5 Management Summary

Datenschutz ist als Aspekt der informationellen Selbstbestimmung im Grundgesetz verankert. Danach hat ein jeder Bürger das Recht, selbst zu entscheiden, wer über seine Daten verfügen darf. Das Bundesdatenschutzgesetz soll ihn in diesem Recht bestärken, allerdings zeigen die Datenschutzskandale der jüngsten Zeit, dass Unternehmen Schwierigkeiten haben ihren Verpflichtungen im Bereich Datenschutz nachzukommen. Natürlich handelt es sich dabei teilweise um Extremfälle und ein Rückschluss auf die gesamte Wirtschaft oder einzelne Branchen ist nicht möglich; Ziel dieser Studie ist es daher, die tatsächliche Situation abzubilden, indem nicht nur Extremfälle betrachtet werden.

Zielgruppe der Studie ist die Versicherungsbranche. Diese wurde gewählt, da sie mit besonders sensiblen Daten in unterschiedlichen Bereichen umgeht. So muss ein Kunde schon beim Abschluss einer Versicherung verschiedene Angaben machen, um der Versicherung das Bearbeiten des Antrags zu ermöglichen. In einigen Fällen werden zusätzlich Daten von früheren Versicherungen oder sogar Daten von Ärzten und Krankenhäusern bezogen, wozu der Kunde diese von der Schweigepflicht entbinden muss. Dazu kommen Daten, die sich während des Vertragsverlaufs ansammeln, wie Inkassodaten oder Schadensdaten. Außerdem werden bei den meisten Versicherungen Daten für Marketingzwecke gespeichert, Daten von Dritten, die in Schadensfällen mit einem Kunden verwickelt waren oder Daten von Mitarbeitern und Bewerbern. Einige dieser Daten werden bei Prüfungen von Anträgen oder bei Schadensfällen beim zuständigen Fachverband oder bei anderen Versicherern abgefragt oder an diese weitergegeben. Diese Vielzahl an Daten und der Umgang mit diesen stellen besonders hohe Anforderungen an Versicherungsunternehmen. Aber auch der Schaden bei fahrlässigem und verantwortungslosem Umgang mit diesen Daten ist besonders hoch.

Die Studie läuft in vier Phasen ab.

In der ersten Phase werden ausgewählte Webseiten untersucht. Ziel ist es dabei zu ermitteln, welche Daten in unterschiedlichen Zusammenhängen erhoben werden und ob Verfahren angewendet werden um diese Daten zu schützen und Missbrauch zu verhindern. Außerdem wird überprüft ob eine Datenschutzerklärung und ein Verfahrensverzeichnis vorhanden sind und ob ein Datenschutzbeauftragter als Ansprechpartner genannt wird.

Die zweite Phase besteht aus einer Datenschutzauskunft, die an alle Versicherungen versendet wird und deren Auswertung. Es existieren bei unterschiedlichen Versicherungen Daten wie Kundendaten, Schadensdaten oder Interessentendaten. Dabei wird die Zeit gemessen, die zum Antworten benötigt wird, der Inhalt sowie die Tonalität.

In der dritten Phase wird eine Onlineumfrage erstellt. Bei alle Unternehmen, die in der zweiten Phase geantwortet haben, wird direkt der Absender angeschrieben, da dieser offensichtlich mit dem Thema betraut ist. Bei denen, die nicht geantwortet haben, werden erneut die allgemeinen Kontaktdaten verwendet.

Die vierte Phase besteht aus einer Kontaktaufnahme mit den Vorstandsvorsitzenden ausgewählter Versicherungen. Ausgewählt werden alle, deren Antworten deutliche Indikatoren für Probleme mit dem Datenschutz aufweisen. Untersucht wird in dieser Phase die Reaktion des Vorstandsvorsitzenden und damit verbunden die Frage, ob es in den betroffenen Unternehmen ein entsprechendes Problembewusstsein gibt.

Die Ergebnisse jeder einzelnen Phase sind bemerkenswert.

Das Opt-In-Verfahren erlaubt es einem Unternehmen, die Daten, die ein Benutzer hinterlässt zu nutzen. Beispielsweise indem dem Benutzer des Kontaktformulars ein Angebot per E-Mail zugesendet wird. Ein Opt-In muss dabei aktiv erteilt werden. Daher sind Opt-In-Erklärungen, die an den eigentlichen Service gebunden sind unwirksam. In den untersuchten Bereichen konnte das Opt-In durchschnittlich in 18% der Fälle erteilt werden, al-

lerdings war es in einem Drittel dieser Fälle an den Service gekoppelt und damit unwirksam.

HTTPS bietet die Möglichkeit Daten über das Internet sicher zu übertragen. Es ist das einzige Verschlüsselungsverfahren, welches von allen gängigen Browsern ohne zusätzliche Software unterstützt wird. Werden die Daten unverschlüsselt übertragen können diese Daten abgefangen und gelesen werden. In den untersuchten Bereichen wurden die Daten durchschnittlich bei 29% unverschlüsselt und damit unsicher übertragen.

Doppel-Opt-In und Capture sind Verfahren, die Missbrauch der Daten durch Dritte verhindern. Das Doppel-Opt-In-Verfahren verhindert, dass ein anderer als der Adressenbesitzer ein Opt-In erteilt. Das Capture verhindert, dass Daten von Programmen eingegeben werden können. Werden beide Verfahren nicht angewendet, kann ein Service als Spam-Quelle genutzt werden oder einzelnen Personen durch ungewollte Abonnements u.ä. schaden. Bei Versicherungen zeigte sich, dass die Nutzung beider Verfahren sehr gering ist.

Eine Datenschutzerklärung dient dazu der Transparenz- und Aufklärungspflicht nachzukommen. Diese Pflicht besteht immer dann, wenn Daten auf der Webseite erhoben werden, dies ist bei allen untersuchten Webseiten der Fall. Dennoch verfügten nur 91% der Webseiten über eine Datenschutzerklärung.

Zweck des Verfahrensverzeichnisses ist es, darüber aufzuklären, wie mit Daten im Unternehmen umgegangen wird. Es muss jedem zugänglich gemacht werden, der dies verlangt. Daher ist die Veröffentlichung auf der Webseite naheliegend. Dies tun allerdings nur 23% der Versicherer. 3% weisen zumindest darauf hin, dass ein Verfahrensverzeichnis auf Anfrage zugesendet wird. Allerdings wurden in allen gesichteten Verfahrensverzeichnissen die Punkte nur formal abgearbeitet, teilweise noch nicht einmal das. Ein Verfahrensverzeichnis, welches tatsächlich Aufschluss über die Datenverarbeitung gibt, gab es in keinem Fall.

Die gravierendsten Ergebnisse der Studie liefert die Datenschutzauskunft. 36% der Versicherungen reagierten gar nicht auf das Auskunftsersuchen. Die verbleibenden 64% enthalten 10%, die nicht korrekt geantwortet haben. Damit antwortete nahezu die Hälfte aller Versicherer (46%) nicht oder nicht korrekt. Auffällig ist in diesem Zusammenhang, dass der Datenbereich Schadensdaten bis auf wenige Ausnahmen übersehen wurde. Nur ein Drittel der Unternehmen lassen erkennen, dass die Datenschutzauskunft als Kundenservice und zur Kundenbindung gesehen wird. Dagegen teilten 8% der Versicherer mit, dass eine Auskunft ohne Kundennummer oder ähnliches gar nicht möglich sei, darunter auch welche, bei denen im Vorfeld Daten auf der Webseite hinterlassen wurden. In zwei Fällen wurde sogar eine Auskunft über die Daten einer fremden Person erteilt obwohl diese nur den gleichen Namen hatte. Diese Auskünfte erhielten auch sensible Daten wie Krankheitsdaten und Bankverbindungen.

Die Umfrage zeigte, dass das Interesse seitens der Versicherer äußerst gering ist. Obwohl der Zeitaufwand mit 2 Minuten sehr gering war, schaffte es nur 6% der Versicherer innerhalb eines Monats die Webseite mit der Umfrage zu besuchen und 1% an der Umfrage teilzunehmen. Dagegen nahmen einige Datenschutzbeauftragte die Studie offensichtlich als Bedrohung war und reagierten mit Beschimpfungen und Bedrohungen.

Schäden, die aufgrund von Verstößen gegen den Datenschutz entstehen werden in den meisten Fällen als grob fahrlässig eingestuft. Damit ist der Vorstand nicht nur verantwortlich, sondern haftet auch mit seinem Privatvermögen. Dies scheint aber den meisten Vorständen nicht bewusst zu sein, denn in der vierten Phase wurden die Versicherer, die in der Studie besonders aufgefallen sind, über ihren potentiellen Handlungsbedarf in Kenntnis gesetzt. Nur 5% von ihnen interessierte sich dafür zu erfahren, wo genau die festgestellten Probleme liegen. 7% baten dagegen von weiteren Kontakten abzusehen. Alle anderen angeschriebenen Versicherer reagierten nicht.

Insgesamt ist zu erkennen, dass die Mehrheit der Versicherer mit dem Thema Datenschutz fahrlässig umgeht. Prozesse, die den Datenschutz sicherstellen könnten sind nur in Ansätzen zu erkennen.

Zusätzlich zu umfangreichen Rechtsverstößen, wird auch das Vertrauensverhältnis zwischen Versicherungen und deren Kunden belastet.