Datensicherheit

Bester Service braucht die sichersten Systeme

Foto: © YB / Fotolia.com

Beim Autokauf merken Sie sofort, wenn Sie statt der bestellten Luxuslimousine einen Mittelklassewagen erhalten. Doch wie verhält es sich beim Thema Customer Services? Was macht exzellenten Service aus, und woran erkennen Sie einen Dienstleister, der dieses Versprechen am Ende des Tages auch einlösen kann? Heute gilt: Die Basis für mehr Performance, Flexibilität und Qualität ist eine zuverlässige und vor allem sichere IT-Infrastruktur.

Performance, Satisfaction, Wertschöpfung, Kundenbegeisterung, Extraklasse, Innovation, Excellence und Erfolg. In der heutigen Werbewelt wird dem potenziellen Auftraggeber sehr viel versprochen – dies gilt insbesondere für saturierte Märkte wie auch den Kundenservice. Die Bedürfnisse, Anforderungen und Präferenzen variieren von Branche zu Branche und von Unternehmen zu Unternehmen, jedoch eint alle der Wunsch nach Service Excellence zu einem marktgerechten Preis. Daher wird seit Ende der 70er Jahre bis heute von allen Anbietern der Arbeitnehmer im Kundencenter auf die relevanten Punkte hin optimiert. Die Unternehmen haben diesbezüglich jedes Konzept und jede Geheimformel für einen Wettbewerbsvorsprung inzwischen ausgeschöpft. Anders beim Produktionsfaktor IT-Infrastruktur. Gerade durch den extremen technischen Fortschritt der letzten Jahre, die rechtlichen Änderungen und Unsicherheiten der letzten Monate zum Schutz der personenbezogenen Daten sowie die gigantischen Steigerungsraten im Bereich der Cyber-Kriminalität, entwickelt sich die IT eines Dienstleisters zum zentralen Differenzierungsmerkmal und Wettbewerbsfaktor. Dies gilt nicht nur für Performance, Flexibilität und Qualität, sondern insbesondere für Zuverlässigkeit und Sicherheit.

Safe ist noch lange nicht sicher

Angefangen beim wegweisenden Safe Harbor-Urteil des Europäischen Gerichtshofs (EuGH) vom Oktober letzten Jahres, das die Übermittlung und Speicherung von Kundendaten in die USA europäischem Recht zufolge als unzureichend erklärt hat, über die bahnbrechende Einführung der Europäischen Datenschutzgrundverordnung, bis hin zu den aktuellen Fällen aus dem Bereich der Cyber-Kriminalität mit nicht zu unterschätzenden Imageschäden und Umsatzeinbußen – die Sicherheit und der Schutz der Kundendaten, bislang eher ein notwendiger Nebenaspekt bei der Einkaufsentscheidung, erfahren dabei notwendigerweise Priorität.

Ebenfalls nicht zu unterschätzen: die Qualität der Infrastruktur selbst. Wie gut sind die Systeme aufeinander abgestimmt? Sind sie auf dem aktuellen technischen Stand und gegen Überlastung, Stromausfall, Wassereinbruch etc. gesichert? Lange Ausfallzeiten und damit einhergehende Verluste für die Unternehmen sind für niemanden hinnehmbar.

Ein weiterer Aspekt: die zunehmende Sensibilität der Internetnutzer. Unternehmen sollten sich heutzutage darauf einstellen, dass die Kunden verunsichert sind, wie mit ihren persönlichen Daten verfahren wird. So befürchten laut „Eurobarometer“ vom Oktober 2014 ganze 58 Prozent der Internetnutzer, dass ihre Daten missbraucht werden, und eine Umfrage der BITKOM aus dem gleichen Zeitraum ergab, dass diese Sorge 24 Prozent der User dazu veranlasst, sich dem Online-Shopping bewusst zu verweigern.

Es ist also eine Frage des Vertrauens in die Zuverlässigkeit und Sicherheit eines Unternehmens und dessen Prozesse, ob ein potenzieller Kunde auch tatsächlich zum Kunden wird.

Mit Sicherheit Vertrauen schaffen

Vor dem Hintergrund des gewaltigen Datenvolumens im Kundenservice und der Dimension des innereuropäischen und

transatlantischen Datenverkehrs, kann der Einfluss der Faktoren Datenschutz, Datensicherheit und Betriebssicherheit auf den Kundenservice und die Service-Organisationen im Call- und Contact-Center-Bereich nicht hoch genug eingeschätzt werden. Insofern sind für Dienstleister aktuell drei Dinge entscheidend: Erstens: der Einsatz und die Gewährleistung modernster IT-Sicherheitsstandards zum Schutz vor Cyber-Kriminalität. Zweitens: Rechtssicherheit bzw. die Sicherstellung der aktuellen Datenschutz- und Datensicherheitsbestimmungen. Und drittens: die Erfüllung von vorgegebenen Industriestandards anhand von Zertifizierungen, wie zum Beispiel der ISO-Norm 27001 oder dem PCI-DSS für den Zahlungsverkehr mit Kreditkarten.

Strategie: intelligente IT – exzellenter Service

Gute Voraussetzungen, um Vertrauen zu schaffen, sind modernste Informationstechnik sowie ein erfahrenes Compliance-Management. Beim Customer Services-Anbieter walter services gehört beispielsweise der Umgang mit personenbezogenen Daten zum eigenen Tagesgeschäft und damit auch die Gewährleistung der Sicherheit und des Schutzes dieser Daten.

Daher setzte das Unternehmen bei Planung und Aufbau der neuen IT-Infrastruktur von vornherein konsequent auf höchste Maßstäbe bei Datensicherheit und Datenschutz und garantiert außerdem aufgrund der Redundanz der Server-Infrastruktur eine hohe Ausfallsicherheit. Für die Kunden, die das Unternehmen mit der Umsetzung von Customer Services beauftragen, gewährleistet walter services eine Verfügbarkeit der Netzinfrastruktur und IT-Systeme von 99,9 Prozent. Das entspricht einer maximalen Ausfallzeit von weniger als neun Stunden im Jahr. Dabei fließt über das hochmoderne MPLS-Netz des Customer Service-Dienstleisters ein Datenvolumen von rund 40 Gigabit pro Minute.

„Um dies zu erreichen, hat walter services in den vergangenen zwei Jahren die Informations- und Telekommunikationstechnik im Unternehmen einem umfassenden Modernisierungsprogramm unterzogen und ganz im Zeichen von Industrie 4.0 die digitale Transformation konsequent umgesetzt", so Frank Wagner, Chief Compliance Officer bei walter services. „Eine zentrale Aufgabe nimmt hier auch das Compliance-Management ein für die Sicherstellung von Datenschutz und Datensicherheit sowohl innerhalb des Unternehmens als auch für Auftraggeber. Zusammen mit vier Jahrzehnten Erfahrung im Kundenservice, bezeichnen wir unsere Haltung und Vorgehensweise als Service Intelligence." Der Customer Service-Anbieter setzt Standards bei der IT-Sicherheit: Er speichert Daten von Auftraggebern und deren Kunden ausschließlich im eigenen Netz, der eigenen „private Cloud" und greift allein auf eigene Server im eigenen zertifizierten Rechenzentrum in Karlsruhe zu. Zusätzlich geschützt wird das Firmennetz von einem dreistufigen Firewall-Konzept. Der Beitritt zur „Allianz für Cyber-Sicherheit" des Bundesamts für Sicherheit in der Informationstechnik und der damit verbundene Wissens- und Erfahrungstransfer runden das Bild ab.

Wie all diese Faktoren schon fast zwangsläufig zur Erweiterung des Geschäftsfeldes führten, erläutert Wagner: „Angesichts unserer eigenen Erfahrungen im Thema Datensicherheit sowie der eigenen komfortablen Situation bezüglich der aktuellen Rechtslage, haben wir uns bei walter services dazu entschlossen, nicht nur den eigenen Geschäftspartnern rechtssichere Customer Services anzubieten. Unter der neuen Marke walter cloud services eröffnen wir auch anderen Unternehmen, im Segment der Business Services mit Data Storage- und Unified Communications-Angeboten, individuelle und hochleistungsfähige Lösungen."

Hinterfragen kostet nichts

Entscheider und Verantwortliche im Kundenservice sind auch aus Kostengründen gut beraten, ihre Serviceorganisationen, Outsourcing-Partner und deren Dienstleister umfassend und gründlich auf alle Aspekte von Sicherheit, insbesondere aber hinsichtlich der Speicherung und dem Transfer personenbezogener Daten, zu prüfen und auf ein sicheres Fundament zu stellen. Wer eine gute Wahl treffen möchte, achtet zusätzlich auf das Compliance-Management des Dienstleisters. So gilt es auch zu klären, ob der Dienstleister bereits auf die aktuelle Rechtssituation eingestellt ist: Erfolgt die Speicherung von Daten ausschließlich innerhalb der EU? Sind die Daten vor einem Zugriff aus so genannten unsicheren Drittländern geschützt? Wie verhält sich die Lage bezüglich etwaiger Sub-Dienstleister? Viele Firmen besitzen keine vollständige Transparenz über den genauen Verlauf der Datenströme bei ihren Dienstleistern. Darüber hinaus ist zu prüfen, ob ausreichende Maßnahmen der Informationssicherheit existieren, wie die Verschlüsselung von Inhalten, damit die Daten vor dem Zugriff durch den Dienstleister selbst geschützt sind. Und zu guter Letzt sind die Aktualität und Leistungsfähigkeit der IT-Infrastruktur kritisch zu hinterfragen.

Verantwortung beruhigt abgeben

So aufgestellt und alle Aspekte bezüglich Rechts-, Betriebs- und IT-Sicherheit berücksichtigend, kann ein Unternehmen seine Kundenschnittstellen beruhigt in die Hände seines Outsourcing-Partners geben, was den Kundenservice anbelangt sowie die Speicherung und Verarbeitung der personenbezogenen Daten. Auch wenn es niemals hundertprozentige Sicherheit geben kann, ist damit dem aktuellen Stand der Informationstechnik Genüge getan. Und wer seiner Verantwortung nachkommt, indem er sie beruhigt abgeben kann, bietet seinen Kunden nicht nur exzellenten, sondern auch intelligenten Service.

Michaela Kreuzpointner ←

CHECKLISTE

Darauf sollten Sie im Hinblick auf das Thema Sicherheit bei der Dienstleisterauswahl achten

Fragen an den Customer Service-Anbieter:

- → Sind die Integrität, Vertraulichkeit und Verfügbarkeit Ihrer IT gewährleistet?
- → Benutzen Sie Verschlüsselungs-Algorithmen?
- → Sind die Integrität, Vertraulichkeit und Verfügbarkeit Ihrer TK-Anlage gewährleistet?
- → Wie ist Ihre Firewall gegen Angriffe gesichert?
- → Ist Ihr Firewall-System mehrstufig?
- → Setzen Sie alle Vorgaben des BDSG§11 um? (Zutrittskontrolle – Zugangskontrolle – Zugriffskontrolle – Weitergabekontrolle – Eingabekontrolle – Auftragskontrolle – Verfügbarkeitskontrolle – Verwendungszweckkontrolle – Organisationkontrolle)
- → Benutzen Sie Secure-E-Mail?
- → Haben Sie ein Notfallmanagement inklusive implementierter Desaster-Recovery-Strategie?
- → Arbeitet das Unternehmen in der Private Cloud?
- → Wo steht das Rechenzentrum? (Deutschland, Europa oder Übersee)?
- → Gibt es namhafte und qualifizierte Technikpartner?