Foto: Yabresse / Fotolia.com

Vertrauen ist gut, Kontrolle Pflicht

Einerseits bietet ein CRM in der Cloud viele Vorteile – so spart der webbasierte CRM-Zugriff Zeit und oft auch Kosten. Andererseits verunsichern die komplexen Anforderungen an Datenschutz und Datensicherheit potenzielle Anwender. Denn sie sind es, die in vielen Fällen haften.

Übersicht

Text _ Karsten Zunke

»Software verkauft sich über Vertrauen«, sagt Christian Fischer. Der Mitgründer und Geschäftsführer der Erfurter Tec-Art Group weiß, wovon er spricht. Als sein Unternehmen im Jahr 2004 ein Online-CRM-System an den Markt brachte, war es ein unbeschriebenes Blatt im webbasierten CRM-Markt. Doch seitdem geht es für die 18-köpfige-Firma steil bergauf. Im vergangenen Jahr wurde das CRM-Angebot des Unternehmens auf der Berliner Messe IT-Profits vom Publikum zur beliebtesten Cloud-Lösung Deutschlands gewählt und erst im vergangenen Monat hat man es bei dem Innovationspreis der Deutschen Telekom unter die Top-5 geschafft, die finale Platzierung stand zum Redaktionsschluss noch nicht fest. Für Vertrauen auf Kundenseite sorgt vor allem die Transparenz des CRM-Anbieters in Sachen Datenschutz und Datensicherheit, wofür die Thüringer erst kürzlich das Qualitätszertifikat »Trust in Cloud« vom Verband SaaS-Eco-System verliehen bekamen. Und Fischer sieht weiterhin großes Potenzial. »Kunden unterschätzen oft die Vielfältigkeit von CRM. Es ist heute weit mehr als ein Vertriebstool«, sagt Fischer. So könne die gesamte Kommunikation – in- und extern – heute über ein Cloud-CRM abgewickelt werden. Auch Marktforscher bescheinigen Cloud-basierten CRM-Lösungen eine vielversprechende Zukunft. Laut einer Studie des US-Marktforschungsunternehmens Saugatuck wird CRM noch mindestens bis zum Jahr 2016 zu den treibenden Kräften des Cloud-Computing gehören.

Bereits heute kommt demnach mehr als jede vierte CRM-Lösung aus der Cloud. Zum Ende des Jahres sollen CRM-Clouds weltweit einen Anteil von mehr als einem Drittel an allen CRM-Lösungen haben.

Auftraggeber in der Pflicht

Beim Cloud-basierten CRM wird mithilfe eines Webbrowsers auf eine CRM-Lösung im Internet zugegriffen. Die Vorteile liegen auf der Hand: kostspielige Installationen entfallen ebenso wie die Hardware-Wartung und die Software ist durch automatische Updates immer auf dem neusten Stand. Zudem haben Cloud-Anbieter gut geschultes Personal und können die eigenen Ressourcen sehr effizient einsetzen.

Insbesondere für mittelständische Unternehmen hierzulande sind Cloud-Lösungen attraktiv, da durch den Dienstleister auch die Sicherheitskosten auf viele Kunden verteilt werden und so auch hochprofessionelle Lösungen erschwinglich werden. Aber genau hier liegt auch die Brisanz. »Cloud-Services sind einfach einzukaufen. Datenschutzrechtliche Bewertungen werden dabei gern vergessen«, sagt Niels Lepperhoff, Geschäftsführer der Xamit Bewertungsgesellschaft. Der Düsseldorfer Dienstleister ist auf Datenschutz, Audits […

> acquisa.de/newsletter

Der acquisa-Newsletter informiert Sie regelmäßig über aktuelle Entwicklungen und Trends.

→ INFO **WAS SIE AUF DER CRM-EXPO 2012 ERWARTET**

Am 10. und 11. Oktober öffnet die CRM-expo in der Messe Essen ihre Pforten. Schwerpunkte der führenden Messe- und Kongress-Veranstaltung für die Themen Kundenbeziehungsmanagement und Neukundengewinnung sind diesmal der Datenschutz, die Verzahnung von Social Media und CRM sowie mobile Konzepte.

Inhaltlich reicht das Spektrum weit: von der Verknüpfung von Facebook mit CRM über die rechtskonforme Nutzung von Kundendaten bis hin zum I-Pad als Vertriebsinstrument. Mobile steht ebenfalls im Fokus: In der »mobile business area« werden Trends und Technologien, Services, Anwendungen und Best-Practices des mobilen Business vorgestellt.
Auch in diesem Jahr werden mit dem »CRM Best Practice Award 2012« wegweisende CRM-Umsetzungen ausgezeichnet. Prämiert werden Projekte in den Kategorien »CRM-Einführung« und »CRM-Weiterentwicklung«. Die Preise werden traditionell am ersten Abend der CRM-expo im Rahmen der »Award Night« verliehen.

Neben dem Bewährten wartet die CRM-expo in diesem Jahr mit zahlreichen Neuerungen auf. Als Brücke von der Forschung zur Wirtschaft fungiert der CRM-Campus mit einem Business-Dating mit Experten, dem Software-Praxis-Test oder dem Angebot »Jobs@CRM«. Parallel dazu haben die Veranstalter ein Loungekonzept in unterschiedlichen Ausprägungen entwickelt. Eine Trendlounge ist als Premium-Informations- und Networkingplattform konzipiert, die CRM-Beraterlounge als Kompetenz-Area.

und IT-Projekte spezialisiert. Xamit wird beratend tätig oder erfüllt die Funktion eines externen Datenschutzbeauftragten. Aus der Beratungspraxis kennen die Experten die Hürden für potenzielle Cloud-Anwender nur zu gut. Zum einen müssen Unternehmen einen Dienstleister finden, der zu ihren Anforderungen passt und zum anderen muss dieser die Daten auch datenschutzkonform verarbeiten können. »Letzteres ist leider nicht immer der Fall«, sagt Lepperhoff. Insbesondere wenn der Dienstleister mit Sub-Unternehmern arbeitet, dies aber vertuschen möchte, kann es auch schon mal durchaus sehr problematisch werden.

In diesem Zusammenhang ist es wichtig, zwischen Datensicherheit und Datenschutz zu unterscheiden. Die Datensicherheit beschreibt vor allem die Vertraulichkeit und Integrität der Daten sowie die Verfügbarkeit. Die Datensicherheit liegt insbesondere in der Verantwortung des Cloud-Anbieters. Dazu muss der Dienstleister viele Maßnahmen umsetzen, um unter anderem sicherzustellen, dass Unberechtigte die Daten nicht lesen, kopieren, ändern oder löschen können. Daher sind beispielsweise Zutritts-, Zugangs- und Zugriffskontrolle wichtige Aufgaben des Dienstleisters. Für den Datenschutz ist hingegen der Auftraggeber verantwortlich, also das Unternehmen, das ein CRM-Cloud-Angebot nutzen möchte.

Auftragenehmer genau prüfen

Seit mehr als zehn Jahren sind webbasierte CRM-Lösungen im Markt. Anfangs wurden sie als ASP, dann als On Demand oder »Software as a Service« (SaaS) vermarktet. Mittlerweile sind die Tools ausgereift, bieten vielfältigste Funktionen und die Serveranbindung ist – wenig verwunderlich – bedeutend schneller als vor zehn Jahren. Nahezu jeder CRM-Anbieter hat mittlerweile auch eine webbasierte Variante im Angebot. Bei vielen Lösungen ist sogar ein späterer Wechsel auf eine klassische Inhouse-Lösung möglich.
Ob eine im eigenen Unternehmen installierte CRM-Lösung auch sicherer ist als eine Cloud-Anwendung, lässt sich nicht pauschalisieren. Für Kleine und Mittlere Unternehmen (KMU) kann es ein Sicherheitsgewinn sein, weil sie unter Umständen weder das Personal noch die Mittel haben, um das hohe Sicherheitslevel eines großen Rechenzentrums zu erreichen. »Prinzipiell kann das gleiche Sicherheitsniveau auch mit eigenen Servern plus eigenem Personal erreicht werden. Allerdings meist zu höheren Kosten«, sagt Lepperhoff. Dem IT-Experten zufolge sollte jedes Unternehmen daher zunächst definieren, welche Leistungen ein Cloud-Service tatsächlich bieten soll – von Support über Backups bis hin zur Verfügbarkeit.

Rechtliche Aspekte beachten

Die wichtigste rechtliche Grundlage, um einen europäischen Dienstleister in die Datenverarbeitung personenbezogener Daten einzubinden, ist die sogenannte »Auftragsdatenverarbeitung« nach § 11 Bundesdatenschutzgesetz (BDSG). Darin werden konkrete Vorgaben in Bezug der technisch-organisatorischen Sicherung, zur Vertragsgestaltung sowie zu Weisungen und Kontrollen durch den Auftraggeber gemacht. Das Gesetz schreibt unter anderem bereits eine sorgfältige Dienstleister-Auswahl vor. »Bei einer Auftragsdatenverarbeitung ist der Auftragnehmer von einigen Datenschutzvorschriften freigestellt, da er datenschutzrechtlich wie ein Erfüllungsgehilfe behandelt wird. Der Auftraggeber hingegen haftet in vielen Fällen sogar für die Tätigkeit seines Auftragnehmers« erläutert Lepperhoff. Allerdings ist der Auftragnehmer auf dieser Gesetzesgrundlage weisungsgebunden. Das heißt, er darf nur auf Weisung des Auftraggebers handeln. Ignoriert der Dienstleister das Weisungsgebot, liegt die Verantwortung beim Dienstleister. Die Kontroll- und Aufsichtspflicht verbleiben aber stets beim Auftraggeber, also demjenigen Unternehmen, welches die Cloud nutzt.
Etwas komplizierter wird es, sobald ein nicht-europäisches Unternehmen als Cloud-Dienstleister gewählt werden soll, denn eine Auftragsdatenverarbeitung gemäß Bundesdatenschutzgesetz ist nur mit Anbietern im Europäischen Wirtschaftsraum (EWR) erlaubt. »Aber auch eine solche Datenverarbeitung lässt sich rechtlich sauber regeln. CRM in der Cloud ist juristisch komplex, aber keineswegs problematisch«, erläutert Kai Westerwelle. Der erfahrene Fachanwalt für Informationstechnologierecht ist Partner in der Wirtschaftskanzlei Taylor Wessing in Frankfurt am Main.

Was passiert außerhalb Europas?

Um personenbezogene Daten in nicht-europäische Länder zu exportieren, wurden die sogenannten EU-Standardvertragsklauseln als Rechtsgrundlage eingeführt. Sie müssen zusätzlich zum Vertragswerk zwischen Auftraggeber und Auftragnehmer abgeschlossen werden. »Auf diese Weise wird für weltweit agierende Anbieter ein Datenschutzniveau erzeugt, das dem europäischen ebenbürtig ist«, erläutert Westerwelle. Auch für den Fall, dass ein europäischer CRM-Dienstleister mit Drittunternehmen in Nicht-EWR-Ländern zusammenarbeitet, sind Westerwelle zufolge die EU-Standard-Vertragsklauseln die geeignete datenschutzrechtliche Grundlage – beispielsweise bei einem sogenannten Follow-The-Sun-Support, bei dem Anwender von einem global aufgestellten Support-Team unterstützt werden – jeweils aus dem Land, in dem es gerade Tag ist und regulär gearbeitet wird. »In solchen Fällen muss der europäische Cloud-Dienstleister mit seinen außereuropäischen Unter-Auftragnehmern die EU-Standardvertragsklauseln abschließen. Indem ein Netz aus EU-Standardvertragsklauseln über die verschiedenen Kooperationspartner gelegt wird, lässt sich mit diesem Instrument die Auftragsdatenverarbeitung in einer internationale Cloud rechtssicher gestalten«, erläutert Westerwelle. Wenn ein Unternehmen einen Cloud-CRM-Dienstleister wählt, der nicht nur im EWR tätig ist, sollte sich der Auftraggeber vom Dienstleister daher stets nachweisen lassen, dass dieser auch in diesen Ländern datenschutzrechtskonform arbeitet und entsprechende EU-Standard-Vertragsklauseln abgeschlossen wurden.
»In vielen Fällen ist dies jedoch gar nicht nötig, da auch internationale Cloud-Anbieter mittlerweile lokal begrenzte Clouds anbieten – beispielsweise rein europäische Clouds, an denen nur Unternehmen aus EWR-Ländern involviert sind«, sagt Westerwelle. Denn eine Cloud kann in der Regel immer so gestaltet werden, wie der Anwender sie benötigt – sogar so, dass die Datenverarbeitung ausschließlich in Deutschland erfolgt.
Mit den USA hat die EU noch eine gesonderte Datenschutzvereinbarung getroffen – das sogenannte Safe-Harbor-Abkommen. US-Unternehmen können Safe Harbor beitreten, indem sie sich zur Einhaltung der in Safe Harbor festgeschriebenen Grundsätze verpflichten. Doch deutsche Datenaufsichtsbehörden halten dies nicht für ausreichend, weil sich US-Unternehmen auf diese Weise quasi selbst zertifizieren. Der Düsseldorfer Kreis – ein Zusammenschluss der obersten deutschen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich – hat bereits darauf hingewiesen, dass sich Auftraggeber nicht auf die Aussage einer Safe-Harbor-Zertifizierung verlassen dürfen, sondern nachweisen müssen, dass die Zertifizierung tatsächlich vorliegt und deren Grundsätze auch eingehalten werden. Zusätzliche Brisanz erfährt das Thema durch den sogenannten Patriot Act, der es US-Sicherheitsbehörden unter bestimmten Umständen erlaubt, auf die von US-Unternehmen gespeicherten Daten zuzugreifen, ohne die Dateninhaber darüber zu informieren.

› acquisa.de
ONLINE-SEMINAR:
»Cloud Computing«
Die rechtlichen Anforderungen einer Auftragsdatenverarbeitung sind schwer zu erfüllen. Was in der Cloud zu beachten ist.
Termin: 11.12.2012

Big Brother is watching you

»Wenn US-Behörden auf Grundlage des Patriot Acts oder eines anderen US-Gesetzes auf Kundendaten in Deutschland oder Europa zugreifen wollen, ist das US-Unternehmen […

»PRINZIPIELL KANN DAS GLEICHE SICHERHEITSNIVEAU AUCH MIT EIGENEN SERVERN PLUS EIGENEM PERSONAL ERREICHT WERDEN. ALLERDINGS MEIST ZU HÖHEREN KOSTEN.«
NIELS LEPPERHOFF, Geschäftsführer Xamit Bewertungsgesellschaft, Düsseldorf

nach US-Recht verpflichtet, die Daten herauszugeben. Nach deutschem Recht darf es die Daten in vielen Fällen nicht herausgeben. Das Unternehmen darf nun wählen, welches Recht es bricht«, erläutert Lepperhoff das juristische Dilemma.
Nach Ansicht von Westerwelle wird diese Problematik aber oft überbewertet »Im Rahmen des Patriot-Act dürfen US-Behörden nur mit richterlicher Zustimmung auf die Daten zugreifen. Ähnliche Reglungen gibt es fast überall auf der Welt.« So könne auch hierzulande ein deutsches Unternehmen mit deutschem Rechenzentrum durch einen richterlichen Beschluss dazu verpflichtet werden, Daten herauszugeben. »Das ist gängige Praxis und passiert nahezu täglich«, so Westerwelle.
Vor allem US-Unternehmen wie die CRM-Anbieter Salesforce.com oder Microsoft sind um Aufklärung bemüht, wollen Vorbehalte ausräumen. Beide Firmen machen im Internet ihre Datenschutz-Bemühungen sehr transparent und öffentlich. Microsoft hat zudem erst kürzlich die EU-Standardvertragsklauseln in seine Cloud-CRM-Lösung integriert.

»CRM IN DER CLOUD IST JURISTISCH KOMPLEX, ABER KEINESWEGS PROBLEMATISCH.«

KAI WESTERWELLE, Fachanwalt für Informationstechnologierecht, Partner bei Taylor Wessing, Frankfurt am Main

Die Verunsicherung hält an

Auf Grund der generellen juristischen Komplexität der Thematik ist die Verunsicherung bei der Dienstleisterwahl zwischen Flensburg und Füssen aber nach wie vor groß, vor allem im Mittelstand. »Entsprechend des Bundesdatenschutz-Gesetzes liegt die Verantwortung für Daten bei den Kunden. Diese sind per Gesetz verpflichtet, sich vor Vertragsabschluss über die Zuverlässigkeit von Dienstleistern kundig zu machen – ein Anspruch, dem mangels erforderlicher IT-Kenntnisse nur die wenigsten mittelständischen Kunden nachkommen können«, erläutert Bernd Becker, Vorstandssprecher von Eurocloud Deutschland_eco. Als Verband der Cloud Computing Wirtschaft am Marktplatz Deutschland ist das erklärte Ziel, die Akzeptanz und das Vertrauen der Anwender in Cloud Computing zu stärken. Mit seinem Zertifikat, dem Eurocloud Star Audit, möchte der Verband den Cloud-Kunden bei der Dienstleisterwahl eine Entscheidungshilfe geben. Zwar gibt es in der IT bereits zahlreiche hochwertige Zertifizierungen – von der ISO 27001 über ITIL bis hin zu Combit. Doch Cloud-spezifische Gegebenheiten und Risiken werden von diesen Zertifizierungen nicht erfasst. Das Eurocloud Star Audit wurde hingegen speziell für Software as a Service (SaaS)-Dienstleistungen entwickelt. Neben den Sicherheitsanforderungen werden auch Vertrag und Compliance inklusive Datenschutz, Betrieb und Infrastruktur, Betriebsprozesse bis hin zur Anwendung und Implementierung überprüft. Je nach erreichtem Leistungsgrad werden ein bis fünf1 bis Sterne vergeben.
Neben der Eurocloud-Zertifizierung gibt es noch weitere Cloud-Zertifikate im Markt. Doch deren Aussagekraft ist häufig begrenzt, da viele Zertifizierer ihre Kriterien nicht veröffentlichen. Daher können potenzielle Auftraggeber die Aussagekraft und den Nutzen des Zertifikats oft nicht einschätzen. Es werden deshalb zusätzliche Kontrollen durch den Auftraggeber nötig. »Die Eurocloud-Zertifizierung hingegen ist transparenter, und sie ist ein Schritt in die richtige Richtung. Nichtsdestotrotz gibt es aktuell keine Norm, welche die datenschutzrechtlichen Anforderungen im Cloud-Betrieb festlegt«, sagt Lepperhoff. Im Unterschied zur IT-Sicherheit mit der ISO 27001 fehle dafür ein anerkannter Standard.
»Rechtliche Unsicherheiten um Datenexport in sogenannte unsichere Drittstaaten, Unklarheiten ob Safe Harbor tatsächlich ein sicherer Hafen ist und die Diskussion um den Patriot Act haben auch unsere Kunden und Interessenten erreicht«, sagt etwa Hansjörg Schmidt, Marketing- und Vertriebs-Chef des deutschen Cloud-CRM-Anbieters Wice in Hamburg. Das Wice-System ist ausschließlich in Deutschland gehostet und unterliegt den strengen deutschen Datenschutzbestimmungen. Mit diesem Argument habe man sogar schon amerikanische Kunden gewinnen können, sagt Schmidt. Während Wice-Kunden früher hauptsächlich nach dem Sicherheitskonzept des CRM-Anbieters fragten, gehen Schmidt zufolge die Fragen nun eher in Richtung rechtlicher Compliance und dem Ort der physikalischen Datenspeicherung. »Jetzt«, sagt Schmidt, »kommt der über die Landesgrenzen anerkannte deutsche Datenschutz als Standortvorteil daher.«
redaktion@acquisa.de

> twitter.com/acquisa
Hier twittert die Redaktion acquisa Aktuelles und Wissenswertes aus der Marketingwelt.

→ CHECKLISTE AUGEN AUF BEI DER DIENSTLEISTERWAHL

Wenn Sie einen Cloud-Dienstleister für Ihre CRM-Daten wählen, sollten Sie darauf achten, dass dieser auch die Datensicherheit gewährleistet. Dafür muss der Dienstleister sorgen:

→ **Zutrittskontrolle.** Unbefugte dürfen keinen Zutritt zu den Datenverarbeitungsanlagen haben.

→ **Zugangskontrolle.** Der Dienstleister muss dafür sorgen, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden.

→ **Weitergabekontrolle.** Während Transport, Übertragung oder Speicherung dürfen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

→ **Auftragskontrolle.** Die Daten dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

→ **Zugriffskontrolle.** Nur Berechtigte dürfen auf die Daten zugreifen.

→ **Eingabekontrolle.** Es muss nachträglich überprüfbar sein, ob und von wem personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

→ **Verfügbarkeitskontrolle.** Persönliche Daten müssen gegen zufällige Zerstörung oder Verlust gesichert sein.

→ **Trennungskontrolle.** Es muss gewährleistet sein, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden können.

Diese Punkte können nur als Anhalt dienen. Die detaillierten Anforderungen sind im Bundesdatenschutzgesetz (BDSG) geregelt. Der §9 BDSG und seine Anlage zu Satz 1 regeln, wie die innerbetriebliche Organisation zu gestalten ist und welche Maßnahmen zu treffen sind, wenn personenbezogene Daten automatisiert verarbeitet oder genutzt werden.