

Schluss mit dem Klau von Kundendaten: Schutzmechanismus Kontrolladressen

Es ist der Albtraum jedes Unternehmens, dessen Geschäft auf dem direkten Kundenkontakt beruht: Die sorgfältig gepflegte Kundendatenbank wird angezapft und Mitbewerbern zugespielt oder beliebig verhökert. Trotz hoher Sicherheitsstandards sind solche Datenlecks praktisch unvermeidbar, wenn ein gaunernder Mitarbeiter im eigenen Haus oder bei einem Servicepartner seine Chance wahrnimmt. Auch die unverschlüsselte Übertragung von Datenbeständen über das Internet öffnet dem Datenklau Tür und Tor. Schließlich liegen die Dateien weltweit auf Vermittlungsrechnern herum, die nicht hackerfest sind. Kontrolladressen, die unauffällig in der Datenbank platziert sind, haben eine zweifache Wirkung: Sie lassen, wenn sie systematisch angelegt, gezielt eingesteuert und gerichtsfest dokumentiert werden, einen Datenabfluss nachvollziehen und die Akteure auffliegen. Hinzu kommt der Aspekt der Prävention. Denn wenn potenzielle Datendiebe wissen, dass eine Kundendatenbank professionell „kontaminiert“ ist, lassen sie eher die Finger davon.

Von **SASCHA GLISS, München.**

Bei der Verwendung von Kontrolladressen gilt es, die unterschiedlichen Einsatzgebiete zu beachten:

- Adressen für Postmailings
- vom Call Center abzutelefonierende Adresslisten
- E-Mail-Adresslisten

und diese durch verschiedene Mechanismen zu berücksichtigen. Professionelle Kontrolladress-Anbieter wie beispielsweise Adress Control GmbH in Saarbrücken verfügen über ausgefeilte Instrumente, die für jeden Kunden auf das individuelle Schutzziel ausgerichtet werden.

Bei den Adresslisten für Mailings funktioniert das so: In die Datenbestände werden Adressen fiktiver Personen eingeschleust. Die Verfahren sind sicher, wenn niemand beim Adressenbesitzer die fiktiven Adressen kennt. Das geschieht durch den Kontrolladressenanbieter, beispielsweise durch einzelne Käufe, bei Zeitschriften durch Kurzabos, im Namen einer fiktiven Person, die postalisch erreichbar sein muss. Man kann also nur mit Vornamen und Titeln neue Personen erfinden. Wenn der Briefkasten beim Empfänger nur den Nachnamen zeigt, wird die Post

zugestellt, egal wie der Vorname lautet und ob ein akademischer oder ein Adelstitel hinzugefügt wurde.

Bei Adressen zum Telefonieren spielen Kontrolladressen eine wichtige Rolle, wenn man den Mitarbeitern und der IT-Sicherheit des Call Centers nicht traut. Hier richtet der Kontrolladressenanbieter Telefonanschlüsse fiktiver Person ein. Die Anrufe für diese Anschlüsse werden umgeleitet und laufen beim Kontrolladressenanbieter auf. Geschulte Mitarbeiter nehmen die Anrufe an; sie können sich anhand der Anzeige im Display „richtig“ melden. Jedes Gespräch wird zwecks weiterer Recherchen gründlich dokumentiert. Vor allem wird der Anrufer schriftlich aufgefordert, die Herkunft der Adresse zu belegen – hier wirkt das Recht auf Auskunft nach § 34 Bundesdatenschutzgesetz.

Auch beim Versand von E-Mails sind Kontrolladressen nützlich. Wer seine Kunden mit Newslettern bedient, kann seinen Adressbestand dadurch schützen, dass für jede beabsichtigte Aktion einige neue E-Mail-Adressen angelegt werden, die auf einen Kontrolleur geleitet sind. Schlägt eine „fremde“ E-Mail dort auf, bedeutet das: Es hat entweder einen Datenabfluss im Unternehmen gegeben, oder die Adresse ist auf einem Vermittlungsrechner durch Hacker kopiert worden. Letzteres lässt sich durch keine Maßnahme 100-prozentig vermeiden – dafür sorgt schon die generell unsichere Struktur des Internets.

Grundsätze

1. Es ist für den Erfolg wichtig, dass eine fiktive Adresse nur für eine ganz bestimmte Aktion verwendet wird, damit nachvollziehbar ist, wo genau eine missbräuchliche Verwendung ihren Ausgang hatte. Kontrolladressen, die über Monate oder gar Jahre in Adressdatenbanken schlummern, sind wertlos. Sie können keine Wege des Datenabflusses nachweisen und erst recht nichts vor Gericht beweisen. Es ist also ein ausgefeiltes Schutzsystem nötig, um den erhofften Erfolg zu erreichen.

2. Die Auswahl der fiktiven Vornamen und Namenszusätze muss so erfolgen, dass bei der Aufbereitung von Adressbeständen zum Zweck der werblichen Ansprache keine Kontrolladresse einem Dublettenabgleich zum Opfer fällt. Ferner reicht es nicht aus, männliche und weibliche Vornamen in gleichem

Umfang zu erfinden; die Namen müssen auch so gewählt werden, dass sie abwechselnd jüngere und ältere Personen darstellen. Beim Zielgruppenmarketing werden bei der Aufbereitung der Werbung die Personenkreise aussortiert, die man nicht als affin betrachtet. Mode für junge Frauen wird beispielsweise weder bei männlichen Vornamen noch bei „Ursula“ oder „Bertha“ beworben, eher bei „Chantal“, „Anne“ oder „Nikola“.

3. Alle Vorgänge müssen akribisch belegt sein, um Verstöße gerichtlich und unter Einschaltung der Datenschutzaufsichtsbehörden verfolgen zu können.

Undichte Stellen

Datenlecks können an verschiedenen Stellen entstehen, ein Kontrolladressenmanagement muss sich auf alle Varianten einstellen.

1. Beim Datenhalter sind mitunter untreue Mitarbeiter am Werk, die eine Chance zu „aggressiver Vermögensbildung“ sehen – und nutzen. Wenn diesem Personenkreis bekannt ist, dass das Unternehmen über ein professionelles Verfolgungssystem verfügt, halten sie sich eher zurück.

2. Beauftragte Dienstleister können, wie aktuell der Fall Schlecker zeigt, eine Schwachstelle sein, weil dort nicht ordentlich gearbeitet wird, unzuverlässige Personen agieren, Leichtsinn oder schlicht Inkompetenz im Spiel sind. Der Auftraggeber hat zwar gesetzliche Pflichten, sich von der Zuverlässigkeit der Verfahren beim Dienstleister zu überzeugen. Wenn aber diese Pflichten vernachlässigt werden, wenn gar kein Know-how vorhanden ist, um Prüfungen durchzuführen und man die Kosten für externe Prüfer scheut, dann kann genau das passieren, wovon derzeit die Medien voll sind. Datenskandal? Eher mangelnde Sorgfalt bei Auftraggeber und Dienstleister.

3. Auch die vagabundierenden Datenbanken, die 2007 und 2008 für Schlagzeilen sorgten, fallen in diese Kategorie: Wer sein Call Center über den Preis auswählt und geflissentlich übersieht, dass es sich um Waschküchenbetriebe handelt, darf sich nicht wundern, wenn seine Daten auf dem schwar-

zen Markt gehandelt werden. Man denke nur an den von der Wirtschaftswoche minutiös belegten Fall der 17.000 Adressen mit Bankverbindung, die Kabel Deutschland durch Kopieren im Call Center abhanden kamen und zu Abbuchungswellen bei den Opfern führten.

4. Das Internet ist durch seine offene Struktur eine weitere undichte Stelle, über die Daten abfließen können. Das Problem: Bei unverschlüsselter Übertragung von Adressbeständen sind diese Dateien auf Vermittlungsrechnern für Cyberkriminelle abgreifbar. Hier helfen Kontrolladressen nur, die Tatsache des Abflusses bekannt zu machen. Täter sind nicht überführbar.

Erfolge?

Im Gespräch mit Fachleuten wird immer wieder deutlich, dass das Kontrolladressengeschäft eine diskrete Branche ist. Wird ein Missbrauch nachgewiesen, kommt es darauf an, ob straf- oder zivilrechtliche Folgen vom Geschädigten erwogen werden. Dieter Süppmayer von Adress Control: „Ein Vergleich zum Zweck der Schadenersatzzahlung kann eine bessere Lösung sein als der Gang durch die Gerichtsinstanzen. Mancher Richter mag nämlich mit dem Thema ‚Adressdatenbanken‘ überfordert sein. Erst kürzlich wurde dies durch einen Fall beim Hamburger Amtsgericht (DSB 4/10, Seite 4) bestätigt.“ Zahlreiche Fälle von aufgedeckten Missbräuchen führten schon zum Abbruch von Geschäftsbeziehungen und zu außergerichtlichen Einigungen.

Und man darf den Aspekt der Prävention nicht gering schätzen: Datensicherheit ist bekanntlich die „Organisation des Nicht-Ereignisses“; man kann nicht beweisen, mit welchem Aufwand man welche Schäden verhütet. Aber den Entscheidungsträgern muss klar sein, dass sie ihre Daten angemessen und wirksam zu schützen haben. Der Fall Schlecker steht hierfür als mahnendes Beispiel. ■

Stichworte: Kontrolladressen, Kundendaten, Datenskandal, Datenabfluss, Marketing