

18.August 2008

## Hintergrundpapier

# Datenhandel Inside – Ein Blick hinter die Kulissen

### Allgemeines

- Interesse an der Ausspähung und Verarbeitung personenbezogener Daten hat neben dem Staat heute vor allem die Wirtschaft. In den Marketingabteilungen haben entsprechende Informationen einen hohen wirtschaftlichen Stellenwert.
- Die Digitalisierung macht es leicht, Daten nicht nur zu sammeln, sondern auch miteinander zu verknüpfen und daraus individuelle Profile zu erstellen.
- Am häufigsten greifen Unternehmen aus den Branchen Handel, Finanzdienstleistungen, Telekommunikation und Versicherungen auf solche Profile zurück (vgl. Thomas Wischniewski, Sicherheit im Internet – Datenschutz- und Datensicherheitsrisiken erkennen und minimieren).
- Der niedersächsische Datenschutzbeauftragte ging 2004 davon aus, dass jeder Bundesbürger über 18 Jahre durchschnittlich in 52 kommerziellen Datenbanken erfasst ist (vgl. ebd.).
- Nach Auskunft des Chaos Computer Clubs (CCC) sind in Deutschland 1.300 Adresshändler registriert, bei denen Unternehmen Adressen und weitere personenbezogene Daten von potenziellen Kunden kaufen können. Alleine der Branchenprimus, die Schober Direktmarketing GmbH, verfügte 2004 über 60 Millionen Adressen mit einer Milliarde Daten (vgl. ebd.).
- Pro Datensatz werden Umsätze zwischen unter 50 Cent und bis zu zwei Euro erzielt (vgl. ebd.).

### Wer handelt mit Daten?

- **Adresshändler** sammeln Daten und bieten diese den Unternehmen an. Bekannt sind Firmen, die Fragebögen mit über 120 Fragen bundesweit an Verbraucher geschickt haben. Die Fragen betreffen das gesamte tägliche Konsumverhalten von Hygieneartikeln bis hin zu Geldanlagen und Versicherungen. Um den Angeschriebenen die Weitergabe ihrer Gewohnheiten schmackhaft zu machen, werden kleine Preise ausgelobt. Ebenso soll das Argument der gezielten Produktinformation überzeugen. Diese Datensätze dürfen jedoch keine Kontodaten enthalten.

- **Firmen**, die im Telemarketing arbeiten, kaufen solche Datensätze auf. Um Streuverluste zu vermeiden, stellen sie konsumspezifische Bedingungen an die Daten.
- **Callcenter** erhalten die Daten von den Firmen oder sie haben eigene Datensätze, deren Nutzung sie sich von den Telemarketingfirmen bezahlen lassen. Anhand dieser Datensätze werden Verbraucher angerufen und zu Geschäftsabschlüssen bewegt.

### Woher stammen die Daten?

- Verbraucherbefragungen anhand von Fragebögen
- Registrierung bei Preisausschreiben
- Kunden- oder Rabattkartensysteme
- Online-Webformulare, die vor Nutzung eines Dienstes ausgefüllt werden müssen
- Computerprogramme wie Cookies, Web-Bugs, Skripte oder Spyware (zum Beispiel Trojaner, siehe unten)
- Datendiebstahl in Unternehmen

### Problembewusstsein? Fehlanzeige

- In einer britischen Studie über E-Mail-Marketing vom Juni 2008 berichten **61 Prozent** der befragten Firmen über Datendiebstahl. Davon gaben wiederum **77 Prozent** an, sie hätten das E-Mail-Marketing an Drittfirmen übertragen. **53 Prozent** der befragten Vermarkter waren nicht sicher, ob ihre Marketingprogramme gegen Datenschutzrechte verstoßen. Und nur **55 Prozent** hielten es für sehr wichtig oder wichtig, dass die Kunden ihren Angaben zum Datenschutz trauen können. (vgl. Ponemon Institute LCC: 2008 UK Study on Email Marketing Practices and Privacy).
- Die Beratungsfirma Deloitte hat 2007 in einer internationalen Analyse Firmen aus den Bereichen Technologie, Telekommunikation und Medien zu Datenmanagement befragt. Demnach glauben lediglich **38 Prozent** der befragten Unternehmen von sich, genug für die Datensicherheit zu tun. Und nur **54 Prozent** der Befragten gaben an, über eine ausgearbeitete Sicherheitsstrategie zu verfügen. **42 Prozent** der Unternehmen hat seine Mitarbeiter in den vorherigen 12 Monaten nicht zu Datensicherheit und Datenschutzmaßnahmen geschult. (vgl. Deloitte: Treading Water. The 2007 Technology, Media & Telecommunications Security Survey)

### Beispiel Trojaner-Angriff

Trojaner sind Programme, mit denen vertrauliche Daten (zum Beispiel Kontoverbindungen) ausgespäht, verändert, gelöscht oder bei der nächsten Datenübertragung an Dritte verschickt werden. Wie einfach und lukrativ sich damit Geld verdienen lässt, zeigt folgendes Beispiel (aus: Panda Security 2008. Neue Bedrohungen, neue Lösungen):

- Ein Trojaner mit der Fähigkeit den Zahlungsverkehr auf dem Computer auszuspionieren kostet heute rund 350 Euro. Eine Empfängerliste mit einer Millionen E-Mail-Adressen, um den Trojaner zu verbreiten, kostet in Deutschland derzeit rund 70 Euro. Ein Programm zur Prüfung des Trojaners gegen alle bekannten Antivirus-Programme kostet rund 15 Euro. Ein E-Mail-Server für die Aussendung des Trojaner-Angriffs kostet rund 350 Euro. Die **Gesamtinvestition des Betrügers** beläuft sich somit auf **785 Euro**.
- Bei 1.000.000 Empfängern ist von einer (niedrig kalkulierten) Infektionsrate von 10 Prozent auszugehen. Von diesen 100.000 infizierten Systemen enthalten wiederum 10 Prozent finanzrelevante Daten. Mit diesen Informationen lässt der Betrüger von jedem der 10.000 Konten jeweils 10 Euro abbuchen. Der **Umsatz des Betrügers** beträgt in diesem Fall **100.000 Euro**.
- Abzüglich der Investitionen bleibt ein **Netto-Gewinn von 99.215 Euro**. Ein profitables Geschäft!