Business Process Outsourcing?

Aber sicher!

Geht nicht. Zu riskant. Nicht sicher genug. Hacker, Phishing[1], Datenklau – die Ängste sind ebenso groß wie berechtigt, wenn es gilt, für ein großes Outbound-Projekt zehntausende von Daten an einen Dienstleister zu übermitteln oder diesem gar Zutritt ins eigene CRM-System zu gewähren. Doch ohne diesen Austausch geht es nun mal nicht und das ist dann leider auch oftmals der Grund, auf das Outsourcing – und im schlimmsten Falle auf das gesamte Projekt – zu verzichten. Dabei gibt es sie längst: exzellente Callcenter-Dienstleister mit Top-Systemen und zuverlässigem Datenschutz. Man muss sie nur finden! Martin Knopp von T.D.M. erklärt, worauf man beim „Business Process Outsourcing" – also beim Auslagern solcher einzelnen Prozesse an externe Dienstleister – achten muss und woran man einen zuverlässigen Dienstleister erkennt.

1: Hacker-Methode, bei der Daten auf ihrem Übertragungsweg „abgefischt" werden

SQUT: Wie oft werden Sie mit der Herausforderung konfrontiert, dass die IT-Abteilung eines potenziellen Kunden ein Projekt kippt, weil sie die Datensicherheit gefährdet sieht?

M. Knopp: Dies passiert leider noch sehr oft. Speziell im Bereich Outbound ist in vielen Unternehmen die Skepsis sehr hoch, weil der Glaube vorherrscht, dass diese Unternehmen so innovative Produkte und Lösungen anbieten, dass die Kunden von alleine kommen werden. Dann herrscht bei den IT-Leitern / Datenschutzbeauftragten oftmals die starke Meinung vor, dass für dieses „Experiment" Outbound dann doch lieber die Datenhoheit nicht aufgegeben wird. Es entstehen dann Vorschläge wie, dass für ein Account-Team von 20 Außendienstmitarbeitern auch z. B. per individuellem Papierkalender durch den Dienstleister terminiert werden kann.

SQUT: Können Sie die Sorgen der IT-ler gut und schnell entkräften oder ist es immer harte Überzeugungsarbeit mit Diskrepanzen, die man in der Akquisephase eigentlich nicht braucht?

M. Knopp: Der IT-/Datenschutzverantwortliche handelt ja nicht absichtlich konträr zu den Möglichkeiten des Dialogmarketings im Marketing und Vertrieb, sondern er vertritt, wie jede Fachabteilung eines Unternehmens, erst einmal seine Interessen. Auch spricht der Datenschutz in seinen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) von möglichst geschlossenen IT-Systemen mit wenig bis gar keiner Zugriffsmöglichkeit von außen. Die Strafen bei entsprechenden Verstößen sind empfindlich angesetzt und können im Einzelfall mehrere zehntausend Euro betragen. Dem Vertrieb eines Dialogmarketing-Unternehmens fällt dann die Aufgabe zu, die verschiedenen Zielrichtungen zu moderieren und in die richtige Richtung zu lenken. Dabei ist es wichtig, darauf hinzuweisen, dass der wirtschaftliche Vorteil, z. B. durch die qualifizierte Marktbearbeitung eines Callcenters, dem Unternehmen in jedem Falle hilft, die Wachstumsziele wirtschaftlich effizient zu erreichen.

Uns gelingt es, die IT-Verantwortlichen mit authentischen Beispielen und überzeugenden Referenzen, in Verbindung mit einer leistungfähigen IT-Umgebung und entsprechenden Datenschutz-Prozessen, für das Thema „Business Process Outsourcing" zu gewinnen.

SQUT: Aus der Praxis: In welchen Formen tauschen in der Regel Dienstleister und Auftraggeber die Daten für eine Kampagne aus und was sind die Vor- bzw. Nachteile?

M. Knopp: Man kann grob von drei Szenarien ausgehen.

1. Die Daten für die Outbound-Kampagne werden an den Dienstleister ausgelagert. Das ist zwar die effektivste Variante, aber der Import und Reimport der Daten müssen technisch absolut zuverlässig und sauber laufen. Damit ist z. B. gemeint, dass es wenig sinnvoll ist, wenn die Ergebnisse der Call-Kampagne dann von Praktikanten manuell ins CRM-System eingepflegt werden. Es muss auch klar geregelt werden, wer die Entscheidung hinsichtlich der ermittelten Datenänderungen (z. B. Adresse) fällt. Sollen z. B. Änderungen in der postalischen Adresse einfach reimportiert werden oder muss das Unternehmen noch einmal einen Blick darauf werfen? Hinzu kommt: Die Daten müssen in der Regel explizit freigegeben werden. Gemäß dem Leitsatz „Vertrauen ist gut, Kontrolle ist besser", sollte im Vorfeld einer Zusammenarbeit auf Basis des BDSG[1] und hier mit dem Stichwort „Auftragsdatenverarbeitung" eine entsprechende Vereinbarung getroffen werden. Hierbei wird z. B. definiert, wie lange die Daten durch den Dienstleister in den eigenen Systemen nach Aktionsende vorgehalten werden dürfen. Auch ist es sinnvoll, sich eine Übersicht der technisch organisatorischen Maßnahmen (TOMs) geben zu lassen und diese als Grundlage für die Beauftragung zu definieren. Die TOMs beschreiben, wie das Unternehmen das Thema Datenschutz administrativ umsetzt.

2. Der Dienstleister arbeitet im System des Auftraggebers. Hier muss die IT-Abteilung den Zugang konfigurieren, Limitierungen definieren etc. Wichtig sind dabei redundante Systeme, denn: Was passiert, wenn ein Provider beim Dienstleister ausfällt? Der Aufwand für dieses Szenario ist schon etwas höher und es führt dazu, dass der Dienstleister mit vielen fremden Systemen arbeiten muss, obwohl er vielleicht eine eigene TOP-Lösung im Hause hätte. Bei dieser sollte man allerdings klarstellen, ob der Dialogmarketing-Anbieter eine eigene IT im Haus vorhält oder ob die IT-Leistung auch von ihm nur eingekauft wird (Stichwort Reaktionsgeschwindigkeit bei Problemen).

3. Der Dienstleister schickt Agenten zum Auftraggeber. Dieses Szenario ist in der Regel mit hohem Aufwand und entsprechenden Kosten (Reisekosten, Mitarbeiterschulung auf Fremdsystemen usw.) verbunden. Grundsätzlich müssen auch überhaupt erst einmal Agenten für den mobilen Einsatz gefunden werden (Stichwort: familiäre Bindung, fremde Arbeitsumgebung usw.), und es ist zu bedenken, dass diese dann beim Dienstleister für andere Projekte nicht zur Verfügung stehen. Auch für den Auftraggeber ist diese Variante nicht ohne. Er muss sich „Fremde" ins Haus holen und somit extra sogenannte „Datenschutzvereinbarungen mit den entliehenen Mitarbeitern" erstellen.

Weiterhin ist auch zu beachten, dass der Mitarbeiter aus der Ferne betreut werden muss, beispielsweise für das interne Coaching. Es kann belastend für den Agenten im Außeneinsatz sein, wenn der gewohnte Support in Form von Feedbackgesprächen mit der Projektleitung oder der Personalabteilung fehlt.

SQUT: Die Horror-Szenarien beim „Datenunfall": Trotz aller Vorsicht gingen Daten verloren, Unbefugte hatten Zugriff oder im eigenen System wurde Schaden angerichtet etc. Was raten Sie einem Dienstleister, wenn trotz aller Vorsicht ein „Datenunfall" passiert?

M. Knopp: Offenheit gegenüber dem Kunden ist jetzt allererstes Gebot der Stunde. Daten, die verloren oder gar veruntreut worden sind, können weitreichenden Schaden verursachen. Je eher desto besser kann ein Maßnahmenplan abgestimmt werden. Weiterhin sollte man nur Dienstleister für die Beauftragung auswählen, die eine entsprechende regelmäßige Zertifizierung ihrer DV-Prozesse vornehmen, damit die möglichen Lücken so klein wie möglich gehalten werden und um dem aktuellen Stand der Technik zu entsprechen.

SQUT: Hat die Verfügbarkeit der „Cloud" für Sie einen kritischen Einfluss auf das Thema Datensicherheit oder vereinfacht sie die Prozesse?

M. Knopp: Cloud-Lösungen sind dem Wesen nach für uns nur andere Plattformen für die benötigten Kundendaten. Ob wir uns als Dienstleister direkt an das

1: Bundesdatenschutzgesetz

Warenwirtschaftssystem des Kunden anmelden oder dies über das Internet vollziehen, ist rein inhaltlich gleich, technisch aber eine andere Basis. Die Wahrnehmung von Cloud-Lösungen hat sicherlich in Zeiten von NSA-Skandalen gelitten. Gleichwohl sind wir der Meinung, dass jedes Unternehmen heute prüfen muss, ob eine eigene IT zur Kernkompetenz des Unternehmens gehören sollte. Oftmals gibt es interessante Einsparungs- und Optimierungsmöglichkeiten in der eigenen Struktur durch den Einsatz von Cloud-Lösungen, wobei dies natürlich auch immer kritisch mit dem Thema Datensicherheit zu bewerten ist.

SQUT: Worauf muss ich als Auftraggeber achten, wenn ich Prozesse effektiv und sicher auslagern will?
M. Knopp: Wie so oft im Leben ist der Partner, den ich von Anfang an in meine Überlegungen mit einbeziehe, am einfachsten zu überzeugen. Sollte also die Entscheidung bei einem Marketing-/Vertriebsleiter gereift sein, das innovative Medium „Telefonmarketing" einmal einzusetzen, so ist es sinnvoll, sobald als möglich die IT-Leiter / Datenschutzbeauftragten mit ins Boot zu holen. Gemeinsam kann dann mit dem erfahrenen Callcenter-Dienstleister erarbeitet werden, welches die Variante ist, die dem Partner für den Dialog den Zugang zu den Daten am einfachsten und in Abstimmung mit individuellen Unternehmensleitlinien ermöglicht.

SQUT: Technisch bzw. juristisch kann man also sehr viel Prophylaxe vornehmen. Aber wie steht es um die Schnittstelle Mensch? Welche Gefahren lauern, wenn Externe Wissen über Interna erlangen und wie schützt man sich davor?
M. Knopp: Das beste Sicherungssystem im Unternehmen ist noch immer die Zufriedenheit der Mitarbeiter. Nur ein Mitarbeiter, der gerne seine Aufgaben erfüllt, wird sich nicht den ganzen Tag den Kopf darüber zerbrechen, wie er die unternehmenseigenen Sicherungssysteme aushebeln kann, um dem Unternehmen zu schaden. Bezahlung über Mindestlohn, feste und langjährige Arbeitsverhältnisse, regelmäßige Schulungen und ein tolles Betriebsklima unterstützen die Unternehmen bei diesem Vorhaben.

SQUT: Wie sorgen Sie bei T.D.M. für reibungslosen Umgang mit eigenen und fremden Daten?
M. Knopp: Wir setzen bei uns alle beschriebenen Maßnahmen und noch weitere ein und binden unsere Mitarbeiter veranwortlich in die Prozesse von Anfang an mit ein. Dies bedeutet, vom Azubi bis zum Geschäftsführer steht das Thema Datenschutz ganz oben auf der Agenda, weil wir wissen, wenn uns unsere Kunden nicht mehr ihre Daten anvertrauen, ist für uns die Tätigkeit als Unternehmen der Dialogkommunikation unmöglich.

SQUT: Was muss ein guter zuverlässiger Dienstleister also bieten?
M. Knopp: Eine einfache Checkliste für die Auswahl sollte die folgenden Fragen beinhalten:

1. Existiert ein IT-Grundschutz beim Dienstleister mit mehrstufigen Sicherungssystemen für Soft- und Hardware im Falle interner und externer Gefahren in Kombination mit regelmäßigen Audits unabhängiger Prüfer?
2. Gibt es überhaupt einen regulär bestellten Datenschutzbeauftragten mit jährlichen Datenschutzberichten und können diese eingesehen werden?
3. Ist ein Vertragswesen für Auftragsdatenverarbeitung, Vertraulichkeitsvereinbarungen und technisch organisatorische Maßnahmen (TOMs) vorhanden?
4. Gibt es eine Verpflichtung aller am Prozess beteiligten Personen auf den Datenschutz im Rahmen ihrer arbeitsvertraglichen Pflichten?
5. Hat der Dienstleister eine Betriebshaftpflichtversicherung für den Fall der Fälle abgeschlossen?
6. Sind Referenzen mit Auskunft über den vertrauensvollen Umgang mit Fremddaten verfügbar? ■

Martin Knopp
Kaufmännischer Leiter T.D.M.
Telefon-Direkt-Marketing GmbH
www.tdm.de/dialogmarketing