Advertorial

Software as a Service: Cloud-Lösungen trotz Datenschutzdiskussionen auf dem Vormarsch

Cloud-Lösungen im Projektmanagement sind weiterhin im Kommen. Doch gleichzeitig trüben Berichte über mangelnde IT-Sicherheit das Vertrauen in die externe Datenhaltung. Im Oktober dieses Jahres verlor die USA offiziell ihren Status als "Safe Harbor" und damit ist infrage gestellt, ob und wie personenbezogene Informationen, aber auch andere Daten dort noch gespeichert werden können und sollten. Kay-Eric Hirschbiegel ist Geschäftsführer der deutschen Sciforma GmbH, die "Software as a Service" (SaaS) anbietet. Da kommen alle Anwendungen aus der Cloud und auch die Projektdaten werden dort gespeichert. Wie erlebt er die aktuelle Diskussion und welche Sicherheitsstrategie empfiehlt er Cloud-interessierten Unternehmen?

Herr Hirschbiegel, haben die jüngsten Diskussionen über die IT-Sicherheit externer Speicherangebote Kunden und Interessenten für diese Cloud- bzw. SaaS-Lösungen verunsichert?

Ja, eine gewisse Verunsicherung ist spürbar. In Deutschland wird das Thema Datenschutz sehr ernst genommen. Die Herausforderung dabei ist, den Betrieb der IT-Lösungen und das Thema Datenschutz so auszubalancieren, dass die Sicherheit gewährleistet ist, aber die IT-Prozesse nicht die Geschäftsabläufe blockieren.

In der Safe-Harbor-Entscheidung urteilte der Europäische Gerichtshof, dass personenbezogene Daten nach dem hier gültigen Datenschutz-Verständnis in den USA nicht ausreichend geschützt werden. Was bedeutet das denn nun genau für Betreiber und Nutzer von Cloud-Lösungen?

Darüber herrscht aktuell viel Unsicherheit. Darf man Google noch als E-Mail-Provider haben? Ist der weltweit größte Cloud-Anbieter, Amazon, noch ein zulässiger Partner für Unternehmen in Deutschland und Europa? Wir warten noch auf offizielle Empfehlungen, wie wir uns als Hersteller und Dienstleister verhalten sollen. Aussagen dazu vom Bundesamt für die Sicherheit in der Informationstechnik BSI könnten hilfreich sein, werden aber frühestens ab Ende des ersten Quartals 2016 erwartet. Tragfähige offizielle Handlungsempfehlung gibt es generell nur für personenbezogene Daten. Dabei können in projektbezogenen Daten ja durchaus schützenswerte Informationen stecken, etwa Patente, Strategien oder Kundendaten. Hier bewegen wir uns in dem großen Themenfeld IT-Security, zu dem offizielle Datenschutzrichtlinien keine Regelungen vorgeben.

Kay-Eric Hirschbiegel

Dipl. Ing. Kay-Eric Hirschbiegel ist Geschäftsführer der Sciforma GmbH. In der selben Funktion hatte er bereits das Vorgängerunternehmen Le Bihan Consulting GmbH aufgebaut und geleitet. Er verfügt über mehr als 20 Jahre Erfahrung im Bereich PPM-IT-Lösungen.

Wir selbst haben aus der Safe-Harbor-Entscheidung die Konsequenz gezogen, dass wir unseren deutschen Kunden grundsätzlich anbieten, ihre Daten auch in Deutschland zu speichern – obwohl wir mit Sciforma.net eine kostengünstige internationale SaaS-Plattform haben. So wie früher eigene Hardware hinzustellen ist für uns und erst recht für unsere Kunden definitiv keine attraktive Option mehr. Wir verantworten den Betrieb, die Rechenleistung kaufen wir ein. Und der Kunde entscheidet, an welchem Ort dieser Welt die Daten gehostet werden.

Um welche Probleme geht es eigentlich? Wovor wollen die Kunden ihre Daten schützen?

Unsere Kunden wollen, wie bereits erwähnt, zum einen die Einhaltung der Datenschutzbestimmungen zu personenbezogenen Daten gewährleisten, wobei im Projektmanagement allerdings in der Regel keine brisanten Informationen, wie etwa Gesundheitsdaten, anfallen. Zum anderen geht es um die Abwehr von Industriespionage und da fallen in vielen Projekten tatsächlich schützenswerte Daten an, die einen hohen Wert für das Unternehmen darstellen.

Erwarten Sie, dass sich der Trend zu SaaS-Lösungen umkehrt und die Firmen ihre Projektdaten wieder zunehmend im eigenen Haus haben wollen?

Nein, dazu sind die Cloud-Angebote zu attraktiv. Der große Vorteil einer SaaS-Lösung ist die hohe Flexibilität. Der Kunde muss nicht investieren, sondern rechnet die Nutzung der PM-Software z. B. auf monatlicher Basis als laufenden Kosten ab. Die Lösung kann innerhalb einer Stunde produktiv eingesetzt werden, um den Betrieb kümmern wir uns als Dienstleister, wobei die vereinbarten Service-Level hohe Zuverlässigkeit gewährleisten. Auf sich ändernde Anforderungen kann man sehr schnell reagieren. Das System ist problemlos skalierbar, etwa wenn am Freitagnachmittag durch Erfassung der IST-Daten oder um einen Periodenwechsel herum eine weit höhere Rechnerleistung benötigt wird. Natürlich ist es wichtig, dass sich der Serviceanbieter um die Einhaltung des Datenschutzes kümmert. Wir selbst beschäftigen uns sehr intensiv mit diesem Thema und ziehen zudem regelmäßig eine renommierte Expertin hinzu, die unsere Aktivitäten begutachtet und uns in allen Dingen der Datensicherheit berät.

Wie gut sind Ihre Kunden denn erfahrungsgemäß zum Thema Datenschutz aufgestellt?

Alle Firmen haben zumindest eine Datenschutzrichtlinie zum Thema personenbezogener Datenschutz. Hinsichtlich einer durchgängigen IT-Datenschutz-Policy sieht es schon anders aus. Oft ist beispielsweise unklar, welche Projektdaten wir und andere sehen und speichern dürfen. Obwohl wir für alle Kundenbeziehungen eine Verschwiegenheitserklärungen (NDA) unterzeichnen, wundern wir uns doch immer wieder, auf welche Daten wir manchmal Zugriff haben und wie Kunden auch intern damit umgehen. Weniger häufig erleben wir auch das Gegenteil: Größere Organisation habe teilweise ziemlich umfangreiche Regelwerke mit massiven Einschränkungen. Das geht bis hin zu einem extrem strengen Datenschutz, der einen normalen Betrieb kaum mehr zulässt.

Würden Sie dazu ein Beispiel geben?

Wenn eine Firma sich beispielsweise auf den Standpunkt stellt: "Unsere Projektdaten dürfen nie unser Haus verlassen." Dann haben wir ein Problem im Supportfall, denn oft brauchen wir die Daten, um den aufgetretenen Fehler zu reproduzieren. Das klappt nicht mit einer leeren Datenbank. Eine Lösung kann dann darin bestehen, dass wir mit der Datenbank arbeiten, bis der Fehler behoben ist. Dann wird sie wieder gelöscht und die Löschung bestätigt. Zudem erhöhen wir die Sicherheit dadurch, dass wir eine quasi gekapselte Support-Plattform betreiben, auf der wir Fehler nachstellen und reproduzieren. Hier arbeiten wir auch mit verschlüsselten Daten, der Kunde ist im Support-Prozess eingebunden und bleibt Herr über die Daten. Wenn auch das nicht akzeptiert wird, müssen wir bei Problemen einen Mitarbeiter persönlich zum Kunden schicken – eine aufwendige und kostspielige Lösung. Unternehmensintern sind die Bereiche IT Security und Betrieb klassische Gegenspieler. Die einen wollen "Fort Knox", die anderen einen reibungslosen einfachen Betrieb realisieren.

Welche Strategie empfehlen Sie SaaS-Kunden, um die Projektdaten zu schützen?

Die eine perfekte Lösung für alle gibt es nicht. Die Anforderungen an den Datenschutz hängen zunächst davon ab, um welche Informationen es in den Projekten geht. Erfindungen und Patente eines technologischen Weltmarktführers erfordern natürlich einen anderen Schutz als die Planungsdaten eines Bauträgers, die sowieso von Dutzenden Firmen eingesehen werden.

Auf jeden Fall empfehlen wir eine Datenverschlüsselung, die über das sogenannte https-Protokoll hinausgeht. Das heißt, nicht nur der Weg sollte gesichert sein, die Projektdaten sollten auch verschlüsselt gespeichert werden. Ein solches Vorgehen gewährleistet bereits einen guten Datenschutz im täglichen Arbeiten. Wobei hier die sichere Lagerung des Schlüssels nicht vergessen werden darf: Es gilt, den Zugang professionell zu administrieren, die Schlüssel regelmäßig zu ändern etc.

Generell ist das größte Risiko weiterhin näher als man denkt – die eigenen Mitarbeiter. Die Anwendung mit dem größten Gefährdungspotenzial, dass Daten in falsche Hände gelangen können, ist die E-Mail. Doch das hat mit SaaS erst mal nichts zu tun, das ist ein generelles Thema der IT-Sicherheit. Hier sollte das Management dafür sorgen, dass ihr Unternehmen Kompetenz aufbaut, und klare Richtlinien vorgeben.

Ihr Fazit für Unternehmen, denen die Sicherheit ihrer Projektdaten am Herzen liegt. Ist SaaS eine gute Option?

Ich denke, die Cloud-Lösungen hinsichtlich Betrieb und Kosten sind so attraktiv, dass langfristig kaum einer darauf verzichten wird. Ob Microsoft oder SAP – alle Big Player gehen diesen Weg und es ist eher eine Frage der Zeit, bis die gesamte Abwicklung der Geschäftsprozesse IT-seitig in der Cloud beheimatet sein wird. Hinsichtlich Sicherheit sind die meisten Hersteller bereits mit professionellen Angeboten am Markt. Die Verschlüsselungs-Algorithmen sind weit fortgeschritten. Sofern Unsicherheit hinsichtlich der Speicherung von Daten in bestimmten Regionen herrscht, haben Unternehmen die Möglichkeit, sich für eine rein deutsche Datenhaltung zu entscheiden. In dieser Thematik ist viel Bewegung und es wird zukünftig keinen vernünftigen Grund mehr geben, den Betrieb im eigenen Haus zu halten.

Herr Hirschbiegel, Danke für das Gespräch.

Kontakt:
Sciforma GmbH, Heinrich-Hertz-Straße 2, 65232 Taunusstein Telefon +49 6128 9665-0, Fax +49 6128 9665-11,
info@sciforma.de, www.sciforma.com