

# Alles unter Kontrolle

## Mit Kontrolladressen Datenmissbrauch verhindern

**Beschleicht auch Sie ab und an die Angst, dass Ihr wertvollstes Kapital, Ihre Kundendaten in die Hände Dritter – vielleicht sogar Ihrer Wettbewerber – geraten? Denken Sie darüber nach, wie Sie die unbefugte Adressnutzung verhindern können? DIREKT MARKETING hat sich bei Dieter Süppmayer, Anbieter von Kontrolladresssystemen erkundigt, mit welchen Möglichkeiten dem Datenmissbrauch begegnet werden kann.**

In den letzten Jahren hat der Stellenwert von Adressen und Kundendaten enorm an Bedeutung gewonnen.

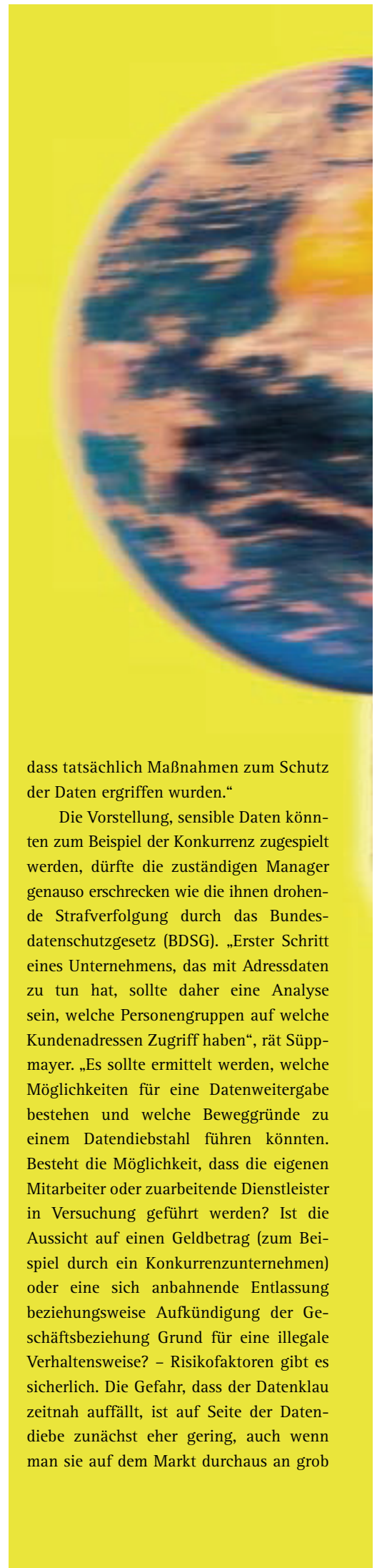
### Wirtschaftsfaktor Daten


Geschäftliche Entscheidungen und Marketingaktionen von Unternehmen, die sich an Endverbraucher richten, basieren zunehmend auf den aus den erhobenen Daten gewonnenen Informationen. Daten und Adressen gelten daher als nicht zu unterschätzende Wirtschaftsfaktoren und müssen auch im Interesse der jeweiligen Firmen geschützt und vertraulich behandelt werden. Dass dabei nicht nur der wirtschaftliche Faktor eine Rolle spielt, betont Dieter Süppmayer, Geschäftsführer AC Süppmayer GmbH: „Datenbestände umfassen personenbezogene Angaben, die

nach Bundesdatenschutzgesetz unter das Persönlichkeitsrecht fallen. Damit sind Unternehmen - neben ihrem eigenen wirtschaftlichen Interesse - auch per Gesetz verpflichtet, Daten zu schützen. Es drohen strafrechtliche Konsequenzen, wenn personenbezogene Daten vorsätzlich oder fahrlässig gegen die Datenschutzbestimmungen erhoben, verarbeitet, genutzt, an Dritte übermittelt, unberechtigt verändert oder gelöscht werden. An hohen Geldstrafen bis zu ca. 250.000 Euro oder einigen Jahren Freiheitsstrafe lässt sich erkennen, wie ernst es dem Gesetzgeber dabei ist und mit welcher Brisanz es um Adressen und Kundendaten zu tun hat. Und tritt tatsächlich einmal der Schadensfall ein, der meist mit Schadenersatzpflichten einhergeht, dann haben Unternehmen oft große Not, den Nachweis zu erbringen,

dass tatsächlich Maßnahmen zum Schutz der Daten ergriffen wurden.“

Die Vorstellung, sensible Daten könnten zum Beispiel der Konkurrenz zugespielt werden, dürfte die zuständigen Manager genauso erschrecken wie die ihnen drohende Strafverfolgung durch das Bundesdatenschutzgesetz (BDSG). „Erster Schritt eines Unternehmens, das mit Adressdaten zu tun hat, sollte daher eine Analyse sein, welche Personengruppen auf welche Kundenadressen Zugriff haben“, rät Süppmayer. „Es sollte ermittelt werden, welche Möglichkeiten für eine Datenweitergabe bestehen und welche Beweggründe zu einem Datendiebstahl führen könnten. Besteht die Möglichkeit, dass die eigenen Mitarbeiter oder zuarbeitende Dienstleister in Versuchung geführt werden? Ist die Aussicht auf einen Geldbetrag (zum Beispiel durch ein Konkurrenzunternehmen) oder eine sich anbahnende Entlassung beziehungsweise Aufkündigung der Geschäftsbeziehung Grund für eine illegale Verhaltensweise? – Risikofaktoren gibt es sicherlich. Die Gefahr, dass der Datenklau zeitnah auffällt, ist auf Seite der Datendiebe zunächst eher gering, auch wenn man sie auf dem Markt durchaus an grob





begangenen Fehlern ausmachen kann (wie zum Beispiel Kontaktmöglichkeit über eine Mobilfunknummer oder eine Internetseite). Aber selbst dann nutzen nicht gerade wenige Adresseinkäufer die Chance auf einen günstigen Erwerb der über solche Wege angebotenen Adressen. Zwar gibt es immer noch wachsame Unternehmen, die den Deutschen Direktmarketing Verband (DDV) oder die Kriminalpolizei informieren, wenn ihnen Adressdaten über zweifelhafte Wege angeboten werden, doch als umfassend wirkende Sicherungsinstanz kann dies natürlich nicht dienen.“

### Gefahren lauern überall

Wenn es um den Schutz von Daten geht, denkt mancher Geschäftsführer oft nur an beispielsweise große Versandhäuser und sieht die Gefahr fernab vom eigenen Betrieb. Ein Irrglaube, denn Adressdiebstahl kann jede Firma treffen – überall dort, wo Daten von Kunden, Lieferanten, Dienstleistern et cetera erfasst, verarbeitet und genutzt werden. Nicht zu unterschätzen sind untreue Mitarbeiter, die täglich mit den Datenbanken arbeiten. Dieter Süppmayer sind nicht wenige Fälle bekannt, bei denen Mitarbeiter diverser Firmen für schnelles Geld Verrat am eigenen Betrieb begangen haben und er erklärt: „Das Thema ‚Datenklau‘ wird oft unterschätzt – nicht, weil er so selten stattfindet, sondern weil er zu selten aufgedeckt und – noch

seltener – publik wird. Oft sind es nur Zufälle, die einen Missbrauch erkennen lassen. Aber selbst dann passiert erstaunlich wenig: Aus Angst vor negativen Folgen wie Imageverlust oder Verlust von Kundenvertrauen kehren geschädigte Unternehmen solche Vorfälle allzu gerne unter den Teppich. Strafanzeigen und Gerichtsprozesse wegen Adressmissbrauch gibt es daher relativ selten. Kein Unternehmen kann sich – gerade in den derzeit



**„Meiner Erfahrung nach geht der Mittelstand sensibler mit dem Thema um, denn hier wurde die Firma und die Adressdatenbank meist selbst beziehungsweise**

**von null aufgebaut. In großen Konzernen verliert dieser Gedanke aufgrund von komplexer Mitarbeiter- und Organisationsstruktur etwas an Bedeutung.“**

*Dieter Süppmayer, AC Süppmayer GmbH*

wirtschaftlich schwierigen Zeiten – einen solchen Skandal leisten. Die Unternehmen sind folglich mit ihrem Datenschutzproblem auf sich alleine gestellt.“

Dass nicht wenige Unternehmen sich in trügerischer Sicherheit wähnen, dass die Gefahr von Datenmissbrauch im eigenen Haus nicht bestünde, bestätigt eine Untersuchung von Arthur Andersen. Demnach warten 75 Prozent der befragten Verantwortlichen erst einmal ab, bis tatsächlich etwas geschehen ist – erst dann werden sie aktiv. Warum, fragt sich mancher Entscheidungsträger, soll man in etwas investieren, dessen Wirtschaftlichkeit man kaum in Zahlen fassen kann. Es ist also nicht verwunderlich, dass viele Entscheider nach der Vogel-Strauß-Politik verfahren und die Gefahren gar ignorieren oder herunterspielen.

### In falschen Händen

Dass Gefahrenquellen für Datenmissbrauch überall lauern, weiß Dieter Süppmayer aus eigener Erfahrung zu berichten. „Eine Kopie der Datenbank zu erstellen ist denkbar einfach. Immer bedienerfreundlichere

Software ermöglicht es leicht, Daten abzurufen, zu kopieren oder über das Internet zu übertragen.

Eine Studie der KPMG belegt, dass solche strafbaren Handlungen zu 45 Prozent von unternehmensinternen Personen begangen werden, gefolgt vom Miteinander zwischen unternehmensinternen und externen Personen (17 Prozent). Auffällig ist, dass 76 Prozent der betreffenden Manager und Entscheidungsträger im Vorfeld keinerlei Anzeichen für wirtschaftskriminelle Handlungen erkennen konnten. Wie schon dargelegt: Datenmissbrauch ist oftmals ein stilles kriminelles Vergehen.

Nicht zu verachten sind im heutigen IT-Zeitalter auch die Sicherheitslücken, die sich bei Datenübertragungen über das Internet auftun. Übermittlungen von Mail-Anhängen können auf ihrem Weg nicht selten von Dritten abgefangen werden. Und auch auf der Empfängerseite ist unklar, ob nur die adressierte Person alleine die Daten einsehen kann beziehungsweise ob noch andere Personen Zugriff auf den Empfänger-PC haben. Um die Unsicherheiten des Datenaustauschs zu vermeiden hilft entweder, diese Form der Datenübermittlung gar nicht erst zu benutzen oder der Einsatz eines Verschlüsselungsverfahrens (Kryptographie), bei dem der Empfänger die Daten erst mit Hilfe eines Passworts öffnen kann, das er vom Absender auf anderem Wege (zum Beispiel telefonisch) erhalten hat.“

## Geheimsache Kontrolladresse

Um Daten- und Adressbestände gegen Diebe aus der eigenen Firma oder zuarbeitenden Dienstleistern zu schützen, lohnt der Einsatz von Kontrolladressen. Insbesondere, wenn man firmenintern und innerhalb der Geschäftsbeziehungen mit Zuarbeitern bekannt gibt, dass sich Kontrolladressen im Datenbestand befinden und harte Strafen bei Vertragsverletzungen in den Verträgen vorsieht.

Es versteht sich von selbst, dass dabei auch die Kontrolladressen geschützt werden müssen, damit niemand deren Schutzfunktion aushebeln kann. Dieter Süppmayer erklärt, dass Kontrolladressen

# Die wichtigsten Aspekte beim Aufbau einer Kontrolladresse

**Kontrolladressen bestehen aus Abweichungen zur tatsächlichen Adresse. Um eine kurze Schilderung der Aspekte, die hier berücksichtigt werden sollten, bat DIREKT MARKETING**

**Dieter Süppmayer, AC Süppmayer GmbH.**

Um eine postalische Zustellung zu gewährleisten, können „Postleitzahl“ und „Straße“ nicht und „Hausnummer“ nur geringfügig variiert werden. Außerdem ist nicht auszuschließen, dass postalische Bereinigungsprogramme diese Abweichungen wieder rückgängig machen. Somit stehen fast nur „Name“ und „Vorname“ als Verfremdungsoptionen zur Verfügung – unter Berücksichtigung folgender Grenzen:

- Die Zustellbarkeit muss weiter gewährleistet sein, so dass Veränderungen von Namen und Vornamen nur dezent vorgenommen werden dürfen.
- Die Person, deren Adresse zu einer Kontrolladresse verfremdet wird, muss in den Prozess integriert werden und als Kooperationspartner dienen. Sie darf die verfremdete Adressversion nicht zu eigenen Zwecken einsetzen.
- Die Möglichkeit, dass Adressen, die aus verschiedenen Datenbanken in einen Gesamtbestand eingeflossen sind, einem Dublettenabgleich unterworfen sind, muss berücksichtigt werden. Bei einem Dublettenabgleich werden beim Vornamen oft nur die erste Stelle oder die ersten drei Stellen berücksichtigt, beim Nachnamen werden in der Regel phonetische Abgleiche verwendet. Aus einem „Meier“ einen „Mayer“ oder aus einem „Schmitt“ einen „Schmidt“ zu machen, ist somit nicht ausreichend für die Erstellung einer Kontrolladresse. Dienlicher sind bei Nachnamen vielmehr erfundene Doppelnamen (zum Beispiel „Müller-Schumann“ statt nur „Müller“) oder konstruierte Vornamendoppel (wie zum Beispiel „Anna-Maria“ statt nur „Anna“). Bei Vornamen kann man zudem die tatsächlichen Vornamen durch deren geläufige Rufnamen abformen – zum Beispiel „Klaus“ statt „Nikolaus“, „Ria“ statt „Maria“ oder „Hans“ statt „Johannes“. Sinnvoll ist es beim Generieren von eindeutigen Kontrolladressen, möglichst viele der dargestellten Adressvariationen zu kombinieren.
- Kontrolladressen sollten im Idealfall in verschiedene Postleitzahlenbereiche eingeschleust werden, da andernfalls ein nur in einigen PLZ-Gebieten begangener Datenmissbrauch unentdeckt bleibt. Es ist also sinnvoll, Kontrolladressen über verschiedene PLZ-Gebiete zu verteilen und in den vorhandenen Datenpool einzuspeisen.



Foto: mauritius RF

den Mitarbeitern, die mit dem Datenbanksystem arbeiten, nicht bekannt sein dürfen. Sie sind „Chefsache“ und dürfen nur dem Unternehmer oder einer externen Hilfsquelle bekannt sein.

Kontrolladressen dürfen auch nicht offensichtlich in eine Datenbank einfließen, sie sollten vielmehr durch anonyme Testkäufe – so genanntes „Mystery Shopping“ – in die Adressbestände aufgenommen werden. Diese anonymen Testkäufer bleiben für die firmeninternen Mitarbeiter unbekannt, wodurch ein Datendiebstahl leicht aufgedeckt werden kann, sollte einer dieser erfassten Testkäufer plötzlich über Dritte kontaktiert werden. Involvierte Kontrollpersonen, die entsprechende Postsendungen erhalten, können den bestohlenen Unternehmern sogar als detektivische Ermittler dienen:

Da jeder Betroffene nach § 34 BDSG das Recht hat, Auskunft über die ihn betreffenden Datenspeicherungen zu erhalten, kann sich auch die Kontrollperson rechtmäßig darüber informieren und die Herkunft der Daten ermitteln. Leitet diese Kontrollperson diese Informationen an das um seine Daten betrogene Unternehmen weiter, werden die Wege des Datendiebstahls offensichtlich und nachvollziehbar.

An dieser Stelle macht der Kontrolladressenexperte noch auf einen Irrglauben aufmerksam, dem viele Unternehmer unterliegen: „Mancher Manager wähnt sich in trügerischer Sicherheit, wenn als Kontrolladressen auch die eigene Anschrift oder die Anschriften einiger leitender Mitarbeiter (zum Beispiel Privatadressen) integriert werden. Die Verlockung, dies zu tun, ist hoch – alleine schon, um jedes Mailing

selbst im Briefkasten vorzufinden. Insbesondere verantwortliche Entscheider aus Geschäftsleitung, Marketing und Vertrieb prüfen auf diesem Wege auch die korrekte Verarbeitung und Postauflieferung. Sie glauben gerne, dass dieses ‚hausinterne‘ Kontrollsystem als Präventivmaßnahme ausreichend ist.

Der Nachteil hierbei ist aber, dass solche statischen ‚Kontrolladressen‘, die immer fester Bestandteil jeder Mailingaktion sind und zudem meist in unmittelbarer Nähe zur Firmenzentrale liegen, leicht ausselektiert werden können – gerade von eigenen Mitarbeitern, zuarbeitenden Dienstleistern oder Vertragspartnern, die die betreffenden Personengruppen beziehungsweise deren Adressen kennen könnten.“ Darüber hinaus, so Süppmayer weiter, „kann es auch problematisch bei der gerichtlichen Beweisbarkeit werden, wenn die eigenen Mitarbeiter als ‚Kontrolladressaten‘ dienen: Durch die Nähe zum Unternehmen könnten solche Zeugen dem Gericht unglaubwürdig erscheinen und Zweifel erwecken. Der Nachweis eines Adressmissbrauchs könnte sich alleine dadurch schon schwierig gestalten und letztlich scheitern.“

## Schutz muss sein

Für jedes Unternehmen und deren Datenschutzbeauftragte muss es von größter Wichtigkeit sein, alle erdenklichen Sicherheitsmaßnahmen zu ergreifen. Denn es steht mit dem Verlust des Wirtschaftsgutes „Adressen“ sowie dem Verlust des Kundenvertrauens beim Publikwerden von Datenschutzproblemen nicht gerade wenig auf dem Spiel. Spezialisierte Kontrolladressenunternehmen sind sicherlich die erste Wahl und können gefährdeten Unternehmen helfen, ein professionelles System von Kontrolladressen aufzubauen. „Aber welchen Weg auch immer man wählt“, so Süppmayer abschließend, „Hauptsache ist, dass überhaupt etwas zum Schutz der sensiblen Daten unternommen wird.“ ■

## Vertrauen ist gut ...

**Der Einsatz von Kontrolladressen ist auch für den kommerziellen Adresshandel einerseits ein abschreckendes Mittel und dient andererseits auch der Kontrolle der vertraglichen Treue der Geschäftspartner, die die Adressen zur Nutzung anmieten.**

„Kommerziell erworbene Adressbestände bei entsprechend professionellen Adressanbietern sind“, so Dieter Süppmayer, „branchenüblich immer mit Kontrolladressen versehen. So kann eine vertragsgerechte Nutzung der vermieteten Daten leicht überprüft und überwacht werden, nämlich:

- Nutzung der vermieteten Adressen nur für den vereinbarten Einsatzzweck (keine Konkurrenzangebote) und Einsatzzeitpunkt
- Durchführung von zum Beispiel unangemeldeten Gewinnspielen, um mittels der dadurch gewonnenen Daten eine eigene Datenbank

aufzubauen und in späteren Nachfassaktionen Neukunden gewinnen zu können

- Unerlaubte Kopien der Datenbestände mitsamt späterer Verwendung der Adressen (zum Beispiel bei weiterverarbeitendem Dienstleistungsbetrieb)
- Verleih der Adressdaten durch Listbroker ohne Genehmigung des Vermieters oder Adresseigentümers
- Fehler im Arbeitsworkflow
- Aufdeckung von unerlaubten Mehrfachnutzungen der vermieteten Datenbestände

