Migration in die Cloud – ohne Regulatorik geht nichts

Jens Borchers
Sopra Steria Consulting Hamburg
Email: jens.borchers@soprasteria.com / jensborchers@acm.org

Abstract: *Die Nutzung von Cloud-Architekturen – ob nun unternehmensintern („private cloud“) oder zunehmend auch bei entsprechenden Service-Unternehmen („public cloud“) – wird immer mehr zu einer gängigen Methode, IT-Leistungen zu virtualisieren und bei externen Anbietern zu betreiben. Neben den technischen und fachlichen Aspekten spielen auch viele rechtliche Bedingungen eine wesentliche Rolle, gerade für Unternehmen im Finanzdienstleistungsbereich, also Banken und Versicherungen. Aber auch Unternehmen in anderen Bereichen unterliegen diversen Regularien, gerade bei geschäftskritischen Anwendungen. In diesem Beitrag wird aus Sicht eines Nicht-Juristen eine Übersicht der wichtigsten Regeln und Beteiligten gegeben.*

1 Einführung

1.1 Cloudbasierte Services

Wie schon in [1] dargestellt wurde, bilden Migrationen in cloudbasierte Architekturen einen immer populäreren Ansatz, sowohl für die Infrastruktur („IaaS“, „PaaS“) von IT-Systemen, aber stark auch für Anwendungen („SaaS“) selbst.

Cloudbasierte Services werden heute in drei wesentlichen Klassen angeboten, die schon 2011 von der NIST und darauf basierend vom BSI wie folgt definiert wurden (auszugsweise Zitate), siehe dazu [1]:

- Infrastructure as a Service (IaaS)

Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. So kann ein Cloud-Kunde z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

- Platform as a Service (PaaS)

Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware).

- Software as a Service (SaaS)

Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie. Als Beispiele seien Textverarbeitung oder Kollaborationsanwendungen genannt, aber auch geschäftskritische Systeme werden zunehmend als SaaS bezogen.

Alle vorgenannten Angebote gibt es in verschiedensten Konstellationen, die sich vor allem dadurch unterscheiden, ob die Services durch einen Provider für den Anwender in einer exklusiven („private“) oder auf Basis einer mit anderen Anwendern geteilten („public“) Infrastruktur zur Verfügung gestellt werden. Auch Kombinationen von beiden („Hybrid“) Cloud-Typen sind möglich.

1.2 Rahmenbedingungen für cloudbasierte Services

Neben den damit durch die Anwender zu lösenden technischen und fachlichen Fragestellungen, vor allem bzgl. der Integration von Cloud-Services mit eigenen noch selbst betriebenen Anwendungen („Cloud Integration“), spielen auch juristische und gerade im Banken und Finanzdienstleitungsbereich aufsichtsrechtliche Anforderungen eine immer größere Rolle.

Die nachfolgende Tabelle aus einer Umfrage [2] zeigt deutlich, dass die größten Hemmnisse offenbar im Bereich Datenschutz und -sicherheit sowie Unsicherheiten im rechtlichen Bereich liegen.

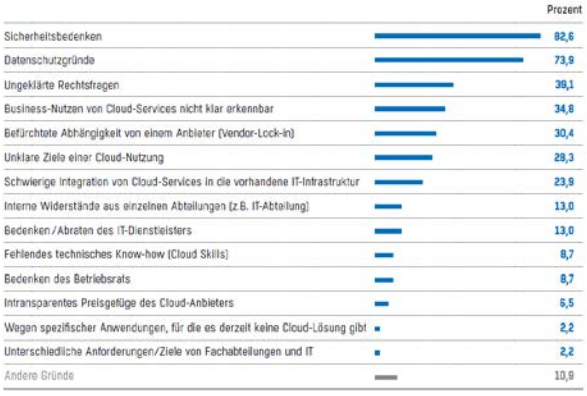

Abbildung 1 - Hemmnisse für Cloud-Nutzung

Im Folgenden werden die wesentlichen juristischen und aufsichtsrechtlichen Rahmenbedingungen (ohne Anspruch auf Vollständigkeit) im Überblick dargestellt. Dabei ist vor allem der Banken- und

Versicherungsbereich auch in diesen Themen einer noch zunehmenden Regulatorik unterworfen.

2 Rechtliche Aspekte

2.1 Vertragsrecht

Bezieht ein Unternehmen Cloud-Leistungen von einem externen Anbieter, so handelt es sich dabei rechtlich nach BGB um ein Dienstleitungs- (§611 ff.) oder auch Werkvertragsverhältnis (§631ff.). Darin unterscheidet es sich nicht von schon lange bekannten klassischen Outsourcing-Vertragsverhältnissen. Hierbei ist es vor allem wichtig, alle Leistungen und ihre Güte („Service Level“) sowie die Kompensation bei Verstößen zu beschreiben. Entsprechende Vertragswerke können daher sehr umfangreich (über 100 Seiten) werden. Während der Vertragslaufzeit sind diese externen Services regelmäßig zu berichten und zu überwachen („Provider-Management“).

2.2 Compliance und Risikomanagement

Die wesentliche eigene Organisationseinheit in großen Unternehmen stellt die Revision dar, die alle IT-Prozesse gegen die dokumentierten Regularien prüft. Darüber hinaus wird von großen Kapitalgesellschaften, die dem Zwang zum Einsatz von externen Wirtschaftsprüfern unterliegen, gefordert, dass sie für externe Dienstleistungen („Auslagerungen“) ein IT-Risikomanagement nachweisen können, das von den Wirtschaftsprüfern anhand entsprechende IT-Prüfkataloge ihrer Verbände (IFAC, ISACA, IDW, siehe z.B. [3]), auch detailliert geprüft wird.

2.3 Datenschutz und Datensicherheit

Eine der wesentlichsten rechtlichen Regularien bei Einsatz von Cloud-Services ist die Einhaltung aller datenschutzrechtlichen (derzeit auf Basis BDSG, ab Mai 2018 EU-DSGVO [4]) und Datensicherheitsanforderungen. Verstöße können ab 2018 mit drakonischen Strafen geahndet werden. Es ist daher unbedingt darauf zu achten, dass Cloud-Provider mindestens nach ISO/IEC 27001 und 20000 zertifiziert ist. Daneben gelten im Bereich der öffentlichen Verwaltung zwingend die Vorgaben des BSI speziell zum Cloud-Einsatz, an denen sich auch Wirtschaftsunternehmen orientieren sollten.

2.4 Externe Regulatorik

Neben den externen Wirtschaftsprüfern ist es im Banken- und Versicherungsbereich vor allem die Regulatorik auf Basis des Kreditwesengesetzes, die sehr hohe Anforderungen an das Risikomanagement stellt. Hierzu wurde 2002 die BaFin als Zusammenschluss anderer Aufsichtsbehörden geschaffen, die vorrangig bei Banken umfangreiche Prüfungen auf Basis der sog. „Mindestanforderungen an das Risikomanagement“ (MaRisk) [5] durchführt. Auch die EZB führt eigene Prüfungen durch, die sich auch auf die Absicherung aller IT-Prozesse inkl. der Auslagerungen beschäftigen. Diese Anforderungen sind über die letzten 10 Jahre immer weiter verschärft und konkretisiert worden, aktuell liegt ein Neustrukturierungsvorschlag in Form der sog. BAIT [6] vor.

Im Versicherungs- (Versicherungsaufsichtsgesetz VAG) und Investmentgesellschaften (InfMaRisk) gelten analoge Regelungen zu den Banken, wenngleich etwas abgeschwächter.

3 Fazit

Der Einsatz von Cloud-Services ist nicht nur ein fachlich und IT-technisch komplexes Unterfangen, sondern unterliegt auch einer großen Menge von juristischen und aufsichtsrechtlichen Bedingungen. Grundlegend ist dabei die Regel, dass sich die rechtliche Verantwortung nicht mit „outsourcen“ lässt, sondern immer beim Anwender verbleibt. Dieser hat daher nachweislich durch ein entsprechendes Risiko- und Providermanagement dafür Sorge zu tragen, dass auch die extern erbrachten Leistungen den gesetzlichen Bestimmungen genügen. Die durch den Provider zu zahlende Pönale wird i.d.R. nicht ausreichen, gerade Strafen bei Verstößen gegen Datenschutzbestimmungen abzudecken. Diese können ab 2018 immerhin bis zu 20 Mio. EUR oder 4% eines Jahresumsatzes betragen.

4 Literatur

[1] Jens Borchers: Migration auf cloudbasierte Plattformen aus Sicht des klassischen Reengineering, 18. Workshop Software-Reengineering und Evolution, Mai 2016, fg-sre.gi.de/fileadmin/gliederungen/fg-sre/wsre2016/WSRE-2016-Proceedings-2.pdf

[2] IDG: Studie Cloud Security 2016, kostenfrei beziehbar über www.freudenberg-it.com/de/fit-cloud-security-studie/

[3] www.idw.de/idw, www.isaca.org

[4] eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

[5] BaFin: Mindestanforderungen an das Risikomanagement, 2012, www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1210_erlaeuterungen_ba.pdf?__blob=publicationFile&v=1

[6] BaFin: Konsultationen BAIT, www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2017/dl_kon_0217_entwurf_bait_ba.html