

Verbraucherschutz im Internet -

Wie viel Vertrauen ist gerechtfertigt?

Dossier zum Weltverbrauchertag 2005

Verbraucherschutz im Internet - Wie viel Vertrauen ist gerechtfertigt?
Dossier zum Weltverbrauchertag 2005
Autorin: Nicola D. Schmidt
Redaktion: Carel Mohn
Herausgeber: Verbraucherzentrale Bundesverband - vzbv Berlin 2005

EINFÜHRUNG

Um sich wirksam gegen die Risiken des elektronischen Einkaufens zu schützen, müsste der Verbraucher sich ein Wissen über das Internet aneignen, als würde er sein Auto komplett selbst reparieren wollen.

Vertrauenskrise im E-Commerce: Ursachen, Folgen, Gegenstrategien

E-Commerce hat ein großes Potential: 34,4 Millionen Deutsche hatten im März 2004 Zugang zum Internet, davon 80 Prozent von zu Hause aus. Fast jeder informiert sich online, bevor er Flugtickets, Hotelbuchungen, Reisen, Aktien oder Digitalkameras kauft. Und 23 Millionen Deutsche kaufen auch bereits am PC ein: Bücher stehen immer noch ganz vorne auf der Liste, aber dicht dahinter folgen Eintrittskarten, Musik, Software und Unterhaltungselektronik.

Dennoch spricht die Branche von einer Vertrauenskrise: Schlechte Nachrichten über Betrugereien bei E-Bay und beim Online-Banking sowie medienwirksame Viren-Ausbrüche und die beständig wachsende Zahl unerwünschter Werbemails in den Postfächern schaden dem Ruf des elektronischen Handels. Verbraucher machen sich Sorgen um die Sicherheit ihrer Daten, viele stehen dem Internet misstrauisch gegenüber, weil sie die tatsächlichen Gefahren nur schwer abschätzen können. Diese Vertrauenskrise hemmt die weitere wirtschaftliche Entwicklung einer Zukunftsbranche.

Eine der Ursachen: Sowohl die rechtlichen als auch die technischen Hintergründe von Internet und E-Commerce sind so komplex, dass der Bürger sie kaum überblicken kann. Online-Banking, Urheberrechtsgesetze, Datenschutzregeln, Viren und Firewalls - all dies müsste der Konsument verstehen und beherrschen, um sich sorglos online bewegen zu können. Hinzu kommt: Die Wirtschaft überlässt es meist dem Verbraucher, sich gegen Gefahren zu schützen. Doch die Online-Händler tragen auch aktiv zur Vertrauenskrise bei. Händler missachten geltendes Recht, wo es die Verbraucher bereits schützt, und nutzen rechtliche Schlupflöcher, um ihre Interessen durchzusetzen.

Der Weg aus der Vertrauenskrise führt zum einen über die Aufklärung von Konsumenten und Anbietern. Beide müssen über Rechte und Pflichten informiert werden. Darüber hinaus muss die Qualität der angebotenen Informationen im Internet besser werden – von der Information, wer eigentlich hinter einer Website oder einem E-Shop steht bis zu leicht auffindbaren Allgemeinen Geschäftsbedingungen. Außerdem ist der Gesetzgeber gefordert, den Verbraucher stärker zu schützen und rechtliche Lücken zu schließen – wenn eine Bank ein unsicheres Online-System anbietet, darf die Haftung nicht allein beim Kunden liegen. Noch wichtiger jedoch ist die Rechtsdurchsetzung, denn die besten Gesetze bleiben wirkungslos, wenn sie nicht befolgt werden. Gesetze zum Kundenschutz im Internet können verbraucherorientierte Unternehmen sogar schädigen – wenn deren Missachtung durch die Konkurrenz nämlich folgenlos bleibt oder durch steigende Umsätze „belohnt“ wird.

In diesem Dossier werden die Gefahren beschrieben, die den Verbraucher im Internet erwarten und ihre Hintergründe erklärt. Mithilfe von Studien wird erläutert, welche Effekte die bisherige Gesetzgebung hat, in welchen Bereichen Regelungen fehlen und welche Gegenstrategien notwendig sein werden. Das Dossier belegt auch, dass Verbraucherschutz und die Investition in eine der Wachstumsbranchen der Zukunft kein Gegensatz sind. Denn eines

zeigen die Untersuchungen: Die Konsumenten wollen in Zukunft mehr im Internet einkaufen, vor allem hochwertigere Güter. Eine stärkere Verbraucherorientierung wird deshalb einer der Schlüssel zu diesen Märkten.

GLIEDERUNG

1. Stand der Dinge

- E-Commerce in Deutschland: Ein Überblick
- Gesetzgeber versucht Abhilfe
- Gesetzestreue: Mangelhaft
- Verbraucher suchen Sicherheit
- Schutz nur für Experten

2. Marktentwicklung

- Vertrauensdefizit führt zu Seitwärtsentwicklung
- Kundenstruktur: „Gut und treu“
- Verbraucher: Wunsch nach Sicherheit steht vorn
- An der E-Kasse: Unsicherheit und Ungeduld
- Händler planen am Verbraucher vorbei

3. Der alleingelassene Verbraucher

3.1 E-Commerce

- Denn sie wissen nicht, bei wem sie kaufen
- Am Anfang war das: Wer steht hinter der Website?
- Sitzplatz- Ja. Lieferung – vielleicht: Kundenservice bei E-Shops
- Informationen im Netz: Problemfall Finanzprodukte
- Europaweit: 100 Einkäufe - 57 korrekt geliefert
- „Geht nicht? Passt nicht? Ihr Pech.“
- Der Grundsatz „Erst Ware, dann Geld“ gilt nicht mehr
- „Zahlen bitte ...“ – Bezahlssysteme als Schwachstelle des E-Commerce
- SET-System: Geschädigte Verbraucher in der Beweispflicht

3.2 Online-Banking

- Online-Konten aus Bankenperspektive: Kostenverlagerung nach außen
- Angriffe auf Verbraucher nehmen zu
- Gefahr durch „Phishing“: „Dürfen wir Ihre Daten haben?“
- Sicheres Online-Banking nur für Belgier und Niederländer?

3.3 Urheberrechte und Digital Rights Management

- Fehlendes Unrechtsbewusstsein bei Software
- Die Urheberrechtsnovelle zur Privatkopie
- Bildung und Forschung blockiert
- Gefahr: Gläserne Nutzer

3.4 Datenschutz: Breite Datenspuren im Internet

- Langlebige, schwatzhafte Kekse
- E-Commerce als Datenfalle
- EU und USA: Unterschiedliche Regeln zu Werbemüll
- Daten verschwinden im Dschungel

3.5 Spam: Die wachsende Gefahr

- Provider ignorieren Beschwerden
- Spam schadet E-Commerce
- Spam verunsichert - und verführt

3.6 Malware: Viren, Trojaner und Co.

- Ungebetene Gäste
- Das Problem: Fehler in Programmen
- Viren als Einfallstor

3.7 Sicherheitstechniken

- Überforderung - nicht nur zu Hause
- Durchschnittsnutzer hilflos

3.8 Sichere Identifikation in offenen Netzen

- Signieren per Computer
- Zu teuer, zu kompliziert – und nun zu unsicher?
- Starke Beweiskraft eines schwachen Systems

3.9 Folgen

- Der Wirtschaftsfaktor Vertrauen gerät unter Druck
- Wirtschaftliche Folgen

4. Ausblick

VERWENDETE LITERATUR

1. Stand der Dinge

E-Commerce in Deutschland: Ein Überblick

„Einkaufen mit Sitzplatzgarantie!“ versprach im Winter 2003/04 ein Werbeslogan des Online-Buchhändlers Amazon.com: E-Commerce wird vermarktet als ungetrübtes Einkaufsvergnügen rund um die Uhr, weltweit, vom heimischen Computer aus. Die Deutschen begaben sich in den letzten Jahren vorsichtig und doch stetig auf die Entdeckungsreise des Online-Shoppings. Doch die Realität sieht oft anders aus als die Werbung glauben machen will. Nationale und internationale Studien kommen übereinstimmend zu dem Ergebnis: Zuviel Vertrauen ist im Internet eher schädlich.

Die Weltverbraucherorganisation Consumers International stellte in ihrer vergleichenden Studie „Should I buy?“ 2001 fest, dass der grenzenlose Einkauf im Internet für den Verbraucher langwierig und frustrierend sein kann (siehe Kasten). Das Europäische Verbraucherzentrum (EVZ) stellte zwei Jahre später 2003 in einer Studie die Frage „Europa - grenzenloses Einkaufsparadies?“ und kam nach 114 Einkäufen zu dem Schluss, dass „die Bedingungen, unter denen grenzüberschreitender E-Commerce stattfindet, für Verbraucher weiterhin ungünstig sind“. Das sieht in Deutschland selbst nicht anders aus: „Kundenservice noch optimierungsfähig“ resümiert für innerdeutsche Einkäufe kurz und knapp die Studie „E-Commerce 2004“ (EVZ 2003, S. 7, Postbank/Europapressedienst 2004, S. 5). Online-Shopping ist zwar in der Tat von zu Hause aus und rund um die Uhr verfügbar, es erfüllt aber oft nicht die Ansprüche, die die Verbraucherzentralen an einen Vertragsabschluss stellen: Es gibt Sicherheitsmängel, die Informationspolitik ist schlecht, Verbraucherrechte werden ignoriert, ausgehebelt oder trickreich umgangen.

Gesetzgeber versucht Abhilfe

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versucht bereits 1999 in der Schrift „Sicherheitsaspekte beim Electronic Commerce“ ein grundsätzliches Missverständnis auszuräumen: „Der Elektronische Handel soll über das Internet stattfinden, ein öffentliches Netz, das nicht zur Übertragung sicherheitskritischer Informationen entwickelt worden ist.“ (BSI 1999, S. 16). Der Gesetzgeber versucht seit langem, diesen Sicherheitslücken mit Gesetzesvorhaben wie dem Teledienste-Gesetz (TDG) und den Bemühungen um die elektronische Signatur sowie der Anpassung der Formvorschriften des Privatrechtes an den modernen Rechtsgeschäfteverkehr beizukommen.

Im Bereich der Finanzdienstleistungen wurde diesem Zustand im Dezember 2004 Abhilfe geleistet. Mit den im Rahmen der Umsetzung einer EU-Richtlinie neu eingeführten Vorschriften über den Fernabsatz von Finanzdienstleistungen werden den Unternehmen Mindeststandards für die Information von Verbrauchern auferlegt, die auch für den Vertrieb von Finanzprodukten im Internet gelten. Trotz dieser rechtlichen Verbesserungen zum Schutz der Verbraucher betrachten viele das Internet offensichtlich noch immer als rechtsfreien Raum.

Gesetzestreue: Mangelhaft

Der Verbraucherzentrale Bundesverband meldet 2002, dass sich sieben von zehn getesteten Einkaufsportalen nicht an das TDG und andere Rechtsvorschriften für den E-Commerce halten. Häufigste Verstöße: Keine genaue Anschrift des Unternehmens online, keine Informationen über Widerrufs- oder Rückgaberechte, keine Angabe über Vertretungsberechtigte. Die Kunden werden auch größtenteils nicht darüber informiert, ob ihre Bestellung gespeichert wurde, wie sie den Fortgang überprüfen und eventuelle Eingabefehler korrigieren können. Europaweit kann Consumers International diesen Zustand nur bestätigen - Websites geben keine vollständigen Kontaktdaten an, Kunden haben kaum eine Chance, ihren Wahrheitsgehalt zu überprüfen. Auch die Lieferung ist mangelhaft: Von den 114 grenzüberschreitenden Bestellungen des EVZ wurden lediglich 57 Prozent korrekt bestätigt, in Rechnung gestellt und tatsächlich ausgeliefert. Bei acht Prozent der Einkäufe verschwand die Bestellung im Datennirwana. Ebenfalls acht Prozent der Aufträge wurden bestätigt, in Rechnung gestellt, aber nie geliefert (EVZ 2003, S. 12).

Verbraucher suchen Sicherheit

Nicht nur in der öffentlichen Debatte, auch unter Verbrauchern ist die Frage nach Sicherheit ein wichtiges Thema. Der Verbraucher muss darauf vertrauen können, dass er richtige Informationen über Produkte erhält, seine Daten geschützt werden und die Ware geliefert wird. Er kann jedoch nicht wie im Ladengeschäft das Produkt und das Verhalten des Geschäftspartners in Augenschein nehmen. Daher versuchen Verbraucher im Internet mit Hilfe der Einschätzungen und Erfahrungen anderer, sich notdürftige Sicherheit zu verschaffen: Projekte wie das Verbraucherportal Dooyoo.de oder die Bewertungslisten bei E-Bay.com und Amazon.com sind solche Versuche. Doch auch hier gibt es immer wieder Betrugsfälle, beispielsweise Händlerringe, die sich gegenseitig gute Bewertungen schreiben (vgl. www.internetfallen.de/).

Schutz nur für Experten

Die Kunden quittieren diese und andere Unsicherheiten mit Rückzug: Um sich wirksam gegen die Risiken des elektronischen Einkaufens zu schützen, müsste der Verbraucher sich ein Wissen über das Internet aneignen, als würde er sein Auto komplett selbst reparieren wollen. Nur wenige „Nerds“, also Internet-Freaks, haben Zeit und Energie dafür. Alle anderen sind darauf angewiesen, dass der Gesetzgeber ihre Rechte schützt und den Unternehmen Anreize zu verbraucherfreundlichem Verhalten gibt. Denn sicher ist: Auf Dauer wird sich der Einkauf über das Internet nur durchsetzen, wenn den Verbrauchern ein Rahmen geboten wird, in dem sie ihrem Gegenüber vertrauen können.

Fallbeispiele:

Ein Amerikaner bucht über die Website www.budgethotels.com ein Zimmer, will es aber dann wieder stornieren. Auf der Website ist eine gebührenfreie Rufnummer für Änderungen und Stornierungen angegeben. Drei Mal an zwei verschiedenen Tagen versucht der Kunde, jemanden unter dieser Nummer zu erreichen, aber er landet stets in einer Warteschleife und irgendwann wird die Leitung unterbrochen. Der Kunde ruft die Buchungshotline an und bekommt dort eine andere Telefonnummer genannt. Hier wird zunächst wieder die Leitung getrennt, aber dann gibt es plötzlich eine Bandansage, dass Stornierungen online auf einer anderen Website zu tätigen seien. Auf dieser Website lässt sich die Buchung schließlich wirklich stornieren.

Ein anderer Kunde bestellt ein Buch auf der britischen Seite www.heffers.com am 7. Dezember 2000. Am nächsten Tag erhält er eine E-Mail, die seine Bestellung bestätigt. Die Lieferzeit betrage drei bis fünf Wochen in die USA. Am gleichen Tag erhält der Kunde eine weitere E-Mail, dass das Buch gerade nicht vorrätig sei und die Lieferzeit zwischen drei und sechs Wochen betragen könne. Die Mail enthält keinerlei Möglichkeit, die Bestellung zu stornieren. Ende Januar 2000, acht Wochen später, ist das Buch noch immer nicht geliefert. Der Kunde schickt eine Mail, um nach seiner Bestellung zu fragen, erhält aber keine Antwort. Er sendet zwei weitere E-Mails. Endlich erhält er eine Antwort, das Buch sei derzeit nicht lieferbar und werde wieder Ende Februar oder Anfang März verfügbar sein. Am 2. März registriert der Kunde eine Abbuchung von seiner Kreditkarte - der Preis des Buches hat sich offensichtlich erhöht, vom Buch selbst immer noch keine Spur. Es taucht schlussendlich am 14. April im Briefkasten auf - vier Monate nach der Bestellung. (Quelle: ConsInt 2001a, S.12 ff)

2. Marktentwicklung

Vertrauensdefizit führt zu Seitwärtsentwicklung

Im April 2003 meldet die Gesellschaft für Konsumforschung (GFK), die Zahl der Online-Käufer habe die 20 Millionen-Grenze erreicht. Damit hat jeder dritte Erwachsene in Deutschland schon einmal etwas im Internet eingekauft. Der Markt entwickelt sich zwar langsam, aber stetig. Vor allem Gutverdienende kaufen gerne bei Online-Shops ein. Diese positiven Trends dürfen über eines allerdings nicht hinwegtäuschen: Der Markt entwickelt sich eher seitwärts und schöpft sein großes Potential nur ungenügend aus.

Im Jahr 2004 zeigte das GFK *Online-Shopping-Survey*, dass sich die Deutschen auch von der schlechten Wirtschaftslage nicht vom Online-Shopping abhalten ließen: Mehr als ein Drittel der Bevölkerung über 14 Jahren, nämlich 23 Millionen, kauften online ein. Die Deutschen interessierten sich vor allem für Bücher, Kleider und CDs, zunehmend aber auch für Digitalkameras, Unterhaltungselektronik und Autozubehör, also hochpreisige Produkte. Im ersten Halbjahr 2004 kauften sie für 5,3 Milliarden Euro Waren über das Internet. Für das Gesamtjahr schätzt die GFK einen Umsatz von über 11 Milliarden Euro. Offensichtlich wechseln die Kunden vom traditionellen Versandhandel aber auch vom stationären Einzelhandel ins Internet.

Kundenstruktur: „Gut und treu“

Interessant für die Online-Händler: Im Internet sind nicht nur Schnäppchenjäger unterwegs. Es sind viele Gutverdienende ab 30 Jahren, die gerne im Internet einkaufen, findet die Studie von Postbank/Europapressedienst heraus. Für sie spielen Zeitersparnis und Unabhängigkeit von Öffnungszeiten die größte Rolle, günstigere Preise stehen erst an zweiter Stelle. Wenn die Händler diese Kunden ausreichend binden, können sie viel Kaufkraft ins Netz holen. Verbraucher sind in diesem Falle „Wiederholungstäter“: Gut die Hälfte aller Befragten der Postbank-Studie hatte in den letzten drei Monaten fünfmal oder häufiger im Internet eingekauft, die übrigen Gelegenheitsshopper zwischen ein- und fünfmal. Die meisten kaufen im Inland (81,5 Prozent), etwa jeder fünfte besucht zusätzlich auch Shops aus anderen Ländern (22,3 Prozent)¹. Zwar erfreuen sich auch Online-Auktionen großer Beliebtheit, 72,7 Prozent hatten dort schon Waren erstanden. Doch je höher der Verdienst, desto eher wenden sich die Kunden direkt an Shops. 86,4 Prozent der Befragten mit einem Nettoeinkommen von über 3000 Euro haben keine Zeit für E-Bay, sie kaufen ihre Waren online und direkt ein. Damit eröffnet sich hier für Händler ein kaufkräftiger Markt mit treuen Kunden - wenn die Voraussetzungen stimmen.

¹ Bei der Frage „Wo haben Sie in den letzten drei Monaten im Internet eingekauft?“ waren Mehrfachnennungen möglich zwischen den Antworten „Deutsche Online-Shops“, „Ausländische Online Shops“ und „Online-Auktionen“.

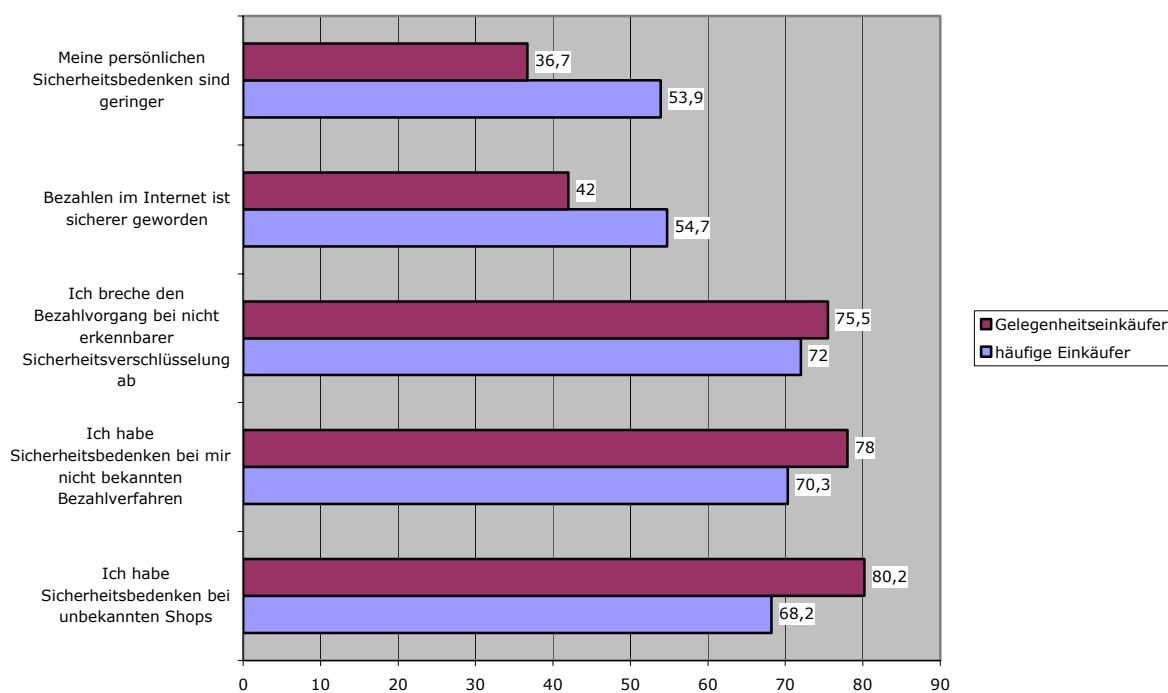
Verbraucher: Wunsch nach mehr Sicherheit steht vorn

Den Verbrauchern ist längst bewusst, welche Probleme beim Online-Shopping auftreten und welchen Gefahren sie sich aussetzen - sie wünschen sich vor allem mehr Sicherheit, Shops, denen sie vertrauen können und Bezahlfverfahren, die sie nachvollziehen können.

Die Postbank/Europressedienst 2004 hat Online-Kunden zu Sorgen und Wünschen beim Online-Shopping befragt. Den meisten Einkäufern ist demnach besonders wichtig, dass sie ihre Waren schnell bekommen (60,4 Prozent), gleich danach rangiert die Suche nach dem günstigsten Preis (55,7 Prozent). Zudem wollen Verbraucher gerne in bekannten Shops einkaufen und nur sieben Prozent der Käufer probieren auch gerne neue Online-Shops aus. Hier spielt das Vertrauen in große Marken und bekannte Händler eine große Rolle. Wer einen guten Service bietet, kann mit treuer Stammkundschaft rechnen.

Die Deutschen, die nicht online einkaufen, tun dies, weil ihnen im Internet das Einkaufserlebnis fehlt (40,5 Prozent) und vor allem, weil sie Sicherheitsbedenken haben (39,7 Prozent). Der Aussage „Meine persönlichen Sicherheitsbedenken sind geringer geworden“ stimmen nur 10,3 Prozent der Befragten voll zu. Wenn keine Sicherheitsverschlüsselung erkennbar ist, also zum Beispiel Kreditkartendaten unverschlüsselt oder für den Nutzer nicht erkennbar geschützt über das Internet übertragen werden, brechen sogar bei den häufigen Käufern 72 Prozent das Bezahlfverfahren ab, bei den gelegentlichen Käufern sind es 75,5 Prozent. Insgesamt ist zu bemerken, dass bei häufigeren Einkäufen auch das Vertrauen in den E-Commerce leicht ansteigt, dennoch stimmen jeweils über die Hälfte der Befragten zu, wenn man sie zu unterschiedlichen Sicherheitsaspekten befragt.

Einkaufshäufigkeit vs. Sicherheitsbedenken beim Online-Kauf



Quelle: Postbank/Europressedienst 2004, Angaben in Prozent der Befragten, Mehrfachnennungen möglich

An der E-Kasse: Unsicherheit und Ungeduld

Die Frage, wie man im Internet seine Ware bezahlt, ist aus Verbrauchersicht die Schlüsselfrage bei der Entscheidung für oder gegen E-Commerce. Mehr als jeder dritte Käufer wünscht sich, besser, sicherer oder komfortabler im Internet bezahlen zu können. Dies spiegelt sich auch in den hohen Sicherheitsbedenken der Konsumenten wieder: 80,2 Prozent derer, die ein bis vier Mal in den letzten Monaten im Internet gekauft haben, plagen sich mit Sicherheitsbedenken bei fremden Shops. Selbst wer häufiger einkauft, macht sich Gedanken bei unbekanntem Zahlverfahren (Postbank/Europressedienst 2004, S.33ff).

Nach einer Studie im Auftrag der Europäischen Kommission hat die Öffentlichkeit in den meisten Mitgliedsstaaten ein „annehmbares Maß“ an Vertrauen in den elektronischen Zahlungsverkehr. Der in der Untersuchung errechnete „Vertrauensindikator“¹ kommt für Deutschland zu wenig schmeichelhaften Ergebnissen. Deutschland liegt dort nur an vorletzter Stelle mit 7,34 Punkten hinter den Anführern Finnland (8,41), Niederlande (7,91) und Schweden (7,79). Nur auf 26 Prozent der von den Forschern im Rahmen der Studie ausgewerteten Websites waren Sicherheitsinformationen ohne weiteres zu finden. Die im Rahmen der Studie befragten Verbraucherorganisationen kamen zu dem Schluss, dass „den Verbrauchern zahlreiche Aspekte des elektronischen Zahlungsverkehrs nach wie vor unklar“ seien. Besonders Haftungsfragen sowie Rolle und Verantwortung beider Parteien bleiben ungeklärt (EU Kommission 2003).

Ein weiteres Problem besteht in der Diskrepanz zwischen dem, worauf Händler Wert legen und den Kundenwünschen. Händler schätzen an einem Bezahlssystem vor allem Bequemlichkeit und niedrigen Zahlungsausfall. Kunden haben Sicherheitsbedenken bei Techniken, die sie nicht kennen. Zudem sind sie ungeduldig: Vor allem erfahrene Shopper brechen den Bezahlvorgang ab, wenn er zu lange dauert. Eine Lösung könnte hier die Online-Überweisung sein, allerdings versuchen viele Händler, über Kreditkartendaten de facto Vorkasse durchzusetzen, für die sie bei Zahlung per Überweisung die Einwilligung des Kunden brauchen.

Händler planen am Verbraucher vorbei

Online-Händler wollen in naher Zukunft in erster Linie ihre Produktpaletten und Shopsysteme ausbauen. Sie glauben, ihre Kunden gut zu kennen – die tatsächlichen Wünsche und Bedürfnisse ihrer Kunden ignorieren sie allerdings.

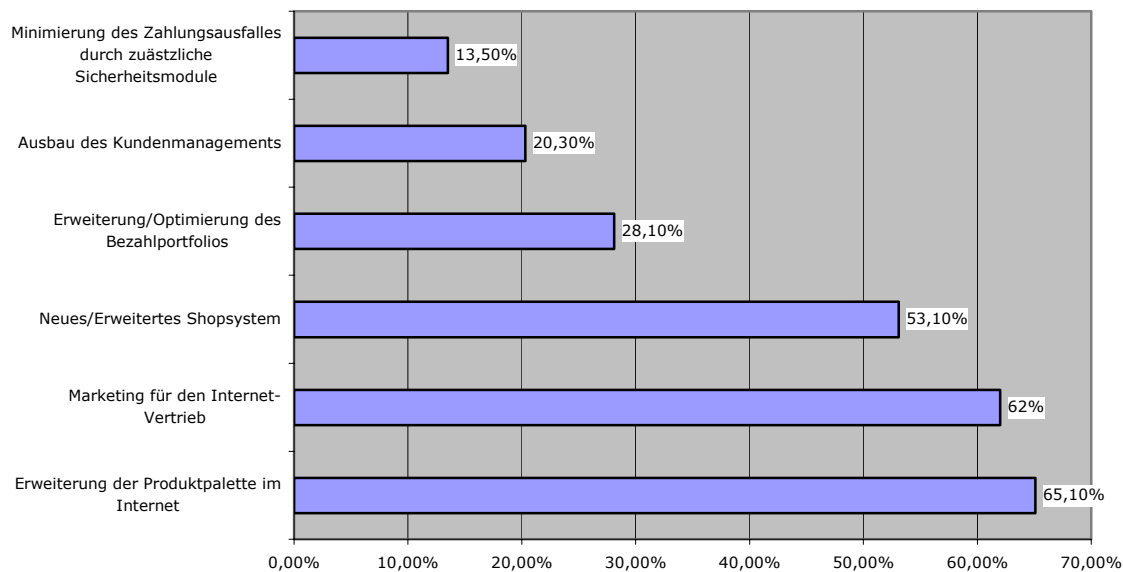
Mehr als die Hälfte der bei Postbank/Europressedienst 2004 befragten Händler erwartet, dass der Online-Anteil am Gesamtumsatz leicht bis stark steigen wird. Besonders optimistisch ist die Gesundheits- und Wellnessbranche, hier rechnen 64,8 Prozent mit steigenden Online-Umsätzen. Die GfK bestätigt diese Hoffnung in ihrem Shopping Survey 2004: 1,8 Millionen Internet-Nutzer haben 2003 ihre Körperpflege- und Kosmetikprodukte im Internet gekauft, 4,9 Millionen können sich dies in Zukunft vorstellen. Noch stärker wird der Handel mit TV-, Video- und HiFi-Geräten wachsen. Während 2003 2,9 Millionen Internetnutzer ihre Unterhaltungselektronik online kauften, können sich dies 6,2 Millionen Deutsche künftig vorstellen (GfK 2004). Der Markt könnte also stark wachsen, wenn es nach den Verbrauchern

¹ Der Indikator errechnet sich aus drei Komponenten: Medienquellen, öffentliche Quellen wie Forschungsergebnisse und Studien sowie direkte Quellen wie der Befragung von 2400 EU-Bürgern und Analyse von 600 Websites. Jeder dieser Bereiche bekam eine Punktwertung von 1 (sehr geringes Vertrauen) bis 10 (sehr hohes Vertrauen). Der Vertrauensindikator errechnet sich aus der gewichteten Kombination der drei Bereiche (vgl. EU Kommission 2003 S. 17ff.)

geht - allerdings müssen die Voraussetzungen stimmen (Postbank/Europressedienst 2004, S. 54).

Konkret muss also das Einkaufserlebnis im Internet stärker auf die Kunden abgestellt werden. Hier klaffen Angebot und Nachfrage noch weit auseinander. Fragt man die Händler, welche Investitionen sie für ihr Online-Geschäft in Zukunft tätigen wollen, erhält man folgende Antworten:

in welche Aktivitäten werden Sie investieren? (Mehrfachnennungen)



Quelle: Postbank/Europressedienst 2004, Angaben in Prozent der Befragten, Mehrfachnennungen möglich

Stärkere Sicherheitsmechanismen stehen an letzter Stelle der Prioritätenliste und das trotz der Sorgen der meisten Kunden. Die Händler wollen lieber ihre Shopsysteme optimieren: Für 63 Prozent der großen Händler mit über 2,5 Millionen Euro Jahresumsatz steht ein neues Shopsystem ganz oben auf der Prioritätenliste, bei kleineren Händlern sind es ebenfalls etwas mehr als die Hälfte. Im Schnitt will jeder Dritte in ein Kunden-Management-System investieren. Außerdem wichtig: Den Kunden „mehr Produkte anzubieten“ und diese „besser zu bewerben“ (ebd., S. 57). Bei der Wahl ihrer Bezahlverfahren ist den Händlern ein „niedriger Zahlungsausfall“ (56 Prozent) sowie eine „bequeme Handhabung“ (43,2 Prozent) am wichtigsten. Kundenfreundlichkeit rangiert erst an dritter Stelle mit 40,2 Prozent. Damit gehen die Planungen an den derzeitigen Kundenwünschen vorbei, die sich mehr Sicherheit, bessere Bezahlssysteme und zuverlässige Abwicklung wünschen.

Etwa die Hälfte der Händler ist sich dennoch sicher, die eigenen Kunden gut zu kennen. Fast drei Viertel (73,5 Prozent) glauben, bereits Stammkundschaft zu haben. Haben die Kunden Sicherheitsbedenken beim Einkauf? Nur 8,3 Prozent der Händler sind davon fest überzeugt, nicht einmal jeder Dritte hält es für zutreffend und 43,2 Prozent halten es für unwahrscheinlich oder falsch. (ebd., S. 63, 68). **Die GFK-Untersuchung zeigt: Viele Händler planen an den Wünschen und Bedürfnissen ihrer Kunden vorbei. Eine Optimierung in Richtung Verbraucherschutz ist von ihnen daher kaum zu erwarten.**

3. Der alleingelassene Verbraucher

Verbraucher sind den Risiken im Internet meistens völlig unzureichend ausgesetzt. Der Informationsdschungel ist für den normalen Nutzer kaum zu überblicken, die technischen Hintergründe sind ebenso wie die rechtlichen meistens ein Fall für Experten. Zudem halten sich viele Online-Händler weder an ihre Informations- noch sonstigen Pflichten, so dass der Konsument oft nur die Probe aufs Exempel machen kann.

3.1 E-Commerce: Denn sie wissen nicht, bei wem sie kaufen

Information ist immer noch das erste Gut der Online-Welt: Der Einkauf im Internet beginnt für die meisten Verbraucher damit, sich auf der Website eines Anbieters über die gesuchten Produkte zu informieren, Preisvergleichsseiten oder eine Suchmaschine zu benutzen (vgl. Postbank/Europressedienst 2004, S. 19). Wenn Verbraucher die Vorteile des 7x24 Stunden verfügbaren, weltweiten Internets nutzen wollen, um Informationen zu finden, Preise zu vergleichen und Kaufberatung zu finden, dann müssen sie in der Lage sein zu unterscheiden, welchen Informationen sie vertrauen können. In der Offline-Welt sind Verbraucher gewohnt, die ihnen gebotenen Informationen zu bewerten: Ein Lexikon hat einen anderen Stellenwert als ein Zeitschriftenartikel, der Rat eines Verkäufers im Laden wird anders bewertet als eine Kaufempfehlung der Stiftung Warentest.

Im Internet fehlen diese Bezüge, dort gibt es nur Websites - mit oft mangelnder Information, unklaren Besitz- und Interessensstrukturen. Der Weltverbraucherverband Consumers International hat in der Studie „Credibility on the web“ im November 2002 europaweit Informationsportale und Beratungsseiten für die Themen Finanzen, Gesundheit und Kaufberatung daraufhin getestet, wie gut der Verbraucher die Informationen findet, die er für eine Bewertung der Website braucht. Das Ergebnis: Die meisten Informationswebsites im Internet bieten alles andere als neutrale und unvoreingenommene Information, versuchen dies jedoch zu verschleiern. Die Sites präsentieren nur einen Aspekt eines Themas oder haben feste kommerzielle Bande zu einem bestimmten Hersteller. Die Informationen sind oft falsch, veraltet oder sogar absichtlich irreführend. Im einfachsten Fall verlieren ratsuchende Verbraucher auf diesen Sites „nur“ Zeit und Geld, bei Gesundheitsfragen können die Folgen jedoch fatal sein.

Am Anfang war das: Wer steht hinter der Website?

Der Anfang aller Information ist die Antwort auf die Frage: Wem gehört die Website? Die wenigsten Verbraucher sind in der Lage, eine DENIC-Abfrage zu starten und festzustellen, auf wen die Domain registriert ist (<http://www.denic.de/de/whois/index.jsp>). Daher sind sie auf Kontakt-Informationen auf den Sites angewiesen.

Die Credibility-Studie von Consumers International hat 460 Ratgeber-Seiten aus den Bereichen Gesundheits-, Finanz- und Preisvergleich in 13 Ländern getestet. Die Tester fanden auf 65 Prozent der Websites eine geographische Adresse, auf 66 Prozent eine Telefonnummer und auf weniger als der Hälfte einen Kundenkontakt (48 Prozent). Ein Drittel aller Seiten hatte überhaupt keine Kontaktadresse. Consumers International wollte auch wissen, ob den Verbrauchern Informationen darüber gegeben wurden, inwiefern Autoren der Seiten Experten auf ihrem Gebiet sind. Besonders bei Gesundheitsinformationen ist es wichtig zu wissen, ob die Personen, die hinter den Informationen stehen, eine ärztliche Ausbildung haben. Auch bei Finanzinformationen kann es wichtig sein zu wissen, wer Anlagetipps gibt. Dennoch

gaben nur knapp zwei Drittel der Gesundheitsseiten und ein Viertel der Finanzseiten an, warum ihre Experten Autorität auf dem besagten Gebiet haben.

Noch viel wichtiger für den Verbraucher ist die Information, ob eine Seite von Sponsoren abhängig ist, von einer bestimmten Firma betrieben wird oder einem Interessenverband nahesteht. Hier waren die Werte erwartungsgemäß sehr gering: Nur sieben Prozent der Seiten präsentierten eine Erklärung, dass sie keine kommerziellen Interessen verfolgten, ebenfalls sieben Prozent ließen den Besucher wissen, dass es auch keinerlei kommerzielle Einflussnahme auf den Inhalt gebe. Der weitaus größere Teil der Websites (60 Prozent) ließ den Nutzer im Unklaren darüber, ob er unparteiische Informationen erhält oder nicht.

Angaben über kommerzielle Interessen bei Ratgeber-Sites

Thema	Gesundheit	Finanzen	Preisvergleich	Alle
Interessen	10	5	5	7
Kommerzielle Interessen haben keinen Einfluss	7	7	6	7
Kommerzielle Interessen haben gewissen Einfluss	6	8	11	8
Generelles Statement zur Unabhängigkeit	1	21	5	9,5
Keine Angaben zu kommerziellen Interessen	65	47	66,5	60

Quelle: *Consumer International, Credibility On The Web 2002, Angaben in Prozent*

Auch der Einfluss von Werbekunden wird dem Nutzer nur selten aufgedeckt. Mehr als die Hälfte aller Websites enthielt Werbung verschiedener Art, besonders Preissuchmaschinen und Gesundheitsseiten (65 und 60 Prozent). Aber nicht einmal jede dritte Site enthielt eine Erklärung, ob die Werbetreibenden Einfluss auf den Inhalt der Seiten haben oder nicht. Noch am ehesten ein Gespür für diese Problematik haben offensichtlich Gesundheitsseiten, sie lagen mit 37 Prozent vorne, gefolgt von 20 Prozent der Preisvergleichsseiten und 13 Prozent der Finanzseiten.

www.netdokter.de

Eine Stichprobe in Deutschland: Eine der bekanntesten deutschen Gesundheitswebsites ist www.netdokter.de. Auf der Seite finden sich ordnungsgemäß eine Geschäftsführerin und eine deutsche Kontaktadresse in München sowie ein Impressum. Ein Link führt auf www.netdokter.com, was auf eine amerikanische Mutterfirma schließen lassen könnte. Hier sind als Kontakt nur die verschiedenen Länder-Filialen angegeben. Dass die Sites einer dänischen Firma namens NetDoktor A/S mit Sitz in Frederiksberg, gehört, erfährt der Nutzer nur über eine Whois-Abfrage bei der Denic. In einem Disclaimer lehnt Netdokter jede Haftung für die Befolgung seiner Ratschläge ab und mahnt die Besucher, immer einen Arzt aufzusuchen. Dies steht im Gegensatz zu den Informationen hinter dem Link „Werbung&Sponsoring“, die potentiellen Werbekunden verspricht, dass die Bundesbürger wegen der Praxisgebühr in Zukunft stärker zur Selbstmedikation und Beratungssuche im Internet gehen werden. Eine Information für die Nutzer über Werber und Sponsoren gibt es hingegen nicht. Die Redaktionsmitglieder werden namentlich, aber ohne Referenzen genannt, dafür gibt es eine lange Liste von „Ärztlichen Beratern und Experten“, die mit Berufsbezeichnung und teilweise auch derzeitiger Tätigkeit genannt werden.

Sitzplatz – Ja, Lieferung – vielleicht: Kundenservice bei E-Shops

Bei Befragungen und Testeinkäufen wird immer wieder deutlich, dass der Online-Einkauf nicht ganz so sorglos ist, wie Amazon mit seinem „Sitzplatzgarantie“-Werbeslogan verkaufen will. In der Deutschen Studie von Postbank/Europressedienst wurden die Kunden nur am Rande zu ihren Erfahrungen befragt. Dennoch stellte sich heraus, dass

- bei 9,6 Prozent der Befragten das im Inland bestellte Gut nie ankam,
- 2,2 Prozent sahen ihre Konto- oder Kreditkartendaten missbraucht,
- 16,8 Prozent der Befragten geben an, dass sie ihre Ware nicht zurückgeben oder umtauschen konnten. (Postbank/Europressedienst 2004, S. 30).

Etwas detaillierter befassten sich Consumers International und das Europäische Verbraucherzentrum Düsseldorf (EVZ) mit den Gepflogenheiten der Anbieter europaweit.

Consumers International untersuchte die Möglichkeiten des Kunden, sich zu informieren und vom Kauf gegebenenfalls zurückzutreten. Das Ergebnis: Fast alle untersuchten Websites (im EU-Durchschnitt 88 Prozent) zeigen dem Kunden seine gesamte Bestellung noch einmal in der Übersicht, bevor er sie bestätigt. Wenn sich der Kunde in dieser Phase aber anders entscheidet, sollte es eine Möglichkeit geben, den Bestellvorgang abubrechen. Dies war in Deutschland nur bei 64,5 Prozent der Seiten möglich, in Frankreich bei 61,5 Prozent. In den Niederlanden hingegen bieten mehr als 90 Prozent der Websites ihren Kunden an, sich wie im Laden noch einmal anders zu entscheiden bis sie die Ware endgültig gekauft haben und halten einen entsprechenden Link bereit.

Wesentlich schwieriger gelangt der Verbraucher an die Information, was er jetzt eigentlich insgesamt ausgegeben hat und wie es weitergeht: Die kompletten Kosten der Bestellung inklusive Versand wurden am Ende von 6,5 Prozent der deutschen Seiten mitgeteilt, hier lagen Frankreich mit 13 und die Niederlande mit 27 Prozent deutlich höher. Besser sah es mit der Auftragsbestätigung aus, denn die verschickten 93,5 Prozent der deutschen Seiten, allerdings enthielten davon nur 11,5 Prozent auch eine Information über ein Rücktrittsrecht (ConsInt S. 36f).

Informationen im Netz: Problemfall Finanzprodukte

Wie oben beschrieben, ist für den Verbraucher die fehlende Möglichkeit des tatsächlichen Kontaktes mit dem Kaufgegenstand ein wesentliches Hemmnis, Waren über das Internet zu erwerben. Durch den seit Jahrzehnten etablierten Versandhandel haben die Verbraucher im klassischen Fernabsatz jedoch ein erhebliches Erfahrungswissen. Dieses Erfahrungswissen fehlt aber gerade bei Finanzdienstleistungen – bei Produkten also, die man weder „anprobieren“ noch „zurückschicken“ kann. Deshalb spielen Informationen vor Vertragsabschluss bei diesen Dienstleistungen für den Verbraucher eine so zentrale Rolle.

Eine vom vzbv von Oktober 2002 bis Dezember 2002 durchgeführte, nicht repräsentative Untersuchung der Internetauftritte von 48 Finanzdienstleistern hat gezeigt, dass der Verbraucher bei den meisten Finanz-Websites bei einer Vertragsanbahnung nicht umfassend informiert wird (vzbv 2003). Die Defizite betreffen vor allem Produktinformationen, aber auch Informationen über die Rechte des Verbrauchers, sich vom Vertrag zu lösen oder sich bei einer unabhängigen Stelle zu beschweren. Lediglich einzelne Anbieter von Finanzdienstleistungen stellen dem Verbraucher die notwendigen Informationen auf ihrer Homepage auch so aufbereitet zur Verfügung, dass er sie einfach auffinden und verstehen kann.

So wurde in allen untersuchten Versicherungssparten nicht über teilweise existenzbedrohende Deckungslücken oder gravierende wirtschaftliche Nachteile und Besonderheiten der angebotenen Produkte aufgeklärt – lediglich bei KfZ-Versicherungen ergab sich ein besseres Bild. So informierte zum Beispiel bei Hausratversicherungen nur einer der sieben untersuchten Anbieter über den fehlenden Versicherungsschutz bei sogenannten Elementarschäden wie Überschwemmung, Erdbeben, Erdbeben und ähnlichen Gefahren. Bei Kapital-Lebens- und fondsgebundenen Versicherungen informierte keiner der elf Anbieter über die zum Teil erheblichen Abschlusskosten und die daraus resultierende Beeinträchtigung der Verfügbarkeit der angesparten Gelder. In der Angebotsberechnung wird nur in einem einzigen Fall die unterstellte Verzinsung genannt, jedoch wurde auch hier keinerlei Aussage dazu gemacht, worauf sich die Verzinsungsannahme gründet.

Durch die neuen Verbraucherschutzregeln beim Fernabsatz von Finanzdienstleistungen gelten für die Unternehmen inzwischen zwar umfassende Informationspflichten. Jedoch wird die Praxis zeigen, ob die Verbraucher dadurch einen wirklichen Informationsgewinn erfahren. Jedenfalls sind die gesetzlichen Vorschriften nicht dafür ausgelegt, dem Verbraucher den Produktvergleich zu erleichtern. Hier wird seit langem eine klare, verständliche und einheitlich strukturierte Information durch die Unternehmen eingefordert.

Europaweit: 100 Einkäufe - 57 korrekt geliefert

In einer anderen Untersuchung hat das Europäische Verbraucherzentrum (EVZ) bei 114 grenzüberschreitenden Testeinkäufen die Erfahrung gemacht, dass nur etwas mehr als die Hälfte korrekt bearbeitet wurde. Die Autoren der Studie bezeichnen das Ergebnis insgesamt als „beschämend und alles andere als eine Werbung für den elektronischen Handel“ (EVZ 2003, S. 12). Nach den Ergebnissen der Studie kann ein Verbraucher, der übers Jahr 100 Mal etwas im Internet bestellt, damit rechnen dass

- acht Bestellungen schlicht ignoriert werden
- fünf Bestellungen nicht bestätigt, aber stillschweigend geliefert und abgerechnet werden
- 18 Bestellungen nicht geliefert werden, aber auch nicht abgerechnet
- acht Bestellungen zwar abgerechnet, aber nicht geliefert werden
- nur 57 Bestellungen korrekt bestätigt, geliefert und abgerechnet werden.

Wird eine Bestellung nicht beachtet, entsteht zwar kein materieller Schaden, aber die Autoren fragen „nach der Sinnhaftigkeit des elektronischen Handels“, wenn so mit Kundenwünschen verfahren wird (ebd.). Wird ein Auftrag nicht bestätigt, ist für den Verbraucher nicht ersichtlich, ob die Bestellung geklappt hat und wann er mit einer Lieferung rechnen kann (ebd. S. 12f).

„Geht nicht? Passt nicht? Ihr Pech.“

Bei den verschiedenen Studien zeigt sich, dass vor allem der Umtausch national und international erhebliche Probleme aufwirft. Die vergleichende Studie von Consumers International fand heraus, dass der Kunde nur auf jeder dritten deutschen Website eine Information findet, wie er Waren zurückgeben kann. Damit lag Deutschland am unteren Ende der Skala hinter Frankreich (46 Prozent) und den Niederlanden (55 Prozent). Oft bleibt für den Verbraucher jedoch völlig unklar, wer die Kosten der Rücksendung trägt. Er wird einem zusätzlichen psychologischen Druck ausgesetzt, weil 59 Prozent der deutschen Seiten nach dem Grund einer Rücksendung fragen, der höchste Wert in Europa (alles ConsInt S. 36f). Dies kann zwar auch interne Zwecke des Qualitätsmanagements haben, aber dann muss der Verbraucher darauf hingewiesen werden, dass diese Angabe freiwillig ist und er nach geltendem Recht in Deutschland 14 Tage lang, EU-weit nach der Fernabsatzrichtlinie mindestens sieben Tage lang nach Erhalt der Ware ohne Begründung vom Kaufvertrag zurücktreten kann. Einige Websites, vor allem international, hatten darüber hinaus sehr restriktive, mithin zumeist rechtswidrige Regelungen bezüglich der Rückgabe und akzeptierten sogar nur defekte oder beschädigte Güter (ebd., S. 25). Die Möglichkeit, eine einmal gemachte Bestellung zu widerrufen, boten immerhin 55 Prozent der europäischen Sites, etwas häufiger als US-Websites (49 Prozent, ebd.). Verbraucher sind also gezwungen, sehr genau vorher die Rückgabemöglichkeiten und -kosten zu überprüfen, bevor sie etwas online kaufen.

Regionaler Vergleich von Praktiken im E-Commerce

	Frankreich	Deutschland	Niederlande	EU Durchschnitt
Information über Rücktrittsmodalitäten	46	35,5	55	52
Information über Sicherheitspraktiken	90	77	65	74,5
Informationen über die Gesamtkosten	13	6,5	27	12
Bestellung kann im letzten Stadium storniert werden	61,5	64,5	100	60
Bestellung	77	93,5	90	80
-beinhaltet Information über Rücktrittsrecht	7	11,5	19	17
-beinhaltet Garantie-Informationen	0	0	0	10

Quelle: Consumers International, Should I buy? 2001, Angaben in Prozent der Websites

Der Grundsatz „Erst Ware, dann Geld“ gilt nicht mehr

Das EVZ prüfte nicht nur die Rücksende-Informationen der Anbieter, sondern machte die Probe aufs Exempel: 57 der 75 gekauften Produkte wurden zurückgeschickt. Dabei machten die Testeinkäufer die Erfahrung, dass sie nur in 39 Fällen auch ihr Geld wiederbekamen. Rechnet man hinzu, dass neun Produkte zwar bezahlt, aber nie geliefert wurden, so ist bei den Testeinkäufen des EVZ insgesamt bei einem Viertel der Waren ein Schaden in Höhe des Kaufpreises entstanden (EVZ 2003, S. 16).

Denn bei der Bezahlung gilt im Internet nach Erfahrung des EVZ europaweit nicht mehr der Grundsatz „Erst Ware, dann Geld“. Zahlte der Kunde mit Kreditkarte, erfolgte die überwiegende Zahl der Abbuchungen bereits innerhalb der ersten zwei Tage nach der Bestellung und damit in der Regel vor der Lieferung. Im Schnitt lagen sechs Tage zwischen Abbuchung und Lieferung - ohne vorherige Einwilligung des Verbrauchers.

Diese Vorliebe für Vorkasse bestätigt sich bei der Händlerbefragung der Postbank/Europressedienst 2004-Studie zu den bevorzugten Bezahlverfahren: 30,8 Prozent der Händler hätten am liebsten Vorkasse, 17,6 Prozent können sich noch für die Kreditkartenzahlung begeistern, Nachnahme und Rechnung finden nur jeweils etwa 15 Prozent Anhänger (Postbank/Europressedienst 2004, S. 62).

Dies führte dazu, dass nicht gelieferte oder defekte Ware in jedem Fall bezahlt wurde und der Verbraucher nicht sicher sein kann, ob er sein Geld jemals wiedersieht.

Die Bedingungen für den Online-Einkauf verdienen nach diesen Ergebnissen allenfalls die Note mangelhaft. Verbraucher werden schlecht informiert, ihre Rechte werden nicht gewahrt, sie gelangen nur schwer an die notwendigen Informationen und werden, wie bei der stillschweigenden Vorkasse, teilweise auch schlicht übervorteilt.

Rückgaberecht bei ebay

Es bedurfte des Gangs durch alle Instanzen und eines Urteils des Bundesgerichtshofes vom 03.11.2004, um durchzusetzen, dass gewerbliche Anbieter auch über ebay ihre Waren mit Rückgaberecht verkaufen. Der BGH bestätigte mit seinem Urteil die Auffassung des vzbv, wonach alle gewerblichen Anbieter bei ebay ihren Kunden - wie bei anderen Internet-Kaufverträgen - ein 14-tägiges Rückgaberecht einräumen müssen. Das Problem ist hier allerdings noch immer, dass nicht alle gewerblichen Anbieter auch als solche auftreten. Der vzbv fordert daher eine obligatorische Kennzeichnungspflicht gewerblicher Anbieter.

Im vorliegenden Fall hatte ein Schmuckhändler auf Zahlung des Kaufpreises geklagt. Er bot 2002 auf der ebay-Website ein Armband zur Versteigerung an - mit der Zusage, dass es angeblich aus 15 Karat Gold bestehe und zudem mit 15 Karat Edelsteinen besetzt sei. Der Ersteigerer gab das Armband, das tatsächlich nur eine dünne Goldauflage aufwies und dessen Steine aus industrieller Fertigung stammten, zurück und weigerte sich, das Schmuckstück zu bezahlen.

„Zahlen bitte ...“ – Bezahlssysteme als Schwachstelle des E-Commerce

Wer im Internet einkaufen oder Dienstleistungen nutzen möchte, muss auch zahlen. Die kommerzielle Nutzung des Internet hängt von der Möglichkeit des Bezahls ab. Dabei sind Zahlungssysteme dem Internet mit seiner ursprünglichen Philosophie des allgemeinen freien Informationsaustausches im Prinzip fremd. So wurde eine Reihe spezieller internet-kompatibler Bezahlverfahren entwickelt, die sich in der Regel aber (noch) nicht allgemein durchsetzen konnten. Die Grundprinzipien derartiger Zahlungssysteme beruhen entweder auf einem Vorkassensystem, bei dem Beträge anschließend gegenüber Anbietern eingesetzt werden können. Der Verbraucher vergibt hier quasi Kleinkredite durch seine Vorleistung. Oder es sind Inkasso- beziehungsweise Billingsysteme, die die Beträge hinterher per Lastschrift vom Konto oder über die Telefon- oder Providerrechnung einziehen. Einzelne Systeme sind dabei bekannter geworden, weil sie es geschafft haben, mit mehreren interessanten Anbietern zusammenzuarbeiten oder einem der großen Internetprovider oder einer bedeutenden Internethandelsplattform angehören. Letzteres betrifft etwa das System PayPal, das zur ebay-Plattform gehört und als Besonderheit eine begrenzte Garantiefunktion enthält, die eine Rückholung des Betrages verspricht, sollte die Ware nicht geliefert werden oder dem Bestellten nicht entsprechen. Derartige Absicherungen sind jedoch selten. Insgesamt haben sich bisher die herkömmlichen Zahlungsweisen des Offline-Handels im Internet durchgesetzt: Überweisung, Nachnahme, Lastschrift und Kreditkartenzahlung.

Vor allem bei Kreditkartenzahlungen kommt es immer wieder zum Missbrauch, da in der Regel die Angaben lediglich der Kreditkarten- oder Kontoinformationen für den Bezahlvorgang ausreichen. Auch wenn man als Verbraucher diese Daten zur Abwehr von Ärger nur sehr vorsichtig im Internet einsetzen sollte, sind dies aber keine Geheimdaten. Jeder ver-

traglich gewollte Einsatz gibt diese Daten Dritten preis. Das gilt auch für die kleine Prüfziffer, die einige Kartensysteme der Kartenummer auf der Rückseite offen angebracht haben und die von einigen Anbietern heute zusätzlich abgefragt wird.

Abgesehen vom möglichen Ärger ist der Verbraucher rechtlich gesehen aber weitgehend geschützt, denn eine Buchung, die er nicht ausgelöst hat, braucht er auch nicht zu bezahlen. Der Händler beziehungsweise das Kartenunternehmen müssen nachweisen, dass sie es mit dem richtigen Verbraucher zu tun hatten.

SET-System: Geschädigte Verbraucher in der Beweispflicht

Auf Grund des zunehmenden Schadens bei den Kartensystemen wurden neue Sicherheitssysteme erdacht. So soll das SET-System (Secure Electronic Transaction System) über eine Software beim Händler, der Bank und dem Verbraucher einen PIN-Code vom Verbraucher abfragen. Dieses Verfahren schränkt für den Verbraucher das Risiko stark ein, an einen unseriösen Händler zu geraten. Das Nachsehen hat der Verbraucher aber dann, wenn es Hackern gelingt, den PIN-Code im Rahmen dieser Softwarelösung zu erlangen. In derartigen Fällen kann sich ein solches Schutzsystem gegen den Verbraucher wenden, weil ihm voraussichtlich wie bei der unberechtigten Geldabhebung mit PIN grob fahrlässiges Handeln unterstellt werden wird - wenn nicht sogar der Betrug, die Zahlung selbst ausgelöst zu haben. Neben der unzureichenden Absicherung kommt ein weiterer Nachteil hinzu, denn für das SET-System ist eine Softwareinstallation erforderlich, die nicht überall erlaubt und möglich ist.

3.2 Online-Banking

Etwa 20 Millionen Bundesbürger erledigen derzeit ihre Bankgeschäfte am Computer. Was noch vor einigen Jahren eine Nische nur für wenige risikobereite Onlinenutzer war, hat sich nicht zuletzt durch die Ausbreitung des Internetzugangs wie auch wegen der Bequemlichkeit und Flexibilität dieser Form des Bankbesuches zu einer bedeutenden Form des E-Commerce entwickelt. Die Banken befördern diesen Trend durch die Preisgestaltung, denn Online-Konten sind meist viel preiswerter als herkömmliche Girokonten.

Die Sicherheit bleibt dabei jedoch auf der Strecke: Im Lichte der zunehmenden Angriffe, der seit langem bekannten Gefahren und der Existenz wesentlich besserer Sicherheitssysteme wird man das Verhalten der meisten Banken in Bezug auf die aktuelle Absicherung des Online-Banking mit dem PIN/TAN-Verfahren in einem Schadensfall nur als „grob fahrlässig“ bezeichnen können.

Der großen Skepsis der technisch versierteren Internetnutzer der ersten Stunde begegnete die Kreditwirtschaft zunächst mit ambitionierten Sicherheitsverfahren. HBCI (Homebanking Computer Interface) heißt der Standard, der bereits 1996 mit Verschlüsselungssätzen und Chipkarten diesen Sicherheitsbedenken begegnen wollte. HBCI setzte sich bereits mit dem Risiko auseinander, dass Schadprogramme schon die Tastatureingaben am heimischen Computer abfangen, Passwörter verraten und Buchungen manipulieren könnten. Der vom HBCI-Verfahren gebotene hohe Sicherheitsstandard wurde jedoch nie wirklich flächendeckend eingeführt, denn er war zu teuer: die Kreditwirtschaft hätte die erforderliche Hardwareausstattung (Kartenlesegeräte) beim Verbraucher gezielt fördern müssen. Neben den Kosten bestehen weitere Hindernisse: So wäre etwa die weit verbreitete Nutzung des

Online-Banking am Arbeitsplatz nur möglich, wenn auch die Arbeitgeber bereit wären, diese Zusatzausrüstung an ihrer Hardware zuzulassen.

Mit der Verbreitung des Internets als Massenmedium rückte das Wissen um die technischen Details und damit das Risikobewusstsein in den Hintergrund. Online-Banking wurde für Verbraucher mit Online-Anschluss praktisch zur Selbstverständlichkeit. Für die Banken entfiel damit die anfängliche Notwendigkeit, vertieft auf die Sicherheitsaspekte einzugehen, damit diese Vertriebsform überhaupt ihren Markt findet. Parallel konnten sich die Banken immer mehr auf die pauschale Aussage zurückziehen, ihr System sei sicher. Interessant ist aber, dass das Kriterium der mangelnden Sicherheit genau bei denjenigen, die sich bewusst gegen die Nutzung von Online-Banking im Internet entschieden haben, nach wie vor an der Spitze steht (vgl. Bundesverband deutscher Banken/ipos).

Online-Konten aus Bankenperspektive: Kostenverlagerung nach außen

Für die Banken hat Online-Banking in erster Linie einen Rationalisierungsaspekt: Die Kunden erledigen damit viele Arbeiten selbst, die früher ein Bankmitarbeiter für sie gemacht hat. Bereits 1999 stellte eine Untersuchung der Arbeitsgemeinschaft der Verbraucherverbände (AgV) dazu fest: „Vom Kunden wird verlangt, dass er sich eine neue Herangehensweise für das Banking aneignet. (...) Angesichts der Heterogenität der Bankkundschaft trifft dies auf völlig unterschiedliche Eignungen und Vorkenntnisse beim Kunden.“ (AgV 1999, S. 4). Dies führt dazu, dass den Verbrauchern zwar der Aspekt der Bequemlichkeit und Verfügbarkeit mittlerweile einleuchtet, sie sich der Risiken jedoch nicht bewusst sind.

Heute funktioniert Online-Banking vermeintlich einfach: Jeder Computer mit einem Browser kann zum Bank-Terminal werden. Die SSL-Verschlüsselung ersetzt die Chipkarte, der Browser die Banksoftware. Der Kunde baut mit dem Klick auf den „Online-Banking“-Link seiner Bank eine SSL-verschlüsselte Verbindung zu seiner Bank auf. Dort loggt er sich mit seiner vier- bis sechsstelligen PIN ein. Für jede Transaktion gibt er zusätzlich eine für sein Konto freigeschaltete, sechsstellige Transaktionsnummer (TAN) an, die er von seiner Bank vorher per Post zugeschickt bekommt. Dieses ganz überwiegend eingesetzte Zugangsverfahren ist abgesehen von der Verschlüsselung noch immer im Prinzip dasselbe Zugangssystem, das es bereits beim alten BTX-Dienst der Telekom gab. In abgewandelter Form existiert es als T-Online classic-Dienst bis heute. Einziger, allerdings bedeutender Unterschied zum Internet: Der Dienst bildet ein geschlossenes Netzwerk, bei dem der Nutzer eindeutig identifizierbar ist. Erst 2003 wurde das veraltetete PIN/TAN-Verfahren auch noch in den HBCI-Standard des Zentralen Kreditausschusses für das Internet als „HBCI PIN/TAN“ aufgenommen. Sicherheitstechnisch muss dies als Rückschritt bewertet werden.

Angriffe auf Verbraucher nehmen zu

In jüngster Zeit nehmen die Angriffe auf den Verbraucher zu, realisiert sich genau das, weswegen aufwendigere Schutzsysteme ursprünglich vorgesehen waren. Gab es seinerzeit eher vereinzelte Angriffe von Hackern, die vor allem zeigen wollten, dass sie Schutzsysteme knacken konnten, geht es Kriminellen heute um den Zugriff auf das Geld von Verbrauchern. Nach dem bereits in den USA erhebliche Schäden entstanden sind, ist spätestens seit Mitte 2004 auch der gezielte Angriff auf Konsumentenkonten hierzulande Realität geworden.

Bis heute ist es den Banken in Deutschland zwar überwiegend gelungen, Angriffe in letzter Konsequenz noch abzuwehren. Dies war jedoch nicht dem Zugangsschutz geschuldet, sondern schnellem Handeln bei der Kontrolle der Buchungen, als man die Taten bemerkte. Es bleibt daher offen, ob es immer gelingen wird, rechtzeitig und nicht zum Schaden des betroffenen Verbrauchers den elektronischen Griff in das Konto zu unterbinden.

Ein genereller Schwachpunkt vieler Sicherungssysteme im Zahlungsverkehr ist nicht das Kernsystem selbst. So wird vermutlich jeder Experte bei genauerer Analyse des Schutzbeziehungsweise Verschlüsselungsmechanismus diesen als sicher bezeichnen. Der Fehler liegt vielmehr darin, dass nicht das gesamte Einsatzumfeld betrachtet wird. Alle Sicherheitssysteme sind jedoch nur so viel wert, wie sie auch beim Verbraucher Schutz vor dem Auspähen und Kopieren von Zugangsdaten und Überweisungsvorgängen bieten.

Gefahr durch „Phishing“: „Dürfen wir Ihre Daten haben?“

Für Online-Banking muss der Verbraucher eine Menge Zahlen bei sich haben: Seine Kontonummer, die Zugangspin, seine TAN-Listen. Wer Kontonummer und PIN jedoch kennt, hat Zugriff auf die Kontodaten. Wer zusätzlich noch die TANs besitzt, kann Überweisungen ausführen. Diese Daten sind für Betrüger von großem Wert und sie versuchen mit „social engineering“, also psychologischen Tricks, an die Zugangsinformationen der Verbraucher zu kommen.

Ende 2004 trat eine Vorgehensweise ins Licht der Öffentlichkeit, die Betrügern Tausende von Kontodaten liefern sollte: „Phishing“. Beim Phishing imitiert eine E-Mail Design und Sprache großer Bankinstitute. Darin wird der Nutzer gebeten, auf einer Website seine PIN und Transaktionsnummern an die Bank zu senden. Mit diesen Daten versuchen die Betrüger dann, die Konten leerzuräumen. Teilweise wird in den Mails angedroht, das Konto zu sperren, wenn der Nutzer nicht reagiert, was den psychologischen Druck auf die Verbraucher erhöht. Von Mai bis November 2004 registrierte zum Beispiel der Anti-Viren-Hersteller Trend Micro 9.709 Phishing-Mails.

Beispielmail

Dear Citibank Customer,

We recently noticed one or more attempts to log in to your Citibank account from a foreign IP address and we have reasons to believe that there was attempts to compromise it with brute forcing your PIN number.

No successful login was detected and you have full protection by now. If you recently accessed your account while travelling, the unusual login attempts may have been initiated by you.

The login attempt was made from:

IP address: 173.77.177.24

ISP Host: cache-282.proxyserver.cis.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site.

However, because user verification on the Internet is difficult, Citibank cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system to help you evaluate with whom you are dealing with. The system is called CitiSafe and it's the most secure Citibank wallet so far.

If you are the rightful holder of the account, click the link bellow, fill the form and then submit as we will verify your identity and register you to CitiSafe free of charge. This way you are fully protected from fraudulent activity on all the accounts that you have with us.

[Click to protect yourself from fraudulent activity!](#)

To make Citibank.com the most secure site, every user will be registered to CitiSafe.

NOTE! If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

** Please do not respond to this e-mail, as your reply will not be received.*

Regards, Citibank Customer Support

Wie kann der Verbraucher erkennen, dass diese Mail nicht von seiner Bank stammt? Die Absender-Adressen sind teilweise so raffiniert gefälscht, dass auch ein versierter Internet-Nutzer den Betrug kaum erkennen kann. Im unteren Beispiel versteckte sich der falsche Link im HTML-Code, teilweise taucht er sogar nur als Zahlen-code auf - für den Normal-Nutzer nicht zu erkennen.

Oder noch gewitzter: Die Kunden der Citibank bekamen Ende 2004 eine gefälschte Mail mit einer URL, die die richtige Citibank-Seite öffnete (siehe Kasten links). Nur das Pop-Up-Menu, das sich vor die echte Seite legte und in das der Kunde seine geheimen PINs und TANs eintippen soll, führte zu einer manipulierten Website. Hier nützen auch Virens Scanner und Firewalls nichts - wer seine Daten weitergab, verschaffte einem Kriminellen freien Zugang zu seinem Konto. Immerhin wurde begonnen, manche Browser mit Warnmeldungen in solchen Fällen nachzurüsten.

Haftungsrisiko liegt beim Verbraucher

Geht der Verbraucher einem Betrüger auf den Leim, hat er den Schaden. Auch wenn die Rechtsfolgen und Haftungsfragen für diese Fälle gerichtlich noch zu klären sind, hat hier der Verbraucher ja objektiv zunächst selbst seine Zugangs-

daten Fremden weitergegeben. Mit besonderen Informationsseiten versuchen die Banken seit den Phishing-Vorfällen ihre Kunden zu sensibilisieren - allerdings sind sie es selber, die mit den kurzen PIN/TAN Kennziffern und dem Verzicht auf Hardware-orientierte Schutzsys-

teme die Methode Phishing überhaupt erst möglich erfolgreich machen. Denn diese Methode setzt voraus, dass Verbraucher einem Unbefugten sinnvoll einsetzbare Zugangsdaten überhaupt übertragen können. Dabei gibt es heute längst technische Möglichkeiten und Verfahren, die genau dieses ausschließen und die auch bereits in Nachbarländer eingesetzt werden.

Sicheres Online-Banking nur für Belgier und Niederländer?

Beispielsweise haben die Banken in Belgien und den Niederlanden für Online-Banking nie auf das PIN/TAN-Verfahren gesetzt, weil es als zu unsicher gilt. Hier bekommt der Verbraucher ein als Token bezeichnetes Zusatzgerät (Kostenpunkt 5 Euro) mit dem man passend zu seinem Überweisungsauftrag ein Passwort generiert, das zum Beispiel nur wenige Momente lang gültig ist. Lange genug, um als Berechtigter die Buchung auszulösen, zu kurz für einen Betrüger, das abgefragte Passwort zum Schaden des Verbrauchers und der Bank anderweitig nutzen zu können. Dieses Zusatzgerät kann von einem Schadprogramm weder abgefragt noch manipuliert werden, weil es eine vom Computer des Verbrauchers und vom Internet unabhängige Komponente darstellt. Andere neue Verfahren sehen vor, dass der Überweisungsauftrag beim Bankrechner die Versendung einer SMS an das Handy des berechtigten Verbrauchers auslöst. Erst wenn der Verbraucher diese, nur ihm auf einem von seiner Internetverbindung völlig unabhängigen Weg zugegangene Zusatzinformation eingibt, wird die Buchung ausgelöst. Auch bei diesem Verfahren ist es nicht möglich, einem Fremden versehentlich nutzbare Zugangsdaten zukommen zu lassen. Auch ein Angriff über ein verstecktes Spionageprogramm auf dem eigenen Rechner hat hier keinen unmittelbaren Erfolg.

Die Verantwortlichkeit für sichere Systeme liegt klar auf Seiten der Banken, denn: Der Verbraucher kann nur nutzen, was ihm als Sicherheitssystem angeboten wird. Deshalb ist es die Pflicht der Anbieter, unsicher gewordene Systeme abzuschalten. Allerdings taugen als Ersatz nur faire Sicherungssysteme, die alle Parteien gleichberechtigt in ihr Schutzkonzept einbeziehen. Ein Schutzsystem darf es nicht mehr zulassen, dass der Verbraucher und sein Rechner das schwächste Glied im Schutzsystem sind, auf die man die Verantwortung abschieben kann.

Beispiel versteckter Link:

Der Link in der Mail lautet:

<http://www.postbank.de/?43x6l0o6l14m8gC4HI53c6DIUvbZe199c5e1l43yn0w1f2pHOpaz9c4Oa3e1o5JgJkns3rm>, ein für den Benutzer auf den ersten Blick kryptischer Zahlencode, der aber bei vielen Links, die einem Benutzer gezielt zugesandt werden, vorkommt, um ihn bei dem Besuch der Internetseite auch identifizieren zu können. Auf den ersten Blick eindeutig eine Seite der Postbank. Ruft man diesen Link aus der Originalmail auf, landet man auf einer ganz anderen Seite, die man mit der angekündigten Seite der Postbank verwechseln könnte, die tatsächlich aber in Russland registriert ist. Denn in der Mail steckt folgender Code:

```
<a href="http://www.postbank.de|fpoi9rg.da.RU/?2fu0QNG5S8mUxPzq9lGO57N2cn">  
http://www.postbank.de/?43x6l0o6l14m8gC4HI53c6DIUvbZe199c5e1l43yn0w1f2pHOpaz9  
c4Oa3e1o5JgJkns3rm</a><br><br>
```

Die erste Adresse mit dem fast nicht auffallenden "fpoi9rg.da.ru" am Ende wird aufgerufen, dabei wird der Text www.postbank.de einfach ignoriert, die zweite Adresse ohne diese Manipulation als eindeutige postbank.de-Adresse in der Mail angezeigt. So kann der Nutzer schnell getäuscht werden, selbst wenn er noch einmal flüchtig in die Adresszeile des Browsers schaut. Auffällig: Die Postbank spricht ihre Kunden auf der falschen Seite auf Englisch an, aber bei weltweit operierenden Banken wie zum Beispiel der Citibank würde das die meisten Nutzer kaum verwundern.

3.3 Urheberrechte und Digital Rights Management

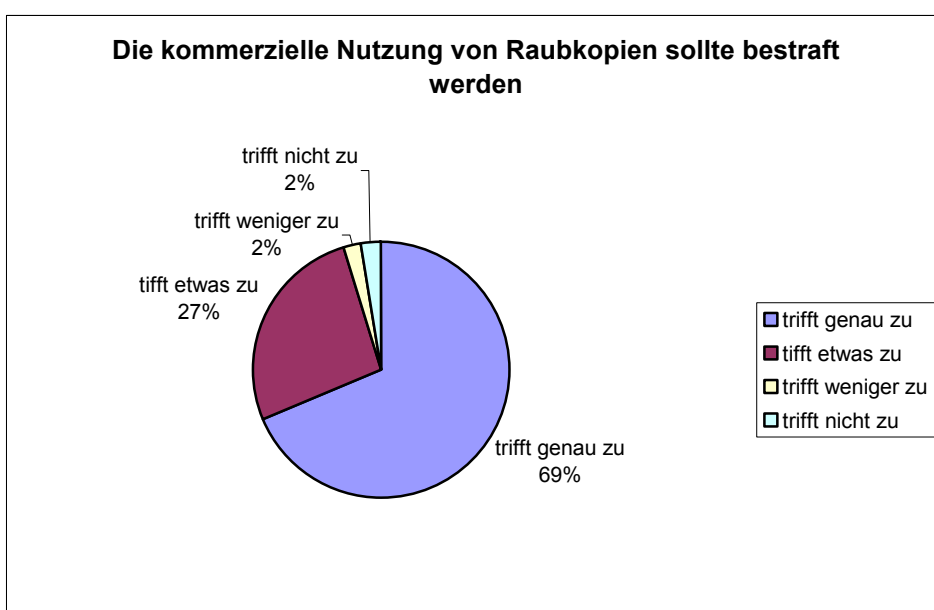
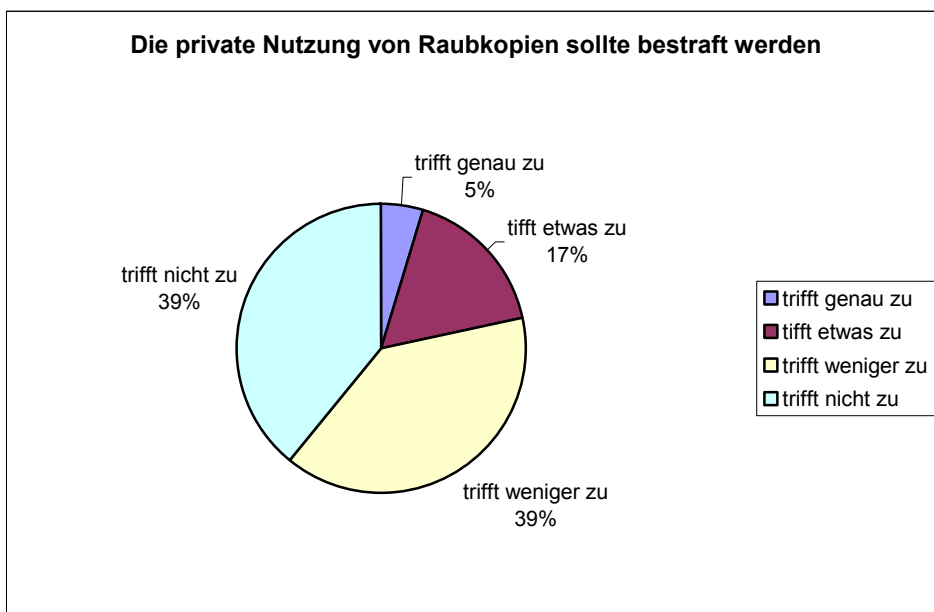
„Was analog ist, können die Nutzer sich digital zumailen lassen. Für das, was digital ist, müssen sie physisch in die Bibliothek gehen. Absurde Welt.“ Volker Grassmuck

Durch die aktuelle Gesetzgebung kann der Verbraucher schon mit der simplen Kopie einer CD eine Straftat begehen, ohne sich dessen bewusst zu sein. Die Gesetzgebung orientiert sich bisher in erster Linie an wirtschaftlichen Interessen und vernachlässigt dabei die Bedürfnisse von Privatanwendern und der Informationsgesellschaft, die es dringend zu schützen gilt, sollen nicht Innovation und Kultur behindert werden.

Die Diskussion um die Privatkopie hat viele Menschen verunsichert. Der Hintergrund des Streits ist ein Technologiewechsel: Bei analogen Daten ist der Privatkopie eine physikalische Grenze gesetzt, da analoge Kopien mit zunehmender Häufigkeit an Qualität verlieren. Dies ist bei digitalen Daten nicht der Fall, so dass sie auch für den Privatanwender mit seiner Technik daheim beliebig oft kopierbar sind. Da das Internet ursprünglich ein Forschungsnetz war, dazu gebaut, um Informationen unter Wissenschaftlern zu teilen und auszutauschen, herrscht hier die Idee vom *free flow of information*. Dieses Konzept steht im Gegensatz zu den Interessen der Rechteinhaber an digital vorliegenden Texten, Musik und Software, die ihre Einkommensquellen versiegen sehen. Doch vielen Verbrauchern ist gar nicht bewusst, ab wann sie eine Straftat begehen.

Fehlendes Unrechtsbewusstsein bei Software

Eine Studie zur „Digitalen Mentalität“ des Institutes für Strategieentwicklung gemeinsam mit der Universität Witten/Herdecke im Jahr 2004 kommt zu dem Schluss: „... die Tatsache, dass der Einsatz nicht ordnungsgemäß lizenzierter Software eine Straftat ist, scheint in der öffentlichen Meinungsbildung keine Rolle zu spielen“ (Digitale Mentalität 2004, S. 3). Dies hat den Autoren der Studie zufolge damit zu tun, dass der Nutzer beim Kopieren von digital vorliegender Software oder Musik niemandem etwas physisch „wegnimmt“, das den historisch gewachsenen Vorstellungen von Diebstahl zugrunde liegt. Auffällig ist, dass das Rechtsverständnis der Deutschen sehr wohl die kommerzielle Nutzung von Raubkopien verurteilt: 68,5 Prozent der Befragten geben an, dass dies bestraft werden sollte, während nur 4,8 Prozent die Privatkopie bestraft sehen wollen (ebd. S. 14). Insgesamt hat die Rechtsprechung bisher vor allem die Interessen der Rechteinhaber zu stärken versucht, stark kritisiert von Verbraucherverbänden.



Die Urheberrechtsnovelle zur Privatkopie: Kriminalisierung der User

Der Entwurf für den zweiten Korb der Urheberrechtsnovelle sollte die Belange der Nutzer stärker berücksichtigen als der erste Korb, der von Verbrauchervertretern und Bürgerinitiativen stark kritisiert wurde. Nach Ansicht des vzbv werden hier die Nutzerrechte jedoch noch einmal deutlich verschlechtert. Der Nutzer hat zwar pro forma das Recht, seine digital vorliegenden Daten zu kopieren, aber ob er dieses Recht ausüben kann, entscheidet der Hersteller. Denn nur wenn dieser freiwillig auf einen Kopierschutz verzichtet, kann der Nutzer seine eigenen CDs auch auf den MP3-Player kopieren und mit zum Joggen nehmen. Umgeht er zu diesem Zweck die Kopierschutzmechanismen, begeht er eine Straftat, obwohl er die Musik rechtmäßig erworben hat.

Zudem sollen Kopien in Zukunft verboten sein, wenn eine „...offensichtlich rechtswidrig...öffentlich zugänglich gemachte Vorlage verwendet wurde“. Auch dies kann zu gefährlichen Konsequenzen für den Nutzer führen, der in Zukunft vor dem Download prüfen müsste, ob die Datei rechtmäßig im Internet platziert worden ist. Es ist denkbar, dass beispielsweise Stücke bekannter Musiker zur Promotion kostenlos angeboten werden. Wie der Verbraucher beurteilen soll, ob dies rechtmäßig geschieht, bleibt ungeklärt.

Bildung und Forschung blockiert

Sowohl auf europäischer als auch auf nationaler Ebene gehen Verbrauchervertreter davon aus, dass die neue Gesetzeslage Bildung und Forschung behindern wird. Bibliotheken dürfen nach der neuen Gesetzeslage ihre Daten zwar in der Bibliothek elektronisch zeigen, aber nur noch dann elektronisch versenden, wenn der Rechteinhaber dies selbst nicht anbietet. Welchen Preis dieses Angebot hat, spielt allerdings keine Rolle. Gleichzeitig dürfen die Bibliotheken weiterhin analog vorliegende Aufsätze als Graphik-Datei einscannen und dem Nutzer senden. „Was analog ist, können sie (die Nutzer, Anmerkung der Autorin) sich digital zumailen lassen. Für das, was digital ist, müssen sie physisch in die Bibliothek gehen. Absurde Welt“, resümiert Volker Grassmuck in *telepolis* im September 2004 (www.telepolis.de). Der Förderverein für eine Freie Informationelle Infrastruktur (FFII) stellt fest: „Während die Rechteindustrie alle Möglichkeiten der digitalen Technologien für sich nutzen kann, sollen die Interessen der Allgemeinheit auf die Möglichkeiten der analogen Vergangenheit beschränkt werden.“ Der Europäische Dachverband der Verbraucherorganisationen BEUC sieht hier ebenfalls Handlungsbedarf: „Eine Kosten-Nutzen Analyse sollte die Effekte der Urheberrechtsgesetzgebung untersuchen (...) um herauszufinden, ob das Urheberrechtssystem die Bedürfnisse der Informationsgesellschaft und die von Wirtschaft und Verbrauchern erfüllt und gleichzeitig die Vorteile des Wettbewerbs voll ausschöpft.“ (BEUC 2004).

Gefahr: Gläserne Nutzer

Verbrauchervertreter und Informatiker sehen die gleichen Gefahren: Verknappung und Verteuerung von Informationen, eine stärkere „digitale Spaltung“ der Gesellschaft sowie eine Verletzung der Privatsphäre der Nutzer. Es gibt bereits Pläne für DRM-Systeme, die in Hardware integriert werden, laufend die Daten des Nutzers ausspähen und diese Informationen an die Hersteller weitersenden. Die Industrie setzt bisher ausschließlich auf restriktive

Systeme, die die Rechte des Nutzers einschränken. Gerade durch diese Systeme aber tun sich neue Sicherheitslücken auf: Im Januar 2005 tauchte ein Trojaner auf, der durch den DRM-Schutz von Windows-Media-Dateien eine Hintertür für Spyware öffnet: Der Media Player 10 versucht bei jeder Datei automatisch, fehlende Lizenzen aus dem Internet nachzuladen und öffnet dazu ein Browserfenster. In WMA-Dateien, angeblich Songs von Alicia Keys, war jedoch der Trojaner Trj/WmvDownloader.A enthalten. Er täuscht vor, eine Lizenz laden zu wollen und lenkt den Browser dann auf eine andere Seite um, die versucht, auf dem PC Adware, Spyware, Dialer und andere Viren zu installieren. Die urheberrechtlich korrekt agierenden Anwender wurden plötzlich mit unerwünschten Pop-Ups und Werbung überhäuft. Microsoft zeigte sich besorgt, dass in Zukunft die DRM-Funktion „missbraucht“ werde und beeilte sich, ein Update für den Media-Player anzukündigen, während bereits ein zweiter Trojaner namens Trj/WmvDownloader.B die Runde machte.

3.4 Datenschutz: Breite Datenspuren im Internet

Der Verbraucher gibt bereits Daten von sich preis, wenn er sich ins Internet einloggt und Websites ansieht. Dies ist den meisten Nutzern im Detail nicht bewusst, da dazu ein weites Verständnis der technischen Gegebenheiten nötig ist. Cookies und Gewinnspiele versuchen dann, dem Verbraucher weitere Daten zu entlocken und geben es an Werbetreibende weiter.

Wenn sich ein Nutzer in das Internet einwählt, gibt er dem Terminal-Server des Providers seine Login-Daten, also Nutzernamen und Passwörter. Der Terminal-Server merkt sich, wann, wie lange und mit welcher IP-Adresse dieser Verbraucher im Internet war. Der Verbraucher erhält daraufhin eine meist dynamische IP-Adresse von seinem Provider. Diese ändert sich bei jedem Zugang. Mit der IP-Adresse alleine ist der Verbraucher also nicht persönlich zu ermitteln, dazu müsste ein Außenstehender zusätzlich auf die Daten des Terminal-Servers zugreifen können. Der Proxy-Server des Providers speichert die Anfragen des Verbrauchers, also seine derzeitige IP, welche Websites er besucht hat und den Status dieser Anfragen. Zusätzlich wird oft noch die Browserversion des Clients, Angaben zum Betriebssystem und die Konfiguration des Rechners abgefragt, Informationen, die auch außenstehenden Websites zur Verfügung stehen. Der Nutzer gibt also schon Daten preis, ohne dass er selbst aktiv etwas tun muss, außer ins Internet zu gehen. Provider sind durch die Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet, diese Daten aufzubewahren und auf Wunsch den Ermittlungsbehörden auszuhändigen.

„Langlebige, schwatzhafte Kekse“

Kommerzielle Datensammler im Netz sind Cookies (engl. „Kekse“), die von Websites auf den Nutzer-PC abgelegt werden. Sie sind in der Lage, personenbezogene Daten des Verbrauchers an einen Werbetreibenden weiterzugeben. Cookies werden von einer Website direkt auf den Verbraucherrechner abgelegt. Meistens geschieht dies, ohne dass er dies merkt, denn bei den gängigen Browsern stehen die Voreinstellungen auf „*Alle Cookies akzeptieren*“. Der Nutzer kann hier einstellen, dass alle Cookies abgelehnt werden oder dass der Browser ihn jedes Mal fragt. Damit behält er vermeintlich die Kontrolle, doch das Dialog-Feld des Internet-Explorers warnt: „Sie können (den Cookie, Anmerkung der Autorin) ablehnen, aber möglicherweise ist eine einwandfreie Funktion nicht sichergestellt“ - eine weitere psychologische und technische Hürde für den unbedarften Surfer.

Cookies bestehen unter anderem aus folgenden Angaben: Die Heimatdomäne, die den Cookie auslesen darf, Gültigkeitsdauer, Name und Inhalt. Durch die Gültigkeitsdauer können Cookies entweder nur für eine Session oder aber für mehrere Jahre auf dem Rechner des Nutzers verbleiben: Ein am 25.01.2005 heruntergeladener Cookie von Ebay.com verfällt beispielsweise erst fünf Jahre später am 25.01.2010. Bis dahin loggt E-Bay Daten mit - welche, darüber gibt der Cookie keine Auskunft. Aus datenschutzrechtlicher Sicht sind vor allem diese dauerhaften Cookies bedenklich: Sie können das Verhalten von Internetnutzern aufzeichnen und diese Aufzeichnungen in Form von ASCII-Dateien festhalten. „Aufgrund dieser Aufzeichnungen ist dann der Cookie-erzeugende Web-Server in der Lage, (beim nächsten Besuch, Anm.d. A.) gezielt Werbung einzublenden“, gibt das BSI zu Bedenken (BSI 2001, S. 38).

E-Commerce als Datenfalle

Sobald der Nutzer eine Website nicht nur besuchen, sondern einkaufen, Clubs beitreten, Feedback geben oder Services nutzen will, wird er offen nach Daten gefragt. Interaktion im Internet ist meistens nur mit der Weitergabe persönlicher Daten möglich.

Doch auch hier lauern Gefahren: Spam-Versender versuchen, an Datenbanken mit gültigen E-Mail-Adressen oder Fax-Nummern zu gelangen, um ihre unerwünschte Werbung zu versenden, Marketing-Firmen erstellen Kundenprofile, manche Firmen öffnen ihre Datenbanken für Partnerunternehmen. In der Praxis wird der Datenschutz daher von den meisten E-Commerce-Anbietern an der einen oder anderen Stelle untergraben. Hierfür gibt es handfeste Anreize, da Nutzerprofile und korrekte Personendaten von konkret materiellem Wert sind – beispielsweise für die spätere Kundenaquise oder den gezielten Versand von Werbematerial. Des Werts der eigenen Daten sind sich die meisten Verbraucher dabei kaum bewusst.

EU und USA: Unterschiedliche Regeln zu Werbemüll

Jeder Betreiber von E-Commerce oder sonstigen Angeboten darf die Daten erheben, die unmittelbar zu diesem Zweck notwendig sind. Während sich der Verbraucher in den USA bewusst gegen eine weitere Datenspeicherung (zum Beispiel Geburtsdatum oder Interessen) und Werbung (zum Beispiel Programmiererweiterung oder Sonderangebote) entscheiden und diese Entscheidung kundtun muss, sieht man dieses Verfahren in Europa als eine zu große psychologische Hürde. Daher gilt in EU-Staaten die verbraucherfreundliche Opt-In-Regelung: Der Kunde muss seinen Willen ausdrücklich bekunden, etwa durch eine gesonderte Unterschrift oder gesondertes Ankreuzen, dass er seine Daten für Werbung und Marktforschung freigibt.

Konkret heißt dies: Auf amerikanischen Websites muss der Kunde ein Kästchen ankreuzen: „Ich will keine Werbung“, ansonsten bekommt er welche. Auf europäischen Websites muss er „Ich will Werbung“ ankreuzen, sich also aktiv für Werbung entscheiden. Dies wird allerdings gerne unterwandert: Dann ist das „Ich will“-Kästchen im Online-Formular von vornherein angekreuzt, so dass ein unachtsamer Nutzer es übersehen und seine Zustimmung unabsichtlich geben kann.

Daten verschwinden im Datendschungel

Die bereits zitierte Studie *Privacy@Net* von Consumers International hat sich auch mit der Frage beschäftigt, wie transparent die Datenverarbeitung und -weitergabe für den Verbraucher auf internationalen Ratgeber-Websites für Finanzen, Preisvergleich und Gesundheitsthemen ist. Das Ergebnis:

- fast alle besuchten Seiten sammelten persönliche Informationen über den Nutzer (99 Prozent)
- Name, Adresse, E-Mail und Telefon sind die am häufigsten abgefragten Daten
- nur 58 Prozent der besuchten Sites hatten ihre Datenschutzbestimmungen online
- nur 32,5 Prozent davon informierten den Nutzer darüber an der Stelle, an der die Daten erhoben wurden.

Auch über die Verwendung der Daten werden die Nutzer nur mangelhaft informiert. 39 Prozent der Websites machten deutlich, *welche* Daten sie sammeln, etwas über die Hälfte lie-

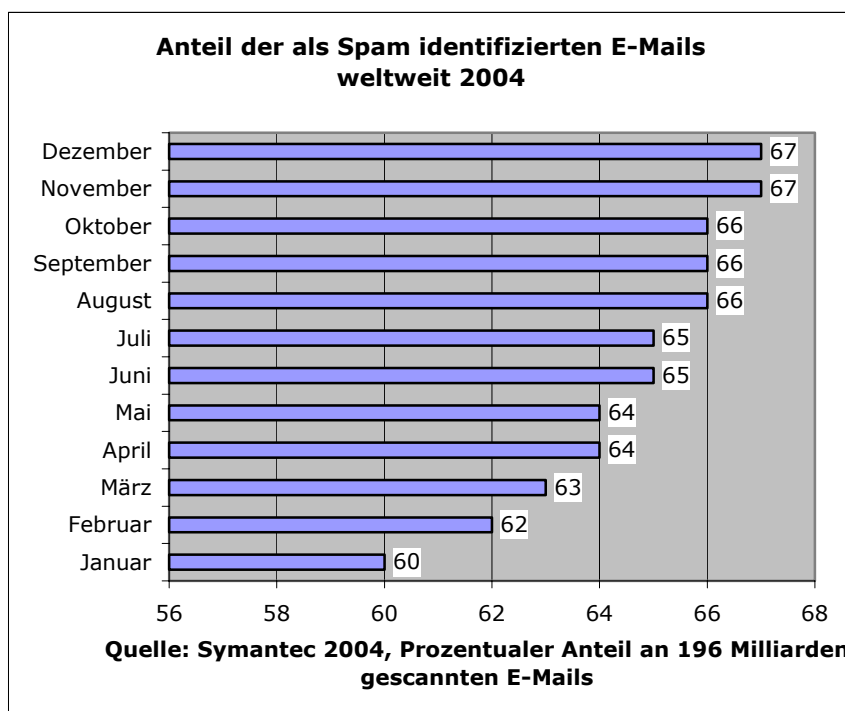
ßen den Nutzer wissen, was sie mit den Daten tun, 42,5 Prozent der Websites informierten darüber, *mit wem* sie die Daten gemeinsam nutzen würden. Die Frage, welche Handlungsmöglichkeiten der Nutzer in diesem System hat, beantworteten nur 17,5 Prozent der Seiten, noch seltener, bei 16 Prozent der untersuchten Websites, wurde der Nutzer darüber informiert, wie er seine Daten wieder löschen kann. 15 Prozent der Seiten versuchten zudem, Daten auf anderen Wegen als den vorbereiteten Formularen zu sammeln, meistens wie oben beschrieben mit Cookies.

Die Durchsetzung seiner Datenschutzrechte verlangt vom Verbraucher, eine außerordentlich komplexe Materie zu durchdringen. Er muss nicht nur seine Rechte, sondern auch die technischen Hintergründe kennen, um Datensammlern nicht hilflos ausgeliefert zu sein. Diese Situation führt zu Unsicherheiten beim Verbraucher. Wie das nächste Kapitel zeigt, macht sich dies besonders bemerkbar, wenn es um Spam und E-Commerce geht.

3.5 Spam: Die wachsende Gefahr

Unerwünschte Massenwerbung per E-Mail (Spam) ist längst ein ernsthaftes Problem. Während die Mails zunächst nur lästig waren, richten sie mittlerweile großen volkswirtschaftlichen Schaden an: Sie rauben dem E-Mail-Nutzer Zeit und Nerven, bringen oft gefährlichen Code mit und verleiten Nutzer zu undurchsichtigen Geschäften.

In den vergangenen drei Jahren hat das Problem überdurchschnittlich zugenommen. Nach Statistiken des Antiviren-Herstellers Trend Micro waren Mitte 2004 über die Hälfte aller Mails



Werbemüll (Trend Micro Virenreport 2004). Die Sicherheitsspezialisten Symantec (siehe Graphik) und Messagelabs stellen den gleichen Trend fest: Im Jahr 2004 wurden vom Messagelabs Sicherheitsservice mehr als 12,6 Milliarden E-Mails gesamtet. Von diesen wurden

mehr als 9,2 Milliarden, das heißt 73,2 Prozent als Spam identifiziert. Damit fressen die unerwünschten Mails Zeit, Netzwerkbandbreiten und Systemressourcen - auch bei Verbrauchern. (Symantec/Hörzu 2004).

Provider ignorieren Beschwerden

Spam-Blocking lässt sich am besten bei Access-Anbietern und Providern einsetzen, die damit verhindern könnten, dass die Mails überhaupt zum Verbraucher gelangen und weitere Bandbreiten benutzen. Doch Provider scheinen sich kaum für das Problem zu interessieren. Ein Test der Zeitschrift IX vom Heise-Verlag brachte eine traurige Bilanz: Von 40 versendeten Beschwerden wegen Spam-Mails, die nachvollziehbar vom Server des Providers verschickt wurden, wurde über die Hälfte einfach ignoriert. Nur 20 Prozent der Angeschriebenen ergriffen Maßnahmen, davon die Hälfte Universitäten. Dies zeigt, dass der Kampf gegen Spam noch immer von einzelnen Enthusiasten geprägt ist, während sich kommerzielle Anbieter kaum um das Problem kümmern. Damit schädigen sie ihre Kunden: Landet der Server auf einer der weltweiten Blacklists für Spamversender, werden alle Mails von dieser Domain als Spam gekennzeichnet - also auch die normalen E-Mails der dort registrierten Kunden.

Was viele Verbraucher nicht wissen: Auch der Heimrechner kann zur Spamschleuder werden, wenn er mit einem Virus infiziert ist, der eine heimliche Hintertür offenlässt. Durch diese kann sich der Spam-Versender Zutritt verschaffen und die Maschine missbrauchen. Da viele Nutzer heute schon DSL-Flatrates haben und ihre Computer - meist ohne den Schutz einer Firewall - non-stop online sind, haben die Betrüger leichtes Spiel.

Spam schadet dem E-Commerce

Spamming hat negative Folgen für den E-Commerce. Mehr als die Hälfte der Verbraucher kauft weniger im Netz ein, weil sie fürchten, ihre Adresse könnte auf die Listen der Spammer gelangen. Dies ergab eine Umfrage der im Trans Atlantic Consumer Dialogue (TACD) zusammengeschlossenen Verbraucherorganisationen Ende 2003 unter 21.000 Webnutzern weltweit.

Dabei fühlen sich 96 Prozent der Befragten von Spam belästigt. 84 Prozent wünschen sich, dass alle unverlangten Werbemails verboten werden und 82 Prozent verlangen von ihrer Regierung eine Opt-In-Regelung, nach der Werbemails nur versandt werden dürfen, wenn der Nutzer sie ausdrücklich angefordert hat. Hier unterscheiden sich US-amerikanische und EU-Bürger nicht in ihren Einstellungen. Die meisten Befragten gaben an, dass 40 oder mehr Prozent ihrer Post aus Werbemüll besteht. Die meisten User halten die Mails für irreführend oder betrügerisch - Spam verunsichert die ohnehin auf Sicherheit bedachten Verbraucher also noch mehr. Zudem schadet das Aussortieren der Mails zunehmend der Produktivität: 65 Prozent der Befragten gaben an, dass Spam sie selbst oder ihre Mitarbeiter Zeit und Geld kostet.

Spam verunsichert - und verführt

Ebenfalls fehlt es offensichtlich an Aufklärung unter den Nutzern: Während überall von einer „Vertrauenskrise des E-Commerce“ wegen Spam gesprochen wird (vgl. golem.de, 10.12.2004), kauft trotzdem jeder Dritte von Spam-Mail angebotene Software (29 Prozent). Auch Kleidung und Schmuck sowie Reisen oder Unterhaltungsangebote werden laut einer Umfrage des weltweit agierenden Marktforschungsunternehmens Forrester im Auftrag des weltweiten Interessenverbandes für den Schutz und den legalen Einsatz von Software *Business Software Alliance* (BSA) gerne gekauft. Allerdings mit mulmigem Gefühl: 51 Prozent der Nutzer geben an, dass Spam ihre Sorge über die allgemeine Online-Sicherheit verstärkt habe und 47 Prozent hat Angst vor Datenklau.

3.6 Malware: Viren, Trojaner und Co.

Sogenannte „Malware“, also Viren, Trojaner und Bot-Programme, stellen für Unternehmen und Verbraucher eine große Gefahr da. Ein infizierter Computer kann zu Datenverlusten führen, seine Reparatur kostet Zeit und Geld. Heutzutage sammeln Viren Daten, öffnen Türen für Spam-Versender und missbrauchen den Verbraucherrechner, ohne, dass er es merkt.

Ungebetene Gäste

Viele Nutzer fürchten noch immer die Legende vom „Format C“-Virus, also ein Schadprogramm, das die Festplatte des Nutzers löscht, ohne dass er etwas dagegen unternehmen könnte. Dies ist allerdings kaum der Fall, die meisten Viren haben ganz andere Ziele, als den Computer des Rechners unbrauchbar zu machen - sie wollen ihn für ihre Zwecke nutzen. Dazu bringen Viren ihre eigenen SMTP-Engines („Send Message Transfer Protocol“ zum Versand von Mails) mit, so dass sie einen befallenen Rechner ohne Kenntnis des Nutzers für ihre Zwecke missbrauchen können. So wird der stolze Besitzer eines PCs mit DSL-Flatrate plötzlich ungewollt zum Ausgangspunkt von Spam-Mails oder DDoS-Attacken (Distributed Denial-of-Service). DDoS ist eine Technik, um aus politischen oder kommerziellen Gründen andere Computer systematisch lahmzulegen, so geschehen mit der Websites der *New York Times* im Oktober 2001.

Das Problem: Fehler in Programmen

Die Verbraucher sind mittlerweile durch Medien und aufsehenerregende Fälle wie den ILOVEYOU-Virus über die Viren-Gefahr informiert. 90 Prozent der Nutzer wissen zum Beispiel, dass ihr Rechner ferngesteuert werden kann. Dennoch ist jeder Vierte PC-Nutzer ohne Virenschutzprogramm im Internet unterwegs, nur die Hälfte der Nutzer hat eine Firewall, so eine repräsentative Studie des BSI im Januar 2005. Dies ist kaum verwunderlich, denn während der Autofahrer nur Inspektions-Rhythmen einhalten und Türen abschließen muss, soll der PC-Nutzer seine Virensoftware stets - also täglich - auf dem neuesten Stand halten, alle neuen Patches für sein Betriebssystem sofort installieren, aktuelle Spam-Filter verwenden und Angriffe mit einer mehrstufigen Lösung aus Firewall und Antivirus abwehren.

Das Problem sind zudem oft Programme, die der Nutzer vorher für teures Geld erworben hat, denn sie enthalten vergessene Hintertüren oder schlicht Fehler, die Hacker ausnutzen können, sogenannte Exploits. McAfee berichtet 2004 von über zwei Millionen verschiedener Exploits auf Rechnern, die von dem Virus-Scan Online der Firma untersucht wurden. Hacker sind sehr daran interessiert, solche Sicherheitslücken zu nutzen, um Systeme von Endanwendern für ihre Zwecke zu nutzen.

Viren als Einfallstor

Hacker kombinieren zunehmend Viren mit Hintertüren, mit denen sie Informationen des Nutzerrechners sammeln oder diesen für ihre Zwecke benutzen. Sie heißen Bot-Programme (von Robot), Spyware, Adware oder Trojaner. Bot-Programme ermöglichen es Hackern, unbemerkt den PC des Nutzers zu kontrollieren, sobald er online ist. Auf diese Weise bauen sie Netzwerke solcher gekapert Computer auf, von denen DDoS-Attacken oder auch Spam-Versendungen gestartet werden. Der Anti-Viren-Hersteller Trend Micro registrierte 2004 insgesamt 2.830 solcher Bot-Programme, 35 Prozent mehr als im Jahr zuvor. Forscher bei McAfee schätzen, dass es mittlerweile über 7.000 verschiedene Bots gibt. Sie sehen einen Trend, dass Bots wiederum Adware auf den Rechner des Nutzers laden, also kleine Programme, die Werbung anzeigen und die Banner bei jeder Internetverbindung neu laden. Oft ist an solche Programme zusätzlich Spyware gekoppelt. Diese Software sammelt Daten über das Nutzerverhalten und gibt sie an eine vorher einprogrammierte Adresse unbemerkt weiter.

Mit den gewonnenen Daten erhoffen sich Marketing-Firmen, die Nutzer gezielter bewerben zu können. Allerdings geschieht all dies ohne Zustimmung des Verbrauchers, der davon oft nicht einmal etwas weiß. „Im Schnitt können auf jedem Rechner wenigstens 13 Adware-Komponenten gefunden werden“, heißt es im Bedrohungsreport von McAfee AVERT für 2004 (McAfee 2005). Die schon länger bekannten Trojanischen Pferde werden mit einem harmlos aussehenden Programm gemeinsam in den Rechner eingeschleust oder kommen als Komponente eines Virus. Sie sammeln ebenfalls Nutzerdaten und spionieren Passwörter aus.

3.7 Sicherheitstechniken

Auf dem Markt ist eine Fülle von Sicherheitstechniken, die Verbraucher, ihre Daten, Computer und e-Mails schützen sollen. Allerdings ist Auswahl, Installation und Wartung etwas für Experten und für den Normalnutzer kaum zu bewältigen.

Die Software-Industrie hat eine ganze Reihe von Programmen entwickelt, mit denen auch Heim-Anwender ihre PCs schützen können:

- *Firewalls* schützen vor fremdem Zugriff auf den Rechner
- *Kryptographie-Programme* verschlüsseln geheime Daten
- *Signaturen* lassen die eigene und fremde Identitäten im Internet verifizieren
- *Antivirus-Programme* filtern Viren aus dem Mailaufkommen und finden Trojaner
- *Spam-Filter* reinigen den Posteingang von unerwünschter Werbung

Doch selbst wenn der Verbraucher diese Techniken kennt, sind sie für den Normaluser meistens kaum komfortabel einsetzbar. Dies zeigt sich daran, dass Nutzer immer wieder glauben, ihre Computer seien mit einem Anti-Viren-Programm ausreichend geschützt. Patrick Heinen, IT-Sicherheitsexperte von Symantec hat die Erfahrung gemacht: „Gegen aktuelle Bedrohungen, wie beispielsweise den Computerwurm „MyDoom“, hilft nur die Kombination aus einer Firewall und einem Virenschutzprogramm.“ Nur jeder Dritte aber hat nach einer Studie von Symantec mehr als eine Art von Sicherheitssoftware installiert.

Überforderung - nicht nur zu Hause

Der Verbraucher ist mit den Bedrohungen überfordert, kann die Zeit nicht aufwenden oder versteht die Technik nicht. Im Januar 2004 meldete das Bundesamt für Sicherheit in der Informationstechnik (BSI), jeder Vierte bewege sich ohne Virenschutzprogramm im Internet und nur die Hälfte der Internetnutzer setze eine Firewall ein. Dies seien zwar erschreckende Erkenntnisse, aber das BSI erklärt zusätzlich: „Doch allein das Einschalten der entsprechenden Schutzmassnahmen reicht nicht aus, um sicher im Internet zu surfen. Wichtig ist das regelmäßige Schließen von Sicherheitslücken in den genutzten Programmen, das so genannte Patchen.“ Für das Patchen von Firmenrechnern gibt es mittlerweile Outsourcing-Lösungen, weil die fest angestellten System-Administratoren nicht mehr hinterherkommen. Vom Privatanutzer wird jedoch erwartet, dass er seine Virensignaturen monatlich, besser wöchentlich aktualisiert, seine Firewall auf dem neuesten Stand hält und regelmäßig nachschaut, ob Microsoft für das Betriebssystem Windows ein neues Sicherheitsupdate herausgebracht hat, das bei der Installation unter Umständen den ganzen Rechner zum Abstürzen bringt.

Durchschnittsnutzer hilflos

Das BSI resümiert schon 1999 in seiner Studie zu E-Commerce: „Eine Vielzahl von Gefährdungen bedrohen ein Electronic-Commerce-System. Einige davon sind augenfällig, andere in der konkreten Implementation verborgen, einige sind nur Experten überhaupt verständlich.“ (BSI 1999, S. 20). Der Nutzer ist aber selten ein Experte, sondern Verbraucher, er will die System nur benutzen und nicht täglich warten, verstehen und sich auf dem Laufenden halten müssen. Er ist damit einer Industrie ausgeliefert, die ihn in falscher Sicherheit wiegt, indem sie ihm eine Firewall verkauft, die er falsch einstellt und dann nie wieder updated. Oder er lässt es ganz und hat damit quasi eine offen stehende Wohnungstür zu allen seinen elektronischen Daten.

Ein Teil des Problems ist die Monopolstellung von Microsoft: Die "Monokultur Windows" stellt ein massives Sicherheitsproblem dar, das mit Linux oder MacOS nicht besteht, da die meisten Viren Sicherheitslücken des Marktführers ausnutzen. Viele Nutzer wissen allerdings gar nicht, dass es Alternativen gibt - hier fehlt es an Aufklärung und Information.

3.8 Sichere Identifikation in offenen Netzen

Bei Geschäften im Internet fehlt das, was man heutzutage an vielen EC-Karten-Terminals leisten muss: Die eigenhändige Unterschrift. Für Vertragspartner in Online-Geschäften ist es schwierig, das oder den Gegenüber eindeutig zu identifizieren, wenn nur Webseiteninformationen und E-Mails ausgetauscht werden. Wird für einen Geschäftsabschluss via Internet eine rechtsverbindliche Unterschrift zwingend, muss der Verbraucher daher bisher meist einen Vertragstext von der Webseite des Anbieters (zum Beispiel eine Bank) herunterladen, ausdrucken, unterschreiben und per Post an den Vertragspartner schicken.

Signieren per Computer

Mit dem „Signaturgesetz“ und der „Signatur-Verordnung“ hatte der Gesetzgeber schon vor ein paar Jahren die gesetzlichen Grundlagen dafür geschaffen, dass diejenigen, die im Internet Online-Geschäfte abwickeln wollen, für die nach BGB eine Unterschrift erforderlich ist, Verträge auch digital „unterschreiben“, präziser „signieren“ können. Hierzu erhält der Signaturnutzer von einer Ausgabestelle (sogenanntes Trust-Center) eine Chipkarte (Signaturkarte) und ein Zertifikat. Auf der Signaturkarte sind zwei Schlüssel gespeichert: der geheime und der öffentliche Schlüssel. Mit dem geheimen Schlüssel wird eine verschlüsselte Kurzfassung (sogenannter Hashwert) des zu signierenden Vertragstextes und die persönliche „qualifizierte elektronische Signatur“ generiert. Hashwert, Signatur, öffentlicher Schlüssel und das zugehörige Zertifikat werden dann dem Adressaten zusammen mit dem Vertragstext übermittelt. Dieser kann mit Hilfe des Hashwertes die Unversehrtheit des übermittelten Vertrages, mit dem Zertifikat zum öffentlichen Schlüssel durch Nachfrage beim Trust-Center die Identität des Absenders eindeutig klären. Den Signaturschlüssel musste der Signaturanwender bis vor kurzem noch schriftlich beantragen und sich gegenüber der die Schlüsselkarte ausgebenden Registrierungsstelle (Trust-Center) persönlich ausweisen. In Deutschland haben unter anderem die Telekom und die DATEV Trust-Center gegründet.

Zu teuer, zu kompliziert – und nun zu unsicher?

Mit der qualifizierten elektronischen Signatur können also Geschäfte im Internet rechtsverbindlich werden. Darüber hinaus bietet sie den Kommunikations- oder Vertragspartnern die Möglichkeit, die Identität des anderen zweifelsfrei zu überprüfen. Soweit die Theorie. In der Praxis gab es in den vergangenen Jahren immer wieder Kritik aus der Wirtschaft an den angeblich zu hohen Kosten und der Kompliziertheit des deutschen Verfahrens. Die qualifizierte elektronische Signatur hat infolgedessen in Deutschland bis heute keine Marktbedeutung bei Online-Verbrauchergeschäften.

Auf Druck der Bankenverbände hat daher der Gesetzgeber vor kurzem das Antragsverfahren im Signaturgesetz vereinfacht - entgegen erheblicher Bedenken des Verbraucherzentrale Bundesverbands und der Bundesnotarkammer. Seit November 2004 muss der Antragsteller nicht mehr wie bisher bei der Beantragung der Signaturkarte eine eigenhändige Unterschrift leisten. Er könnte vielmehr eine künftig von seiner Bank per Post erhaltene kombinierte Bank-Signaturkarte auf elektronischem Wege freischalten lassen. Dadurch kann aber die Bank nicht mehr kontrollieren, ob ein bestimmter Antrag rechtmäßig gestellt wurde - wird die Karte missbraucht, trägt der Inhaber dennoch alle rechtlichen Konsequenzen.

Insofern wird ein im Grundsatz sicheres Instrument einem erheblichen Missbrauchsrisiko ausgesetzt.

Starke Beweiskraft eines unsicheren Systems

Die qualifizierte elektronische Signatur ist über den Paragraphen § 126a des BGB eng mit dem Zivilrecht verkoppelt. Nach dieser Vorschrift kann die „gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden“. Hierdurch erlangt die qualifizierte elektronische Signatur eine starke rechtliche Beweiswirkung, die zu einem Zeitpunkt in das BGB aufgenommen wurde, als das gesetzlich vorgegebene Signaturverfahren noch als hoch sicher galt. Spätestens seit Wegfall der Schriftlichkeit im Signaturgesetz ist aber die eindeutige Zuordnung einer Signatur zum rechtmäßigen Inhaber nicht mehr ausreichend gewährleistet. Daher verliert nach Auffassung des vzbv auch aber der starke Anscheinsbeweis im § 126 a BGB seine Grundlage. Reagiert der Gesetzgeber im BGB nicht auf diese aktuelle Verfahrensänderung im Signaturgesetz, hat wegen der beim Karteninhaber verbleibenden Beweislast der Verbraucher im Streitfall vor Gericht nur eine geringe Chance zu beweisen, dass eine angeblich "sichere" Technik missbraucht worden ist.

3.9 Folgen

Der Wirtschaftsfaktor Vertrauen gerät unter Druck

Der Effekt der oben beschriebenen Situation ist eine Vertrauenskrise beim Verbraucher. Viele Studien finden Zusammenhänge zwischen schlechtem Datenschutz, unrechtmäßigem Händlergebaren und einem Vertrauensschwund beim Verbraucher. Nutzer brechen Transaktionen ab, wenn sie zu kompliziert oder zu gefährlich erscheinen, kaufen erst gar nicht online ein oder bewegen sich wissentlich auf gefährlichem Boden. Wenn der E-Commerce weiter wachsen soll, steht das Vertrauen des Verbrauchers an erster Stelle. Händler müssen ihre Websites an den Kunden orientieren, die Vertragsbedingungen müssen auch europaweit und grenzüberschreitend fair sein, der Kunde muss informiert und geschützt werden.

Im Weihnachtsgeschäft 2004 machte eine Studie von Forrester-Research Furore, die zeigte, dass jeder Zweite wegen Spam Bedenken wegen Datensicherheit hat: „Spam schadet dem Online-Marktplatz, indem er das Verbrauchervertrauen in diese neue Form des Handels schwächt“, erklärte Georg Herrleben, Regionalmanager der Business Software Alliance für Zentraleuropa. „Das Internet als solches droht seine dynamisierende Wirkung für die Wirtschaft zu verlieren, wenn Verbraucher sich aus berechtigter Sorge vor kriminellen Machenschaften zurückziehen.“

Wirtschaftliche Folgen

Das Internet könnte große Rationalisierungseffekte haben, wenn die Verbraucher es stärker nutzen würden.

Die EU-Kommission hat sich im September 2003 über die Effekte Gedanken gemacht, die eine Ausweitung des Online-Banking auf die mehr als 207 Millionen bargeldlosen Zahlungen haben könnte, die 2001 täglich in der EU getätigt wurden. „Ein erheblicher Anteil dieser Zahlungen erfolgte elektronisch. Könnte dieser Anteil weiter erhöht werden, so würde die Wirtschaft effizienter. Allerdings (...) muss dazu das Vertrauen der Verbraucher gestärkt werden.“ Die EU geht davon aus, dass E-Commerce zusätzlich ein „massives Potenzial hat, die europäische Wirtschaft anzukurbeln“, dabei spiele vor allem „maximale Sicherheit“ eine Rolle (EU 2003). Auch in Deutschland wollen Händler stärker ins Internet investieren. Bisher sind vor allem die großen Marken vertreten, aber auch der Mittelstand zieht langsam nach. Dies wird nur Erfolg haben, wenn die Verbraucher ihre Angst vor neuen und kleinen Shops verlieren, weil sie gute Erfahrungen gemacht haben.

Ausblick

Die aktuelle Situation lässt sich an vielen Stellen verbessern: EU-weit müssen bessere Möglichkeiten geschaffen werden, um Verbraucherrechte durchzusetzen. Unabhängig überwachte Gütesiegel könnten hier ein Stück weit Sicherheit geben. Allerdings stellt die Studie des EVZ 2003 fest, dass es mittlerweile eine so große Anzahl von Siegeln und Zeichen gibt, dass „Außenstehende kaum noch durchblicken“ (EVZ 2003, S. 25).

Zu begrüßen ist, dass sich verschiedene deutsche Gütesiegelanbieter zusammengeschlossen und für die Siegelvergabe und Überwachung gemeinsame Kriterien geschaffen haben. Bestehende nationale Gesetze müssen den Verbraucherbedürfnissen angepasst, ihre Durchsetzung in der Praxis verbessert werden. Sowohl Anbieter als auch Konsumenten müssen offensichtlich besser über ihre Rechte und Pflichten informiert werden. Bei beiden Seiten zeigt sich ein Mangel an Wissen über das, was sie dürfen, können und müssen.

afgis – Initiative für mehr Transparenz im Internet

Das Aktionsforum Gesundheitsinformationssystem (afgis) e.V. ist ein Zusammenschluss von Verbänden, Unternehmen und Einzelpersonen zur Förderung der Qualität und Transparenz von Gesundheitsinformationen im Internet. Zu den Mitgliedern gehört auch der Verbraucherzentrale Bundesverband. Mit dem afgis-Qualitätslogo antwortet der Verein auf die steigenden Qualitäts- und Sicherheitsbedürfnisse der Nutzer von Gesundheitsinformationen. Das Verfahren zur Vergabe dieses afgis-Qualitätslogos wurde 2004 inhaltlich präzisiert und organisatorisch und technisch neu geordnet. Websites, die das afgis-Logo tragen, dokumentieren auf für Nutzer leicht nachvollziehbare Weise, dass sie sich einer Prüfung unterzogen haben. Dabei geht es um Transparenz in folgenden Bereichen:

- Anbieter (Wer steht hinter eine Webseite?)
- Ziel, Zweck und angesprochene Zielgruppe(n) der Information
- Autoren und die Datenquellen der Informationen
- Aktualität der Daten
- Möglichkeit für Rückmeldungen seitens der Nutzer
- Verfahren der Qualitätssicherung
- Trennung von Werbung und redaktionellem Beitrag
- Finanzierung und Sponsoren
- Kooperationen und Vernetzung
- Datenverwendung und Datenschutz



Der Trend weg von sicheren hin zu einfachen Systemen muss aufgehalten werden: Sicherheitsprodukte müssen zuverlässig und gleichzeitig so gestaltet sein, dass der Verbraucher sein Kryptographie-System so selbstverständlich nutzen kann wie den Sicherheitsgurt im

Auto. Es muss außerdem alternative Lösungen für Verbraucher geben, die das Internet nicht nutzen wollen oder können - ein *digital divide*, eine digitale Spaltung der Gesellschaft darf nicht dazu führen, dass einzelne Bürger von günstigen Angeboten oder von einzelnen Dienstleistungen insgesamt ausgeschlossen bleiben.

Staatliches Eingreifen kann auch beim besonders ungreifbar scheinenden Spam-Problem etwas bewirken: An den Statistiken des Mail-Filters Messagelabs lässt sich ablesen, dass rechtliches Einschreiten von Seiten der Regierungen jedes Mal auch das Aufkommen von Spam-Mails für eine gewisse Zeit reduzieren konnte.

Um für die Verbraucher mehr Sicherheit und mehr Vertrauen im Internet zu erreichen müssen, geht es nicht in erster Linie um neue Institutionen und neue Vorschriften. Trotz teilweise gravierender rechtlicher Lücken – etwa bei Haftungsfragen in Zusammenhang mit dem bargeldlosen Zahlungsverkehr oder bei der digitalen Signatur – ist die fehlende Rechtssicherheit nicht das Kernproblem. Zentrales Problem ist vielmehr, dass bestehende sinnvolle Schutzrechte der Verbraucher in der digitalen Welt kaum durchgesetzt werden. Ein Ausweg aus der Vertrauenskrise muss also über eine wirksamere Durchsetzung geltender Verbraucherrechte führen.

VERWENDETE LITERATUR**Arbeitsgemeinschaft der Verbraucherverbände e.V. (AgV)**

- 1999 Banken und Internet - das Online-Angebot von Banken aus der Perspektive des Verbraucherschutzes, Stefanie Jack, Rotraud Gitter, Hamburg, aktualisierte Fassung Mai 1999

Bundeskriminalamt, www.bka.de

- 2003 Betrug-5100- PKS Berichtsjahr 2003, 190
2003 Computerkriminalität-8970- PKS Berichtsjahr 2003, 240

Bundesamt für Sicherheit in der Informationstechnik BSI, www.bsi.de

- 1999 Sicherheitsaspekte beim Electronic Commerce, Schriftenreihe des BSI, Band 10, Juli 1999
2001 Das Ende der Anonymität? Datenspuren in modernen Netzen, Harald Kelter, Ingelheim 2001
2005 Bürger zu sorglos im Internet, Studie BSI/TNS Emnid, PM vom 27.01. 2005

Bundesverband deutscher Banken/ipos, www.bdb.de

- 2003 Warum Offliner Offliner sind – Zugangsbarrieren bei der Online-Nutzung, Online-Monitor III, Umfrage von ipos im Auftrag des Bundesverbandes deutscher Banken, November 2003

Business Software Alliance (BSA), www.bsa.org/Forrester Data, www.forrester.com

- 2004 Verbraucher-Einstellung zu Spam in Deutschland, www.bsa.org

Consumers International (ConsInt), www.consumersinternational.org

- 2001 Privacy@Net, An international comparative study of consumer privacy on the internet, Kate Scribbins, Jan 2001
2001a Should I buy? Shopping online 2001, An international comparative study of electronic commerce, Kate Scribbins, Sep 2001
2002 Credibility on the web, An international comparative study of credibility of consumer information on the internet, Kate Scribbins, Nov 2002

EU-Kommission

- 2003 Konferenz und Studie der Kommission geben Aufschluss über Sicherheit und öffentliche Wahrnehmung des öffentlichen Zahlungsverkehrs, Brüssel, 2003, IP/03/1265 2003
2003a Study on the Security of Payment Products and Systems in the 15 Member States, Final Report, Tony Hegarty, Luxembourg 2003

Europäisches Verbraucher Zentrum Düsseldorf (EVZ), www.evz.de

- 2003 Europa- grenzenloses Einkaufsparadies? Online-Shopping auf dem Prüfstand, EVZ Düsseldorf (Hrsg), Düsseldorf 2003

Gesellschaft für Konsumforschung (GfK), www.gfk.de

- 2004 Online Shopping Survey (OSS) mit tns infratest, enigma GfK

Institut für Strategie-Entwicklung/Universität Witten/Herdecke

- 2004 Digitale Mentalität, Witten 2004

IX Magazin für professionelle Informationstechnik. www.heise.de/ix/

2005 Viele Provider ignorieren Spam-Hinweise, iX-Ausgabe 02/2005

McAfee® Avert, www.mcafee.com

2005 McAfee® Avert gibt Top 10 der Bedrohungen 2004 bekannt - Ausblick auf kommende Trends, PM 12.01. 2005

2005a Vorsicht vor Sicherheitstücken beim Online-Einkauf, PM Januar 2005

2005b Internet Security und die zukünftigen Bedrohungen, Vincent Gullotto, 15.12.2004

NDR-Media/ARD

2000 Vorsicht, ihr Konto wird beklaut, Bernd Leptihn, NDR-Redaktion ARD-Ratgeber Technik (Hrsg), Königswinter 2000

Postbank/Europressedienst, www.postbank.de

2004 E-Commerce 2004, Strukturen und Potenziale des E-Comemrce in Deutschland aus Kunden und Händlersicht, Nov 2004

Stern

2005 Extra: Kopieren - was ist noch erlaubt?
http://www.stern.de/computer-technik/technik/index.html?eid=513240&id=513505&nv=ex_rt

Symantec/Hörzu, www.symantec.de

2004 Mensch ärgere dich nicht - Was Deutsche am Computer am meisten nervt, April 2004

Trans Atlantic Consumer Dialogue (TACD)

2004 Consumer Attitudes Regarding Unsolicited Commercial Email (Spam) October – December 2003

TREND MICRO

2004 Viren-Report für 2004: Mehr als 3 Millionen Infektionen pro Monat

Telepolis

2004 Der Markt wird es schon regeln, Justizministerin Zypries stellt Entwurf der neuen Urheberrechtsnovelle vor, Volker Grassmuck 11.09.2004

Verbraucherzentrale Bundesverband (vzbv), www.vzbv.de

2002 Verbraucherinformationen im Internet: Mehrzahl der Websites aus Verbrauchersicht untauglich, 04.11.2002

2002 Einkaufen im Netz, 18.12.2002

2003 Gutachten zu Kundenbindungssystemen und Datenschutz, 02.12.2003

2003 Fernabsatz von Versicherungen im Internet, 06.02.2003

2004 Spamming behindert E-Commerce, 09.02. 2004

2004 Beitrag zum Symposium des Bundesministeriums der Justiz und des Institutes für Urheber- und Medienrecht, Patrick v. Braunmühl