Rollout intelligenter Messsysteme

Risiken und Chancen durch Cloud-Lösungen und IT-Outsourcing

Bei der Umsetzung der vielfältigen Anforderungen aus dem Messstellenbetriebsgesetz geht es nicht nur um die Anpassung einzelner Systeme. Vielmehr ist zu prüfen, wie die neuen Vorgaben in der IT-Architektur abgebildet werden können. Dafür müssen die einzelnen Anforderungen und Risiken detailliert geprüft und deren Umsetzung in die gesamte IT-Architektur definiert werden. Nur so wird es möglich, Transparenz zu erhalten und Risiken zu beherrschen.

Um herauszufinden, wie die neuen Anforderungen aus dem Messstellenbetriebsgesetz (MsbG) in die IT-Architektur implementiert werden können, ist zunächst zu analysieren, welche Bereiche der Architektur grundsätzlich betroffen sind. Die aus der Umsetzung des Interimsmodells und der Anpassung des Datenmodells auf Markt- und Messlokation folgenden Anpassungen werden sich bei den meisten Unternehmen hauptsächlich auf Änderungen in den bestehenden Abrechnungssystemen beschränken.

Die Einführung intelligenter Messsysteme erfordert dagegen vollständig neue Funktionen und Systeme, die bisher in den IT-Landschaften noch nicht abgebildet sind: Systeme zur Gatewayadministration, zum Messdatenmanagement (MDM), zur Verwaltung intelligenter Messsysteme und nicht zuletzt zur Abrechnung des Messstellenbetriebs gegenüber Lieferanten und Endkunden (*Bild 1*).

Der Gedanke liegt nahe, an diesen Stellen die Wirtschaftlichkeit von On-Premise-Lösungen im eigenen Rechenzentrum zu hinterfragen und das Outsourcing der Systeme oder den Einsatz einer Cloudlösung zu prüfen. Dafür sprechen die voraussichtlich schnellere Implementierung und die einfache Skalierbarkeit, die vor allem für wettbewerbliche Messstellenbetreiber (MSB) interessant sind. Auch die einfache und direkte Zuordnung der entstehenden Kosten in den getrennt auszuweisenden Bereich des grundzuständigen Messstellenbetriebs sind Argumente für eine Auslagerung.

Doch außer den Chancen gibt es auch die Risiken, die im Folgenden ausführlich dargestellt werden. Unternehmen, die den Einsatz von Cloudlösungen erwägen, sollten die genannten Aspekte detailliert prüfen und im Rahmen der Entscheidung für die IT-Architektur bewerten. Im Einzelnen sind das:

- Verantwortung für Systeme und Daten
- IT-Sicherheit
- Datenschutz gemäß EU-Datenschutzgrundverordnung (DSGVO)
- Zugriffssteuerung
- rechnungslegungsrelevante Prozesse und Funktionen.

Verantwortung für Systeme und Daten

Wichtig ist es, die Verteilung der Aufgaben und Verantwortungen im Rahmen eines Outsourcings oder beim Einsatz einer Cloudlösung genau zu klären.

Die Verteilung der Aufgaben bei der Auslagerung sowie der Nutzung einer Cloudlösung, also die Beantwortung der Frage »Wer macht künftig was?«, ist nicht problemlos, aber ein strukturiert lösbarer Prozess. Aufgaben und Zuständigkeiten sind in den Verträgen zwischen Auftraggeber und Auftragnehmer mög-

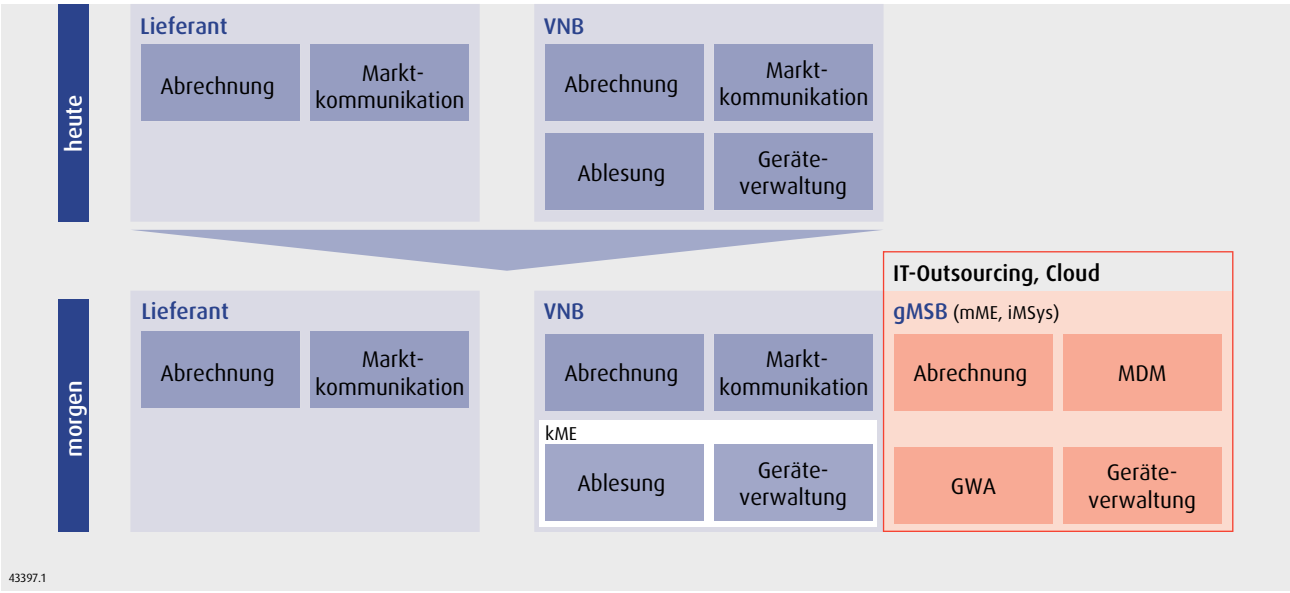

Bild 1. Erweiterung der Kernsystemlandschaft und Möglichkeiten der Auslagerung am Beispiel gMSB

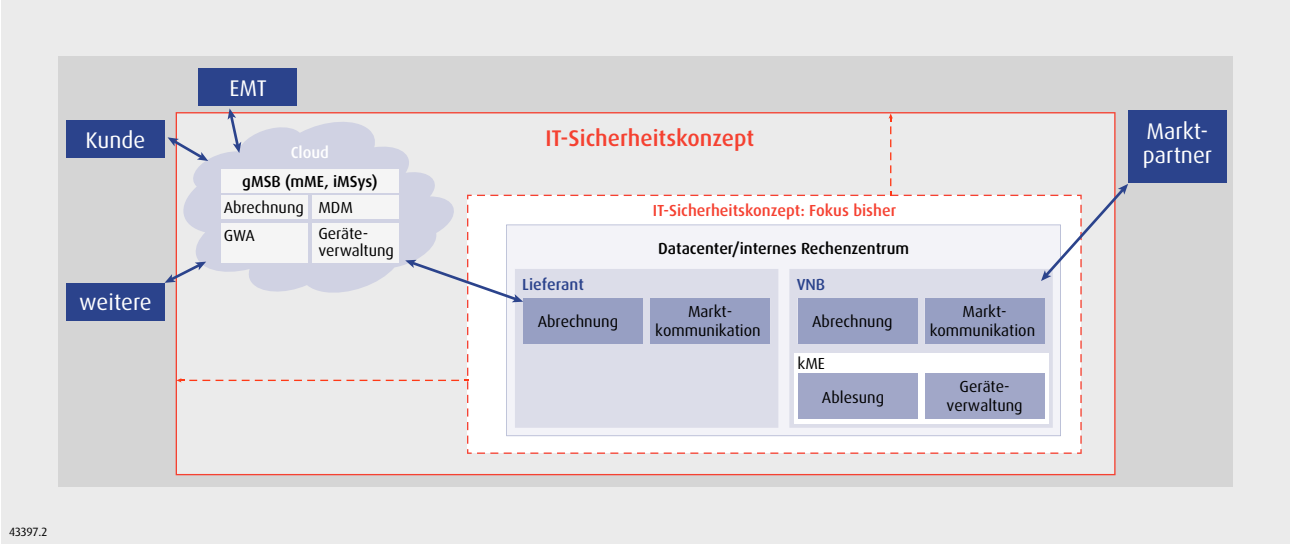

Bild 2. Erweiterung der Sicherheitsbetrachtungen auf Cloud-Lösungen

lichst vollständig und widerspruchsfrei zu regeln, um im operativen Betrieb die Prozessabwicklung und den Systembetrieb reibungslos zu gestalten.

Außerdem ist zu klären, wer für die korrekte und sichere Verarbeitung der Daten verantwortlich ist. Hierfür sind zwei Aspekte zu beachten: der Datenschutz für personenbezogene Daten (BDSG, DSGVO) und die Grundsätze ordnungsmäßiger Buchführung für rechnungslegungsrelevante Prozesse und dazugehörige Daten. Liegen solche Daten vor, verbleibt die Verantwortung für die Daten auch im Fall von IT-Outsourcing oder der Nutzung von Cloudlösungen zwingend beim Auftraggeber.

IT-Sicherheit

Ist die Verantwortung für Systeme und Daten geklärt, stellt sich die Frage nach den Erfordernissen einer übergreifenden IT-Sicherheit. Grundsätzlich ist festzustellen, dass die Methoden und Strukturen zur Gewährleistung der IT-Sicherheit ganzheitlich betrachtet werden müssen.

Nicht mehr nur die eigenen Assets sind Gegenstand der Sicherheitsüberlegungen, sondern auch die ausgelagerten Systeme und Daten. Wie weit sich die Betrachtungen über die eigenen Unternehmensgrenzen hinweg ausdehnen, ist abhängig von der Gestaltung der Auslagerung. Die vollständige Betrachtung bei einer On-Premise-Lösung reicht dabei von physischer Zutritts- und Zugriffsüberwachung über Applikationsmanagement bis zum Identity-Management und zur Datenverantwortung. Dagegen genügt bei einem Software-as-a-Service-Angebot die Fokussierung auf Daten und das Zugriffsmanagement der Clients.

Auf jeden Fall sind die ausgelagerten Bestandteile der IT-Architektur in die Betrachtungen des Information-Security-Management-Systems (ISMS, zum Beispiel nach DIN ISO 27001) einzubeziehen. Die Analyse und Bewertung der Risiken, die im Rahmen eines ISMS stattfinden müssen, sind auszudehnen, um die erweiterten Risiken zu erkennen, die durch eine Auslagerung von Teilen der IT entstehen. Dabei ist es – auch mit Blick auf die ausgelagerten Systeme und Applikationen – empfehlenswert, die Bewertung der Risiken und die entsprechende Definition von Gegenmaßnahmen mit Fokus auf die Ausfallfolgen für die Geschäftstätigkeiten vorzunehmen. Ebenso muss die Überwachung der Systeme und Applikationen, die üblicherweise organisatorisch und technisch an einer zentralen Stelle gebündelt stattfinden sollte, die

ausgelagerten Bestandteile der IT-Architektur so einbeziehen, dass die im Verantwortungsbereich des auslagernden Unternehmens liegenden Risiken mit überwacht werden.

Entscheidend für die Überlegungen zur IT-Sicherheit ist in jedem Fall der Schutz der gespeicherten und verarbeiteten Daten. Neben den Regelungen für die Speicherung der Daten und zum Zugriff darauf ist aus IT-Sicherheitsaspekten die Verschlüsselung bei Übertragung und eventueller Speicherung sicherzustellen, vor allem bei Unklarheit über den physischen Ort der Speicherung. Zu beachten ist hierbei, dass die Hoheit über die Verschlüsselung im auslagernden Unternehmen bleiben sollte.

Datenschutz gemäß DSGVO

Der Schutz der gespeicherten und verarbeiteten Daten bleibt, sofern es sich um personenbezogene Daten im Sinne der DSGVO handelt, unabhängig von der Ausprägung des IT-Outsourcings oder der Cloudnutzung im Aufgaben- und Verantwortungsbereich des auslagernden Unternehmens. Außer der Einhaltung der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten Datenschutz- und Datensicherheitsstandards für Smart-Meter-Gateways ist der Schutz der Daten in den Systemen und den sich anschließenden Prozessen (zum Beispiel MDM, Abrechnung des Messstellenbetriebs) sicherzustellen. Das gilt sowohl für On-Premise-Lösungen als auch für (Teil-)Auslagerungen.

Auch hier ist wieder eine Ausdehnung des Betrachtungsbereichs vom eigenen Rechenzentrum auf die externen Bestandteile der IT-Architektur notwendig (*Bild 2*). Es muss für alle eingesetzten Applikationen sichergestellt sein, dass die im Zusammenspiel der Festlegungen des Messstellenbetriebsgesetzes und der DSGVO geforderten Schutzmaßnahmen für Daten beachtet werden. Hier sind vor allem die Prüfung der Rechtmäßigkeit der Datenverarbeitung, die Forderung nach Anonymisierung und Pseudonymisierung, die Pflicht zur Löschung personenbezogener Daten sowie das Recht auf Auskunft über die gespeicherten Daten und deren Löschung zu nennen.

Der Auftraggeber muss bei einer Auslagerung der IT durch entsprechende Verträge, Nachweise oder Zertifizierungen (zum Beispiel nach ISO 27018) dafür sorgen, dass diese Regelungen vom Auftragnehmer und den eingesetzten Subdienstleistern eingehalten werden.

Zugriffssteuerung

Um einen umfassenden Schutz der Daten zu gewährleisten, muss der geregelte und gesteuerte Zugriff auf die Daten definiert werden. Darunter ist einerseits die Betrachtung und Definition des grundsätzlich berechtigten Nutzerkreises zu verstehen (Identity Management), andererseits die Definition, die Zuweisung und der Entzug detaillierter Berechtigungen zur Ansicht und Änderung bestimmter Daten (Access Management).

Ausgelagerte Applikationen sind bereits beim Design der Businessrollen, das heißt der Definition des für eine Rolle im Unternehmen notwendigen Zugriffsberechtigungsbündels, übergreifend und zusammen mit den On-Premise-Applikationen zu berücksichtigen. Eine Identity- und Access-Management-Lösung bietet hier die Möglichkeit, über vielfältige Schnittstellen sowohl interne als auch externe Applikationen anzubinden und die zugewiesenen Berechtigungen gesamtheitlich und effizient je Rolle zu verwalten. Zusätzlich unterstützt ein Reporting über existierende Identitäten und zugewiesene Zugriffsrechte den Nachweis über die Einhaltung interner und externer Compliance-Regeln.

Hinsichtlich der Zugriffssteuerung ist es wichtig, dass die Entscheidung über eine Rechtevergabe und deren Genehmigung in der Hand des auslagernden Unternehmens bleiben muss. Zumindest müssen ausreichende Regeln und Kontrollinstanzen implementiert sein, die eine unkontrollierte Rechtevergabe durch externe Dienstleister verhindern. Ebenso ist die Vergabe privilegierter Rechte (Privileged Access Management, PAM), zum Beispiel von Administrationsrechten, eng zu reglementieren und zu überwachen oder auf interne Mitarbeiter zu beschränken.

Rechnungslegungsrelevante Prozesse und Funktionen

Die gesetzlichen Ordnungsmäßigkeitsanforderungen – vor allem die Beachtung der Grundsätze ordnungsmäßiger Buchführung – gelten uneingeschränkt auch bei der Auslagerung der IT für rechnungslegungsrelevante Prozesse und Funktionen. Dieser Bereich kann beim Rollout intelligenter Messsysteme durchaus relevant sein, nämlich bei der Erhebung, Speicherung und Verarbeitung von Messwerten als Grundlage der Rechnungslegung oder im Fall der Abrechnung des Messstellenbetriebs.

Hier gilt, dass die Verantwortung für die Ordnungsmäßigkeit rechnungslegungsrelevanter Prozesse und Daten beim auslagernden Unternehmen bleibt. Neben vielfältigen weiteren Anforderungen und Risiken besteht vor allem auch die Pflicht zur Aufbewahrung von Unterlagen – unter den Aspekten Anforderung für die Dokumentation, Dauer der Aufbewahrung und Unveränderlichkeit der Unterlagen –, zur Gewährleistung von Datenzugriffen externer berechtigter Dritter und zur Dokumentation der Verfahren. Dies gilt unabhängig davon, ob die notwendigen IT-Dienstleistungen intern oder extern erbracht werden.

Zur Einhaltung der Ordnungsmäßigkeitsanforderungen muss der Prozess der Auslagerung strukturiert geplant und umgesetzt werden. Einer detaillierten Analyse der mit der Auslagerung verbundenen Risiken müssen die Definition geeigneter Kontrollmaßnahmen und die Aufteilung der Pflichten, Prozesse und Kontrollen zwischen auslagerndem Unternehmen und Dienstleister folgen. In diesem Zusammenhang ist auch festzulegen, ob die Kontrollen vom auslagernden Unternehmen oder vom Dienstleister durchgeführt werden. In letzterem Fall muss das auslagernde Unternehmen wiederum prüfen, ob die Kontrollen korrekt durchgeführt und dokumentiert wurden.

Fazit

In jedem der angesprochenen Bereiche müssen die einzelnen Anforderungen und Risiken detailliert geprüft werden. Auf dieser Basis ist für die gesamte IT-Architektur – interne und externe Bereiche – zu definieren, wie die einzelnen Anforderungen umgesetzt und Kontrollmechanismen installiert werden. Nur so ist es möglich, Transparenz zu erhalten und Risiken zu beherrschen.

Andreas Woelke,
Senior Manager,
PKF Fasselt Consulting GmbH,
Duisburg

>> andreas.woelke@pkf-consulting.de

>> www.pkf-consulting.de

43397