an das bisher Gesagte, taucht über kurz oder lang das Problem auf, daß man über eine große Anzahl an Pseudonymen und Passwörtern verfügt. Hinzu kommen noch die diversen Geheimnummern von Bank- und Kreditkarten aus der realen Welt. Gebetsmühlenartig wiederholt bekommt man immer wieder erzählt, daß man seine Paswörter, PINs etc. niemals niederschreiben und nur im Gedächtnis behalten sollte. Das mag sachlich richtig sein, geht aber weit an der Realität vorbei. Viele Menschen haben schon am Geldautomaten mit den (bei

[3] Gemeint sind in diesem Falle Endkunden. Für den Endkunden kostenlose Dienste finanzieren sich meist über Werbung.

uns) vierstelligen PINs Probleme, wie sollen die sich dann an etliche 6-8stellige zufällige Zeichenfolgen und die dazugehörigen Pseudonyme erinnern?

Passwortlisten in passwortgeschützten Text- oder ZIP-Dateien abzulegen wäre wirklich mehr als fahrlässig. Diesen Schutz kann man getrost als wirkungslos bezeichnen. Am sichersten greift man in solchen Fällen auf eine Kombination eines Zusatzprogrammes von PGP, dem PGP-Disk [29], und einem der vielfältigen Passwortmanager zurück. Mit PGP-Disk legt man sich ein sicheres, verschlüsseltes virtuelles Laufwerk an, auf dem dann die Datei des Passwortmanagers gespeichert wird. Diese virtuelle Diskette wird nur dann geöffnet, bevor man sie wirklich braucht.

Besonders praktisch für solche Fälle sind auch die sich derzeit massiv verbreitenden. feuerzeugroßen USB-Speicherstäbchen (ab ca. 30 €). Sie sind mechanisch recht stabil, transportabel, nahezu betriebssystemunabhängig und weisen mit 64 MByte - 1GByte hinreichend große Kapazitäten selbst für anspruchsvollere Dateien auf. Bei Bedarf werden sie einfach in den nächsten freien USB-Platz gesteckt und umgehend stehen die Daten am Rechner zur Verfügung.

Resümee

Seien Sie also mißtrauisch, gehen Sie immer davon aus, das erhobene und gespeicherte Daten — egal ob von staatlichen Behörden oder Privatunternehmen — irgendwann zu ihren Ungunsten mißbraucht werden werden. Es wird sich nie vollständig verhindern lassen — wie auch, sie haben ja keine wirksame Kontroll- und Eingriffsmöglichkeit —, aber Sie können aktiv versuchen das Risiko zu reduzieren und den möglichen Schaden gering zu halten.

Die persönliche Freiheit Dinge zu tun oder zu lassen schließt auch die Verantwortung ein, wo immer es machbar ist, sich um sich selber kümmern und nicht nach staatlichen Regelungen zu rufen, denn niemals wird sich alles regeln lassen, schon gar nicht im Voraus. Außerdem wird im Zweifelsfalle jedwedes bekannte Staatswesen immer mit der Begründung von sogenannten „höheren Interessen“ das Eigeninteresse des Individuums hinten an stellen.

Alle gemachten Vorschläge beruhen auf der einfachen Grundregel, daß Daten, die nicht erhoben worden sind auch nicht geschützt werden müssen. Man sollte also immer das Prinzip der Datensparsamkeit walten lassen. Ansonsten bleibt einem nur der Verzicht und das Füttern der Datenbanken mit möglichst vielen falschen und unterschiedlichen Informationen. Insbesondere auch vor dem Hintergrund des beginnenden Masseneinsatzes von Transpondern (RFID, ***R***adio ***F***requency ***Id***entification) zur Kennzeichnung von Objekten aller Art, die alles in den Schatten stellt was bisher für das Sammeln von Daten benutzt wurde.[78, 79]

Haftungssauschluss

Die im Text genannten Bezeichnungen können marken- oder urheberrechtlich geschützt sein, auch wenn dies im Textfluss nicht explizit vermerkt wurde.

Die angegebenen Verweise sollen dem Leser als Beispiele und zum Einstieg für eine tiefergehende Recherche dienen, sie sind aber nicht als Empfehlungen zu verstehen. Außerdem wird kein Anspruch auf Vollständigkeit erhoben, d.h. eine Nichtnennung ist nicht als Wertung aufzufassen.

Referenzen

1. Wachhunde — 13 Virenscanner für Windows. A. Vahldiek, A. Marx. c’t 2004, Heft 3:122.
2. Test: Sicherheits-Suiten — Glatter Durchschuss. A. Winterer. com! 2004 Heft 3:66.
3. Selbstverteidigung — Die wichtigsten Sicherheitsmaßnahmen für Windows. K. Violka. c’t 2003, Heft 21:100.
4. Bundesdatenschutzgesetz (BDSG) http://Bundesrecht.juris.DE/bundesrecht/bdsg_1990/
5. 99+1 Beispiele und viele Tipps zum Bundesdatenschutzgesetz; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Vzbv Verbraucherzentrale Bundesverband e.V., Verbraucherzentrale Schleswig-Holstein e.V.; 1. Auflage 2003; (kostenlos) http://www.vzbv.de/go/dokumentepositionen/269/1/4/index.html
   Oder als elektronische Variante unter (800 kByte) http://WWW.VZBV.DE/mediapics/bdsg_handbuch.pdf
6. Gute Zahler, schlechte Zahler — Bonitäts-Check im Internet. H. Dambeck. c’t 2002, Heft 13:94.
7. http://WWW.Schufa.DE/
8. http://WWW.DeutschePost.DE/
9. 795. Sitzung des Bundesrates vom 19.12.2003

http://WWW1.Bundesrat.DE/coremedia/generator/Inhalt/DE/1_20Aktuelles/1.4_20Informationsdienst_20Beschl_C3_BCsse/1.4.8_20Beschl_C3_BCsse_20der_20795._20Sitzung/index,templateId=renderUnterseiteKomplett.html

10. Entwurf eines Telekommunikationsgesetzes (TKG) Drucksache 0755_2D03 (25 MByte) http://WWW1.Bundesrat.DE/coremedia/generator/Inhalt/Drucksachen/2003/0755_2D03,property=Dokument.pdf
11. Beschluss der 795. Sitzung des Bundesrates vom 19.12.2003 Drucksache 0755-03B (248 kByte) http://WWW1.Bundesrat.DE/coremedia/generator/Inhalt/Drucksachen/2003/0755_2D03B,property=Dokument.pdf
12. Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz, GWG) http://Bundesrecht.juris.DE/bundesrecht/gwg/
13. Lotsen los! — Data Mining: Verborgene Zusammenhänge in Datenbanken aufspüren. D. Janetzko. c't 1997, Heft 15:294.
14. Arrowsmith http://d-swanson.uchicago.edu/
15. Schufa-Eigenauskunft https://WWW.Schufa.DE/forms/formular-eigenauskunft.html
16. http://Anon.inf.TU-Dresden.DE/
17. http://WWW.Metacrawler.DE/
18. http://WWW.Denic.DE/
19. http://WWW.Denic.DE/de/whois/index.jsp
20. IRC-Research Corporation http://WWW.IRC-Research.com/
21. http://Robinsonlist.DE/
22. http://WWW.Spamflam.DE/
23. http://WWW.Spammer-Hammer.DE/
24. http://WWW.Privacy.net/email/
25. http://WWW.trans-ocean.org/tabelle-freemailer.htm
26. http://WWW.GMX.net/
27. http://Freemail.Web.DE/
28. http://WWW.ePost.DE/
29. http://WWW.PGPi.org/
30. PGP — Pretty Good Privacy. Das Verschlüsselungsprogramm für Ihre private elektronische Post. C. Creutzig, A. Buhl, P. Zimmermann. Verlag ART D'AMEUBLEMENT, Bielefeld. 4. Auflage. ISBN 3-9802182-9-5. http://WWW.FoeBuD.org/texte/publish/pgp.html
31. http://WWW.GnuPG.org/
32. http://WWW.Heise.DE/newsticker/newsticker/meldung/6738
33. http://WWW.Heise.DE/newsticker/meldung/4063
34. http://WWW.Heise.DE/newsticker/meldung/4128
35. http://WWW.Heise.DE/newsticker/meldung/7096
36. http://WWW.computerbytesman.com/privacy/blair.htm
37. http://WWW.casi.org.UK/discuss/2003/msg00457.html
38. http://WWW.RegTP.DE/reg_tele/start/in_05-06-05-00-00_m/index.html
39. Beschluss des Landgerichts Saarbrücken vom 11.11.2003, Aktz.: 7 II O 116/03
40. Wettbewerbszentrale http://WWW.Wettbewerbszentrale.DE/de/news/detail.asp?id=131&bereich=&typ=&kategorie=&suchtext=0700&suchart=and&autor=&nb=1
41. Der Bundespostminister warnt: Telefonieren schadet Ihrem Geldbeutel! W.-D. Roth. 05.02.2004 Telepolis. http://WWW.Heise.DE/tp/deutsch/inhalt/te/16689/1.html
42. http://WWW.Abmahnwelle.DE/
43. http://WWW.Google.DE/
44. http://WWW.Google.com/
45. Bezahlen im Web — aber sicher! K. Kranz, S. Reinke. CHIP Mai 2003:206-211.
46. http://WWW.Firstgate.DE/
47. http://WWW.MicroMoney.DE/
48. http://WWW.NetDebit.DE/
49. http://WWW.Paypal.com/
50. http://WWW.PaySafeCard.DE/
51. http://WWW.SimCash.DE/
52. European Committee for Banking Standards (ECBS) http://WWW.ECBS.org/
53. ECBS: Broschüre, Kurzinformation (128 kByte) http://WWW.ECBS.org/Download/LFL9204V3.pdf
54. Internationale Bankleitzahl (BIC, Bank Identifier Code) http://WWW.Pruefziffernberechnung.DE/B/BIC.shtml
55. Internationale Bankkontonummer IBAN — International Bank Account Number http://WWW.Pruefziffernberechnung.DE/I/IBAN.shtml
56. http://WWW.Azubo.DE/
57. http://WWW.Auctions.DE/
58. http://WWW.Ebay.DE/
59. http://WWW.EchtWahr.DE/
60. http://WWW.Intoko.DE/
61. http://WWW.Undertool.DE/

62. http://WWW.Tipp24.DE/
63. Zuschlag ohne Rückschlag — Betrüger bei eBay erkennen und meiden. A. Kossel. c't 2004, Heft 4:90.
64. Drei, zwei, eins...– Ärger? — Spezielle Rechtsfragen rund um Internet-Auktionen. K. Mielke. c't 2004,Heft 4:96.
65. https://WWW.HappyDigits.DE/
66. http://WWW.MilesMore.DE/
67. http://WWW.Payback.DE/
68. http://WWW.ReweCard.DE/
69. http://WWW.Webmiles.DE/
70. FoeBuD e.V. FAQ zu Kundenkarten http://WWW.FoeBuD.org/texte/aktion/nocards/index.shtml
71. http://WWW.NoCards.org/
72. http://WWW.Pruefziffernberechnung/P/Payback.shtml
73. „Datenschutz ist Verbraucherschutz" — Kundenkarten: Unternehmen erforschen Einkaufsverhalten der Verbraucher. 19.06.2003. http://WWW.VZBV.DE/go/presse/240/5/25/index.html
74. Preisnachlässe und Kundenbindung nach dem Wegfall des Rabattgesetzes. IFAV Institut für angewandte Verbraucherforschung e.V. April 2002 (116 kByte) http://WWW.VZBV.DE/mediapics/1020687606IFAV_Rabatt_Kundenbindung_02-04-23.pdf
75. Kundenkarten: Flächendeckende Verstöße gegen den Datenschutz. Bonuskarten sollen Kundenprofile und Kaufverhalten erforschen. 01.12.2003. http://WWW.VZBV.DE/go/presse/321/5/25/index.html
76. Kundenbindungssysteme und Datenschutz (Kurz-Zusammenfassung des Gutachtens). 12.2003. VZBV (124 kByte) http://WWW.VZBV.DE/mediapics/kundenbindungssysteme_kurzfassung_2003.pdf
77. Gutachten zu kundenbindungssystemen und Datenschutz. 02.12.2003-vzbv. udl (536 kByte, 408 kByte) http://WWW.VZBV.DE/go/dokumentepositionen/244/1/4/index.html http://WWW.VZBV.DE/mediapics/gutachten_kundenbindungssysteme_2003.pdf http://WWW.VZBV.DE/mediapics/kundenbindungssysteme_anlagen_2003.pdf
78. WWW.AutoIDcenter.org/
79. Etikettierungen — Vom Barcode zum Smart-Label. E. Adolf. c't, 2002, Heft 9, S. 8.