Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

Peter H. Deussen, Klaus-Peter Eckert, Petra Hoepner, Christian Hoffmann, Linda Strick

CLOUD-FAHRPLAN FÜR DIE ÖFFENTLICHE VERWALTUNG

in Kooperation mit:

LORENZ-VON-STEIN-INSTITUT
FÜR VERWALTUNGSWISSENSCHAFTEN
an der Christian-Albrechts-Universität zu Kiel

Fraunhofer
FOKUS

IMPRESSUM

Autoren:
Peter H. Deussen, Klaus-Peter Eckert, Petra Hoepner,
Christian Hoffmann, Linda Strick

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage April 2014

EINLEITUNG

Die Cloud wird reichhaltiger, flexibler und dynamischer. Durch eine Vielzahl von Initiativen, sowohl im nationalen als auch im europäischen Kontext, bietet sich für Behörden ein ständig breiter werdendes Spektrum an komplementären Cloud-Dienstleistungen.

Diese Informationsschrift hat die Zielsetzung, einen Überblick über die Problemfelder zu geben, die sich für Verwaltungen bei der Migration von IT-Dienstleistungen in die Cloud ergeben. Im Einzelnen werden die folgenden Themen behandelt:

- Was ist überhaupt Cloud-Computing? Definition und Abgrenzung zu klassischen Dienstleistungsmodellen.
- Welche Betriebsmodelle und welche Standorte für Datenspeicherung und -verarbeitung kommen für den behördlichen Kunden in Frage?
- Die Verwaltung und die Cloud: Stand der aktuellen Forschung, Initiativen auf deutscher und europäischer Ebene.
- Was nützt der Verwaltung die Cloud …
- … und was sind die Risiken?
- Welche Anforderungen muss die Verwaltung an die Cloud stellen? Wir betrachten die Themenfelder Recht, Organisation, Technik und Sicherheit.
- Wie kommt die Verwaltung in die Cloud? Es wird ein »Fahrplan« vorgestellt, der die Migration von IT-Dienstleistungen in die Cloud in fünf Schritten darstellt.

Diese Informationsschrift wurde durch das Kompetenzzentrum Öffentliche IT am Fraunhofer-Institut FOKUS in Berlin in Zusammenarbeit mit dem Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel erstellt.

INHALTSVERZEICHNIS

1. CLOUD-COMPUTING: WAS IST DAS ?

Cloud-Computing ist ein Modell zur Bereitstellung von IT-Dienstleistungen, das *on-demand* und *online* den Zugriff auf einen gemeinsamen Pool konfigurierbarer Ressourcen wie Netzwerke, Server, Speichersysteme und Anwendungen ermöglicht. Anbieter versprechen diese passgenau, schnell, kostengünstig und mit minimalem Verwaltungsaufwand bereitstellen zu können.

Organisationen, die Cloud-Ressourcen nutzen, sind selbst also nicht oder nur zum Teil mit der Verwaltung der Ressourcen beschäftigt; diese Aktivitäten finden beim Dienstanbieter statt. Für die nutzenden Organisationen entfällt dadurch die Notwendigkeit eine eigene Infrastruktur, Dienstplattformen und Dienste anzuschaffen und zu unterhalten. Es werden Geschäftsmodelle möglich, die Ressourcen auf Nutzungsbasis anbieten und abrechnen.

1.1 WIE IST DIE CLOUD DEFINIERT ?

Cloud-Computing ist durch die folgenden Eigenschaften charakterisiert:

Automatische Diensterbringung auf Anforderung: Nutzer sind in der Lage, selbstständig Dienste und Ressourcen anzufordern, ohne dass eine Interaktion mit menschlichen Operatoren auf Seiten des Anbieters notwendig wird.

Netzwerkbasierter Zugang über das Internet oder aber auch über ein dediziertes Netzwerk, so dass Dienste aus der Cloud auf verschiedenen Endgeräten verwendet werden können.

Ressourcen-Pooling bzw. Mandantenfähigkeit: Die Ressourcen des Anbieters sind in Pools konsolidiert, die eine parallele Diensterbringung für mehrere Mandanten (Kunden) erlaubt. Dabei werden die Ressourcen (und damit Daten und Prozesse) der einzelnen Mandanten auf sichere Weise voneinander getrennt.

Elastizität. Ressourcen und Dienste werden »elastisch« zur Verfügung gestellt, d. h. entsprechend seines augenblicklichen Bedarfs erhält der Benutzer innerhalb eines gering bemessenen Zeitrahmens Ressourcen in adäquaten Quantitäten. Für den Nutzer stehen dadurch Ressourcen in unbeschränkten Quantitäten zur Verfügung.

Messbare Dienstqualität: Cloud-Systeme verfügen über eingebaute Monitoring- und Messfunktionen, die sowohl eine optimierte Ressourcen-Nutzung als auch eine Validation der erreichten Dienstqualität seitens des Nutzers erlauben.

1.2 BETRIEBSMODELLE

Es können verschiedene Betriebsmodelle unterschieden werden.

In einer **öffentlichen Cloud** teilen sich eine hohe Anzahl von Kunden die Ressourcen der Cloud – potenziell kann jeder eine öffentliche Cloud verwenden. Dienstangebote werden pauschal erbracht, individuelle Anpassungen sind nicht möglich.

Im Unterschied dazu werden in der **privaten Cloud** Dienstleistungen für einen einzelnen Kunden oder für einen eng begrenzten Kundenkreis erbracht (z. B. Kommunalverwaltungen einer spezifischen Region). Das Dienstangebot kann hier an die spezifischen Bedürfnisse angepasst werden.

Eine **Community-Cloud** stellt Dienstleistungen für eine Benutzergruppe mit gleichartigen Interessen bereit (z. B. Kunden einer spezifischen Branche). Das Dienstangebot ist in höherem Maße standardisiert als bei der privaten Cloud.

Schließlich können Clouds verschiedener Betriebsmodelle miteinander kombiniert werden; man spricht dann von einer **hybriden Cloud**. Ein Beispiel ist der Betrieb einer privaten Cloud

für die Bearbeitung sensibler Daten in Verbindung mit Ressourcen einer öffentlichen Cloud z. B. zur Bereitstellung öffentlicher Informationen, Statistiken, etc.

1.3 DIENSTMODELLE

Schließlich können verschiedene Dienstmodelle unterschieden werden. In der Literatur findet sich meist die folgende Unterscheidung:

Infrastruktur als Dienst (*infrastructure as a service – IaaS*). Die Dienstleistung besteht in der Bereitstellung virtualisierter[1] IT-Infrastrukturkomponenten – Rechenleistung, Speicherplatz, Netzwerk. Dem Kunden wird im Grunde die Hardware eines Rechenzentrums zur Verfügung gestellt. Der Betrieb der zugehörigen Software – vom Betriebssystem bis zur Endnutzer-Anwendung – obliegt dem Kunden.

Plattform als Dienst (*platform as a service – PaaS*). Dieses Dienstmodell besteht in der Bereitstellung von Software-Komponenten, die noch nicht für die direkte Verwendung durch den Endnutzer geeignet sind: Datenbanken, Laufzeitumgebungen, Entwicklungsumgebungen oder Integrationsunterstützung.

Software als Dienst (*software as a service – SaaS*). Hier werden Endnutzer-Anwendungen als Cloud-Dienste zur Verfügung gestellt: Office-Anwendungen, E-Mail-Klienten, Kundendatenbank-Anwendungen, komplette Desktop-Umgebungen, usw.

1.4 CLOUD-COMPUTING – WAS IST WIRKLICH NEU?

Viele Aspekte des Cloud-Computing wurden in der Vergangenheit bereits als Innovationen dargestellt und tauchen nun unter neuem Namen wieder auf: Netzwerkbasierter Zugriff wurde vor einigen Jahren als *application service provisioning* bezeichnet. Virtualisierung gehört längst zum Standard-Instrumentarium einer jeden IT-Abteilung. Die Grundlagen für die Integration einer hohen Anzahl von IT-Ressourcen wurden mit dem sogenannten Grid Computing gelegt.

Cloud-Computing ist – wie jede andere Technologie – aus vorhergehenden Entwicklungen erwachsen. Auf technologischer Ebene besteht ihr innovativer Charakter zunächst in der umfassenden Automatisierung der Diensterbringung: Die Bereitstellung[2], der Betrieb und das Management komplexer Applikationen kann ohne das Zutun menschlicher Administratoren für eine hohe Anzahl von Kunden stattfinden. Die Cloud wird damit – wie das Internet im Bereich Datenübertragung – zum umfassenden Instrument der Datenspeicherung und -verarbeitung.

Die Cloud bestimmt längst das digitale Leben von Bürgern und Unternehmen:

- Soziale Netzwerke werden auf der Basis von Cloud-Infrastrukturen realisiert – Facebook ist ohne Cloud nicht denkbar.
- Als Cloud-Klienten genutzte mobile Endgeräte werden als Erweiterung des Büros angesehen – und die Nutzung privater Geräte für dienstliche Zwecke (»bring your own device«) verwischt die Grenzen zwischen Privat- und Berufsleben.
- Online-Speicher wird als zuverlässige Alternative zur externen Festplatte oder zum USB-Stick angesehen.
- Viele Unternehmen – auch aus dem KMU-Segment – nutzen Cloud-Angebote, um Investitionen und operative Kosten für ihre IT zu reduzieren.[3]

[1] Unter »Virtualisierung« versteht man die Implementierung von Hardwarekomponenten (Server, Netzwerkelemente, Speicher) in Software. Virtualisierung ist eine Grundvoraussetzung für Cloud-Computing. Cloud-Dienste operieren auf virtualisierten Ressourcen, die durch die Cloud-Systeme auf reale Hardware-Komponenten abgebildet werden.

[2] Engl.: Deployment

[3] Cloud-Monitor 2013, Cloud-Computing in Deutschland – Status quo und Perspektiven, KPMG, BITKOM, Studie, 2013, http://www.bitkom.org/files/documents/BITKOM_KPMG_PAC_Studie_Cloud_Monitor_2013.pdf

1.5 DATENSCHUTZ UND STANDORT

Die umfassende Datensammlung durch US-amerikanische und britische Geheimdienste und die daraus resultierende Diskussion zum Thema Datensicherheit im Internet macht deutlich: Die Cloud ist ebenso ein technisches wie auch ein gesellschaftliches und politisches Phänomen.

– Pressemeldungen der letzten Zeit legen nahe, dass z. B. US-amerikanische Cloud-Dienstanbieter einem starken Druck von Seiten der dortigen Nachrichtendienste ausgesetzt sind, Informationen über nachrichtendienstlich interessante Kunden preiszugeben.

Behörden, die die Nutzung von Cloud-Angeboten planen, sollten deshalb prüfen, ob für die Speicherung und Verarbeitung personenbezogener oder anderer sensibler Daten ein ausreichendes Schutzniveau gegeben ist: Behörden sollten möglichst einen Anbieter wählen, der sicher stellen kann, dass personenbezogene oder sonstige sensible Daten in Rechenzentren gespeichert und verarbeitet werden, die sich im deutschen Hoheitsgebiet befinden und deutschem Recht (insbesondere Datenschutz) unterliegen. Zugriffe Dritter auf behördliche Daten müssen ausgeschlossen sein. Private Clouds, die durch behördliche Rechenzentren bereit gestellt werden, und Community-Clouds (etwa der Zusammenschluss mehrerer behördlicher Rechenzentren zu einer gemeinsam genutzten Cloud) werden diese Anforderungen leichter erfüllen als Anbieter öffentlicher Clouds, deren Angebot nicht auf die spezifischen Sicherheitsanforderungen behördlicher Kunden zugeschnitten ist.[4]

Das BSI hat ein Eckpunktepapier[5] veröffentlicht, welches Sicherheitsanforderungen an Cloud-Dienstleister formuliert und insbesondere auch die behördliche Perspektive berücksichtigt. Zum Thema Spionageabwehr verweisen wir auf die hierfür zuständigen Stellen, nämlich das Bundesamt für Verfassungsschutz bzw. die Landesämter für Verfassungsschutz.

[4] In diesem Zusammenhang ist auch zu beachten, dass öffentliche Cloud-Anbieter zunehmend dazu übergehen, Lastspitzen durch die dynamische Integration von Cloud-Diensten abzufangen, die durch Dritt-Anbieter bereitgestellt werden, wobei dann insbesondere auf Ressourcen großer (US-amerikanischer) Anbieter zugegriffen wird, die vollautomatisch angemietet und in Betrieb genommen werden können. Diese als »*cloud burst*« bezeichnete Vorgehensweise ist als kritisch zu bewerten, da durch die dynamische, kurzfristige Nutzung solcher Sekundär-Dienstleister eine rechtlich, vertraglich und technisch komplexe Situation geschaffen wird, in der nicht mehr klar ist, wie Anforderungen bzgl. Sicherheit, Datenschutz, Verfügbarkeit, Haftung usw. insgesamt sichergestellt werden können.

[5] BSI, Cloud-Computing Eckpunktepapier, Februar 2012, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

2. DIE ÖFFENTLICHE VERWALTUNG UND DIE CLOUD

Die öffentliche Verwaltung steht der Cloud eher skeptisch gegenüber. Unsicherheit bezüglich gesetzlicher Rahmenbedingungen, wie in Abschnitt 5.1 dargestellt, und bezüglich Sicherheitsrisiken (Kapitel 4) stehen für Bedenken, die einer Nutzung der Cloud in der deutschen Verwaltung entgegenstehen. Herstellerabhängigkeiten (Kapitel 4), verursacht durch fehlende Standards und damit fehlende Interoperabilität zwischen Anwendungen, Diensten und Geräten, stellen ein weiteres Problemfeld dar, das nicht nur zu einer Fragmentierung der Technologien führt, sondern auch den Wechsel von einem Cloud-Anbieter zu einem anderen erheblich erschwert.

Im Folgenden werden neue Entwicklungen und Best-Practice Ergebnisse beispielhaft vorgestellt.

2.1 FORSCHUNGSARBEITEN

Die *Trusted Cloud* Initiative[6] des Bundesministeriums für Wirtschaft und Technologie (BMWi) hat mit dem Wettbewerb »Sichere Internet-Dienste – Sicheres Cloud-Computing für Mittelstand und öffentlichen Sektor Forschungs- und Entwicklungsaktivitäten (FuE-Aktivitäten)« eine Initiative zur Förderung von Forschungs- und Entwicklungsarbeiten in den Bereichen effiziente und innovative Cloud-Strukturen sowie cloud-basierte Dienste ins Leben gerufen. Die Forschungsprojekte goBerlin und CloudCycle sind im Bereich der öffentlichen Verwaltung angesiedelt und legen besonderen Wert auf Vertraulichkeit, Sicherheit und Rechtskonformität von Cloud-Anwendungen.

CloudCycle[7] beschäftigt sich mit dem gesamten Lebenszyklus von Cloud-Anwendungen und will damit die Bedenken hinsichtlich Sicherheit und rechtlicher Rahmenbedingungen ausräumen. Schwerpunkte des Projektes sind die flexible Nutzung von Cloud-Anwendungen auf unterschiedlichen Plattformen, garantierte Sicherheit und Compliance, Nutzung standardisierter Schnittstellen zur Erreichung von Interoperabilität zwischen verschiedenen Cloud-Plattformen und die Darstellung von Mandantenfähigkeit. Das Anwendungsfeld ist die sogenannte Bildungs-Cloud, die eine auf die Bedürfnisse von Schulen zugeschnittene Auswahl an Cloud-Diensten über ein Portal zur Verfügung stellen wird.

Das Projekt **goBerlin**[8] realisiert eine Cloud-Plattform für die Vermittlung öffentlicher Leistungen und ergänzender gewerblicher Angebote. Im IT-Dienstleistungszentrum Berlin (ITDZ)[9] wird dazu eine vertrauenswürdige Cloud-Infrastruktur aufgebaut, die insbesondere die datenschutzrechtlichen Anforderungen der öffentlichen Verwaltung sicherstellt. Das Kernziel des Projekts geht jedoch weit über die Entwicklung einer Cloud-Infrastruktur für Verwaltung und Wirtschaft hinaus: Es wird eine technologische Marktplatz-Plattform eingerichtet, die es Behörden und Unternehmen zusätzlich ermöglicht, sichere und vertrauenswürdige IT-Dienste anzubieten und zu verknüpfen.

2.2 INITIATIVEN AUF LANDES- UND KOMMUNALER EBENE

Die private Cloud für die Hauptstadt. Mit der privaten Cloud will das IT-Dienstleistungszentrum (ITDZ) Berlin seinen Kunden Cloud-Dienste, d. h. neue Infrastruktur-Dienste (Server und Speicher) sowie Plattform-Dienste, bereitstellen. So sollen Beschaffungs- und Bereitstellungsvorgänge für die Kunden verkürzt und Produktivitätssteigerungen erreicht werden. Besonderer Wert wird auf ein hohes Sicherheitsniveau, das den strengen Datenschutzanforderungen der öffentlichen Verwaltung gerecht wird, gelegt.

[6] Trusted Cloud Initiative, http://www.trusted-cloud.de/
[7] Projekt CloudCycle, www.cloudcycle.org
[8] Projekt goBerlin, www.goberlin-projekt.de
[9] ITDZ Berlin, http://www.itdz-berlin.de/

Die Polizei-Cloud in Rheinland-Pfalz. Für die Polizei in Rheinland-Pfalz stellt der Landesbetrieb Daten und Informationen (LDI) den Betrieb einer virtualisierten Infrastruktur als Cloud-Lösung bereit, die sogenannte Polizei-Cloud.[10] Der LDI hat vor der Bereitstellung der Cloud ca. 340 physische Serversysteme für die Polizei betreut. Mit der Polizei-Cloud konnte die Zahl der physischen Serversysteme mit Hilfe von Virtualisierungstechnologien deutlich reduziert werden. Damit können Fachanwendungen in verschiedenen polizei-exklusiven Netzen betrieben werden. Hinsichtlich Sicherheit ist zum einen die virtualisierte Infrastruktur im Verwaltungsbereich von dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis des IT-Grundschutzes zertifiziert, zum anderen zeigen Erfahrungen aus dem Alltag, dass die Sicherheitsarchitektur täglich mehr als 44 Millionen Zugriffe blockiert, von denen rund 200.000 Fälle potenzielle kriminelle Angriffe darstellen.[11]

Die GovCloud für Kommunen. Die Bundes-Arbeitsgemeinschaft der kommunalen IT-Dienstleister, Vitako[12], stellt seit Dezember 2013 eine Plattform für Cloud-Computing Dienste bereit[13]. Das Angebot wurde von der ProVitako, der Marketing und Dienstleistungsgesellschaft der kommunalen IT-Dienstleister entwickelt. Die ProVitako umfasst mehr als 20 IT-Dienstleister der öffentlichen Hand, die die Gesellschaft als Genossenschaftsmitglieder tragen. Die Cloud-Dienste werden durch die einzelnen Genossenschaftsmitglieder erbracht. Um vergabe- und kartellrechtlichen Anforderungen zu genügen, wurde die Organisationsform einer Genossenschaft gewählt. Dadurch werden die Dienstangebote und Dienstnutzung in einem Inhouse-Verfahren geregelt. Die ProVitako kann so Cloud-Dienste der Mitglieder einkaufen und an andere Mitglieder weiterverkaufen, wobei die Genossenschaftsmitglieder ihrerseits die Cloud-Dienste ihren Kunden zu einem günstigen Preis anbieten können. Die Abrechnung der Dienste ist nutzungs- und verbrauchabhängig; die Preisbildung für die Cloud-Dienste erfolgt im Wettbewerb. Die Plattform bietet Cloud-Dienste wie z. B. Speicherplatz, Fachverfahren für Querschnittsaufgaben und Office-Lösungen an.

2.3 INITIATIVEN AUF EUROPÄISCHER EBENE

Europäische Union. Neelie Kroes, Vizepräsidentin der Europäischen Kommission, hat mit der digitalen Agenda einen Meilenstein für eine europäische Cloud Strategie gesetzt. Im November 2013 legte Kroes während einer Konferenz in Berlin dar, dass ein einheitlicher europäischer Markt für Cloud-Computing ein primäres Ziel der Europäischen Union sei.[14] Der europäische Markt könne nur durch Investitionen in eine interoperable Infrastruktur erreicht werden. Um die Nachfrage, insbesondere aus dem öffentlichen Sektor, zu steigern, sei es notwendig, Investitionen in Forschung und Innovation zu leisten, Vertrauen aufzubauen und sicherzustellen, dass die Datenschutzbestimmungen befolgt werden.

Im Rahmen der europäischen Cloud-Strategie hat die Europäische Kommission Maßnahmen vorgestellt, um 2,5 Millionen neue Arbeitsplätze in Europa zu generieren und zusätzlich das Bruttoinlandsprodukt um ca. 160 Milliarden Euro bis 2020 jährlich zu erhöhen. Eine in einem Strategiepapier vorgestellte umfassende Analyse vorhandener politischer, technischer und gesetzlicher Regularien zielt darauf ab, die Potenziale des Cloud-Computing zu identifizieren und zu maximieren.[15]

---

[10] LDI, Hintergrundinformationen zur Polizei-Cloud, http://ldi.rlp.de/fileadmin/ldi/Downloads/Nachrichten/Hintergundinfos_Cloud.pdf

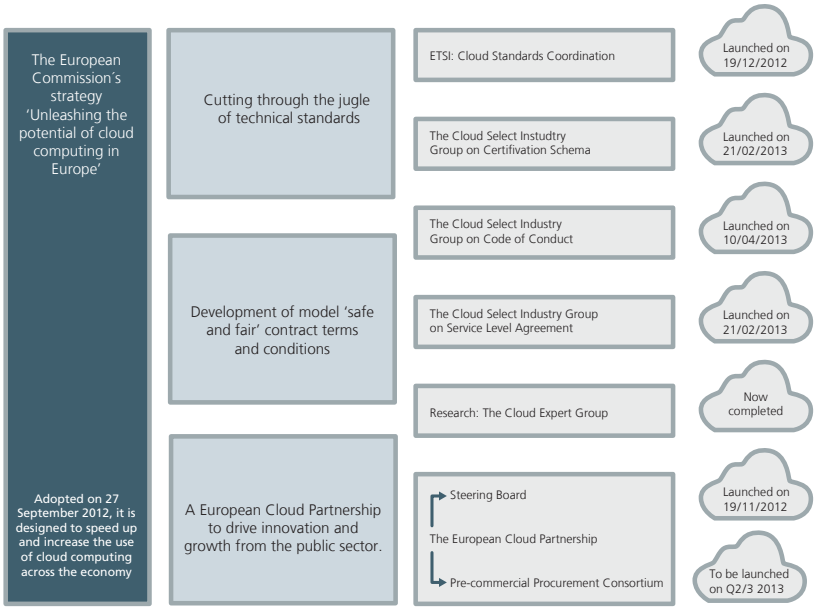
[11] Rheinland-Pfalz zertifiziert als erstes Bundesland den Betrieb einer virtualisierten Infrastruktur für die sog. Polizei-Cloud, http://ldi.rlp.de/aktuelles/einzelansicht/article/rheinland-pfalz-zertifiziert-als-erstes-bundesland-den-betrieb-einer-virtualisierten-infrastruktur-f-1/

[12] Vitako, http://www.vitako.de/aktuelles/Seiten/default.aspx

[13] GovCloud, http://www.govcloud.de/

[14] Readiness for Cloud Computing in the European Public Sector, 14 – 15 November 2013, Konferenz, Berlin, http://ec.europa.eu/deutschland/press/pr_releases/11815_de.htm

[15] Unleashing the potential of Cloud Computing in Europe, Communication from the Commission of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 529 final, Brüssel, September 2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf



Überblick der Aktivitäten der Europäischen Kommission zur Akzeptanz von Cloud-Computing[16]

Die drei Hauptaktivitäten zur Förderung von Cloud-Computing zielen darauf ab:

- einen Überblick über verfügbare Standards und deren Relevanz für Cloud-Computing zu erhalten;
- die Entwicklung von zuverlässigen und fairen Vertragsklauseln voranzutreiben;
- durch die »*European Cloud Partnership*« Innovation und Wachstum in den öffentlichen Sektor zu bringen.

Dazu hat die Europäische Kommission entsprechende Arbeitsgruppen initiiert, die sich mit diesen Themen befassen: Das »European Telecommunication Standards Institute« (ETSI) hat Ende 2013 einen Überblick über relevante Standards veröffentlicht.[17] Die Entwicklung von Modell-Verträgen steht im Vordergrund der Arbeitsgruppe zu sicheren und fairen allgemeinen Geschäftsbedingungen. Die Europäische Cloud-Partnerschaft dient dazu, die Akzeptanz von Cloud-Dienstleistungen im öffentlichen Bereich zu erhöhen und die zersplitterte Nachfrage zu bündeln. Dazu hat die Europäische Kommission ein Projekt aufgesetzt, das mit dem Instrument der vorwettbewerblichen Auftragsvergabe Forschung und Entwicklung der Industrie fördern und somit die Bereitstellung von Cloud-Dienstleistungen für den öffentlichen Bereich effizienter und mit höherer Qualität unterstützen soll.[18]

Großbritannien. Die **G-Cloud**[19] ist ein Programm in Großbritannien, das vom dortigen Justizministerium geleitet und durch das Innenministerium unterstützt wird. Im Fokus steht die Einführung von Cloud-Dienstleistungen in Ministerien, Behörden und lokalen öffentlichen Institutionen. Basierend auf der IKT-Strategie der öffentlichen Hand bietet G-Cloud Möglichkeiten, über Ministerialgrenzen hinweg Cloud-Dienste zu nutzen. Die Beschaffung von Dienstleistungen beruht auf einem gemeinsamen Beschaffungsrahmen. Rahmenverträge sind auf den Bedarf der öffentlichen Verwaltung zugeschnitten. Ein »Cloud-Store«[20] ermöglicht es Verwaltungen, Dienstleistung per Einkaufswagen einzukaufen und zu nutzen. Derzeit gibt es vier Kategorien von Dienstleistungen: Infrastruktur, Software, Plattform- und Fachdienste.

[16] Ken Ducatel, Eurocloud Congress October 16-16, Luxemburg 2013
[17] European Telecommunication Standards Institute, Cloud Standards Coordination, Final Report, http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF
[18] Cloud for Europe, www.cloudforeurope.eu
[19] G-Cloud, http://gcloud.civilservice.gov.uk/
[20] G-Cloud-Store, http://gcloud.civilservice.gov.uk/cloudstore/

3. NUTZEN

Kostenersparnis durch Skaleneffekte

Die Ressourcen klassischer Datenzentren sind nie ausgelastet: Die Nutzung von IT-Diensten zeichnet sich durch Lastspitzen aus, für die Kapazitäten vorgehalten werden müssen, die außerhalb der Spitzenzeiten jedoch ungenutzt bleiben. Werden IT-Ressourcen gemeinschaftlich durch verschiedene Kunden genutzt, ergibt sich die Möglichkeit, temporär hohe Kapazitätsanforderungen des einen Kunden durch zurzeit ungenutzte Ressourcen eines anderen Kunden abzudecken. Pro Kunde müssen also weniger Ressourcen vorgehalten und verwaltet werden; die entstehenden Kostenersparnisse können an die Kunden weitergegeben werden. Diese Rechnung funktioniert umso besser, je mehr Kunden auf die gemeinsam genutzten Ressourcen zugreifen und je mehr ihre Nutzungsprofile voneinander divergieren.

Die elastische Zuteilung von IT-Ressourcen macht auch die Einführung von Abrechnungsmodellen möglich, bei denen der Kunde nur für die tatsächlich genutzten Ressourcen und nicht für die potenziell vorgehaltenen bezahlt: *pay-as-you-go*.

Es muss jedoch angemerkt werden, dass die beschriebenen Skaleneffekte insbesondere öffentliche Clouds betreffen.

Konsolidierung von IT-Ressourcen

Cloud-Technologien erlauben die Integration von IT-Ressourcen nicht nur innerhalb einer IT-Abteilung oder eines Datenzentrums, sondern auch über die Grenzen von Datenzentren hinweg. Zumindest technisch werden damit Dienstbereitstellungsmodelle möglich, in denen bisher exklusiv genutzte IT-Ressourcen nun gemeinsam von einer Reihe von Institutionen genutzt werden können, sodass die oben beschriebenen Skaleneffekte und die damit verbundenen Kostenvorteile in solchen Community-Clouds wirksam werden können. Eine wesentliche Voraussetzung hierfür sind effektive Mechanismen zur Mandantenfähigkeit, damit Daten und Prozesse verschiedener Kunden voneinander getrennt bleiben.

Bündelung von Know-how

Mit dem oben angeführten Argument der Konsolidierung von IT-Ressourcen geht auch eine Bündelung des zum Betrieb einer IT-Infrastruktur benötigten Know-hows einher. Dieser Umstand ist für den öffentlichen Sektor – angesichts reduzierter Personalbudgets und demografischen Wandels – von besonderem Interesse.

Modernisiertes IT-Management

Der Betrieb einer IT ist mehr als nur das Aufstellen von Servern und das Verlegen von Netzwerkkabeln. Das effektive und effiziente Management einer IT-Infrastruktur ist eine außerordentlich komplexe Aufgabe, die von kleineren IT-Abteilungen nur ungenügend gelöst werden kann. Viele Aspekte des IT-Managements können jedoch automatisiert und in einer modernen IT-Infrastruktur durch sogenannte *operational support systems* (OSS) erledigt werden. Cloud-Technologien stellen solche OSS bereit.

Für eine Organisation, die einen Teil ihrer IT-Infrastruktur in die Cloud migrieren möchte, stellt sich damit jedoch auch die Frage: Inwieweit gibt die neue Cloud-Umgebung IT-Management-Prozesse vor? Sind diese mit den eigenen Prozessen verträglich oder sind Umstellungen notwendig?

Sicherheit

Angesichts fast täglicher Meldungen über Sicherheitslecks bei großen IT-Dienstanbietern stellt sich die Frage: Wie sicher ist die Cloud eigentlich? Diese Frage ist jedoch nicht pauschal zu beantworten: Ein Angriff auf einen großen Dienstleister mag nur deshalb durchgeführt worden sein, weil dieser Anbieter ein großes Ziel bietet, und überhaupt erst in die Presse gelangt sein, weil er ein hohen Schaden verursacht hat. Und wie wurde der Angriff überhaupt durchgeführt? Wurden wirklich kritische Komponenten einer Cloud angegriffen, oder beruht der Angriff

auf *social engineering* (z. B. Ergaunern von Passwörtern), das mit der unterliegenden Technologie nichts zu tun hat.

Sicherheit ist immer das Ergebnis einer Vielzahl technischer Mechanismen und organisatorischer Maßnahmen. Moderne Cloud-Infrastrukturen implementieren solche Mechanismen; ihre Herstellerfirmen verstehen es als Marktvorteil, für zeitgerechte Sicherheitsupdates zu sorgen. Integrierte Monitoring- und Analysefunktionen vereinfachen das Aufspüren von Angriffen. Schließlich ist der Betreiber einer Cloud eher in der Lage, ein dediziertes Expertenteam für Sicherheitsfragen zu finanzieren als eine kleine IT-Abteilung, in der jeder Mitarbeiter multiple Aufgaben hat.

Sicherheit als Risiko werden wir weiter unten ausführlich diskutieren. Dieser Abschnitt soll darauf hinweisen, dass die Cloud Optionen bietet, mit Sicherheitsrisiken besser umzugehen als klassische IT-Infrastrukturen.

4. RISIKEN

Organisatorische Risiken

Organisationsstrukturen innerhalb einer Verwaltung und die Organisationsstrukturen und Prozesse der unterstützenden IT wachsen in der Regel organisch; es ergeben sich eine Vielzahl von Querbeziehungen innerhalb und zwischen innerbehördlichen Abteilungen (und teilweise darüber hinaus), die (häufig unzureichend dokumentiert) auf die interne IT-Landschaft abgebildet werden. Die Auslagerung eines bestimmten IT-Systems sprengt notwendigerweise viele solcher Beziehungen und definiert neue. Hierzu zählen:

- Sicherheitsregelungen und -anforderungen: Verwaltung von Benutzern, Zugangsregelungen zu bestimmten Bereichen der IT, Zugriffsregeln für Daten, Administrationsrechte für Netzwerkkomponenten und Datenbanken, usw.
- IT-Management Prozesse wie z. B. Kapazitäts- und Inventarmanagement.
- Management von externen Anbietern von IT-Dienstleistungen.
- Kontrollverlust über die ausgelagerten Daten und Prozesse.

Die Auslagerung von Dienstleistungen in die Cloud beinhaltet also das Risiko, dass solche Prozesse nach der Migrationsphase nicht mehr effektiv oder hinfällig geworden sind.

Sicherheit

Bedenken bezüglich Informationssicherheit und Datenschutz beim Cloud-Computing gelten als ein großes Nutzungshindernis. Sicherheitsrisiken und Maßnahmen können teilweise aus den Bereichen Outsourcing, Virtualisierung, Web-Anwendungen und Netzmanagement übertragen werden, müssen für ihre Anwendung auf das Cloud-Computing allerdings angepasst werden:

- Standorte: Daten können geografisch verteilt sein, wobei die Standorte unterschiedliche Datenschutzrechte aufweisen können (vgl. hierzu auch die Diskussion nachrichtendienstlicher Gefährdungen in Abschnitt 1.5)
- Mandantenfähigkeit: Mehrere Nutzer teilen sich eine gemeinsame Infrastruktur, daher besteht auch ein Angriffsrisiko durch andere Nutzer.
- Rechteverwaltung: Jede Person darf nur berechtigt auf Daten oder Komponenten zugreifen, d. h. der unberechtigte Zugriff durch Cloud-Nutzer oder Cloud-Anbieter muss durch eine geeignete Rechteverwaltung verhindert werden.
- Löschung: Nachdem ein Vertrag mit einem Cloud-Anbieter gekündigt wurde, müssen alle Daten des Cloud-Nutzers vollständig gelöscht werden, damit diese nicht zu einem späteren Zeitpunkt für Unberechtigte zugänglich werden.
- Verfügbarkeit: Ausfälle von Cloud-Lösungen stellen ein höheres Risiko dar, da ein Cloud-Nutzer keine oder nur eine eingeschränkte eigene Infrastruktur vorhält und somit vom Cloud-Anbieter abhängig ist. Hier ist auch die Verfügbarkeit der Netzwerkanbindung des Kunden an den Anbieter zu berücksichtigen, da Netzausfälle ebenfalls zur Nichtverfügbarkeit von Diensten führen können.
- Attraktives Angriffsziel: Die Konzentration vieler Daten macht die Dienste von Cloud-Anbietern zu einem attraktiven Ziel für kriminelle und geheimdienstliche Angriffe, insbesondere wenn es sich um sensible, z. B. personenbezogene Daten handelt.[21]

Abhängigkeit

Eine Verlagerung der eigenen IT (oder Teile dieser IT) in die Cloud kann – wie jedes Outsourcing-Vorhaben – zu ungewollten Abhängigkeiten führen, die einen Anbieterwechsel oder ein Insourcing mit hohem finanziellen und organisatorischen Aufwand verbinden. Zunächst ist hier die Bindung an die Technologien, die von dem jeweiligen Cloud-Dienstanbieter verwendet werden, zu berücksichtigen – diese Form der Abhängigkeit

[21] Vgl. hierzu aber auch die in Kapitel 3 angestellten Überlegungen zur erhöhten Sicherheit in modernen Clouds.

wird als »vendor lock-in« bezeichnet. Darüber hinaus existieren aber noch weitere Formen der Abhängigkeit:

Strukturelle bzw. organisatorische Abhängigkeiten ergeben sich, wenn zur Durchführung des Outsourcings die Organisationsstrukturen der eigenen Verwaltung abgewandelt wurden, um die gemieteten Cloud-Dienste optimal (oder überhaupt) zu nutzen. Dies betrifft unmittelbar IT-spezifische Prozesse, die nach dem Outsourcing nicht mehr benötigt werden bzw. abgewandelt wurden.

Schließlich führt jedes Outsourcing von IT zu einem Verlust von operativem Wissen zum Betrieb einer IT-Infrastruktur, das bei einem Insourcing erneut erworben bzw. eingekauft werden muss.

5. ANFORDERUNGEN

5.1 RECHTSFRAGEN DES CLOUD-COMPUTING IM ÜBERBLICK

Bevor sensible Daten in die Cloud ausgelagert werden können, ist eine Reihe von rechtlichen Fragen zu beachten. In Anbetracht der unterschiedlichen Betriebsmodelle (private, öffentliche, Community und hybride) sowie den unterschiedlichen Dienstmodellen (SaaS, Paas, IaaS) sind pauschale Aussagen über die rechtliche Zulässigkeit der Nutzung von Cloud-Angeboten kaum möglich. Vielmehr bedarf es stets einer Einzelfallbetrachtung, die z. B. den Standort und die Art der Daten berücksichtigt. Aufgrund der Komplexität des Themas können die rechtlichen Rahmenbedingungen an dieser Stelle jedoch nicht erschöpfend dargestellt werden.

Datenschutzrecht

Sollen personenbezogene Daten in der Cloud verarbeitet oder gespeichert werden, bedarf es nach dem deutschen Datenschutzrecht einer entsprechenden Legitimationsgrundlage. Denn nach dem Grundsatz des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann erlaubt, wenn eine gesetzliche Erlaubnisvorschrift vorliegt oder der Betroffene wirksam eingewilligt hat (»Verbot mit Erlaubnisvorbehalt«). Datenauslagerungen in die Cloud mit Hilfe von Einwilligungserklärungen der betroffenen Bürger erweisen sich dabei als kaum praktikabel, da diese zum einen stets mit einer gewissen Unsicherheit bzgl. der Reichweite verbunden sind und zum anderen entsprechende Einwilligungen – zumindest wenn bereits vorhandene Datenbestände ausgelagert werden sollen – nachträglich eingeholt werden müssten. Bei der Suche nach der erforderlichen Ermächtigungsgrundlage bleibt daher lediglich die in §11 BDSG geregelte Auftragsdatenverarbeitung. Die größte Herausforderung dieser Vorschrift besteht darin, dass diese noch aus einer Zeit lange vor der Cloud-Technik stammt.

Grundsystematik des § 11 BDSG ist, dass der Auftraggeber für die Auftragsdatenverarbeitung verantwortlich bleibt (insbesondere für Auskunft, Löschung und Schadensersatz). Er hat den Auftragnehmer »unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen« sorgfältig auszuwählen. Dafür ist ein schriftlicher Vertrag zu schließen, in dem eine Reihe von Einzelheiten festgelegt werden müssen (Gegenstand und Dauer des Auftrages, Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung usw.). Schwierigkeiten bereitet in diesem Zusammenhang u. a. die Pflicht, auch die Berechtigungen zur Begründung von Unterauftragsverhältnissen vorab festzulegen, da sich Cloud-Angebote eben durch den Umstand auszeichnen, dass die Daten je nach Verfügbarkeit auf unterschiedlichen Servern gespeichert werden.

Dies gilt umso mehr, wenn die Server der Cloud-Anbieter weltweit verteilt sind. Die Übermittlung von personenbezogenen Daten außerhalb der Europäischen Union ist gem. § 4b Abs. 2 und 3 BSDG nur gestattet, wenn in den Zielstaaten ein angemessenes Datenschutzniveau gewährleistet ist. Nachgewiesen kann dies etwa durch die Verwendung der sog. EU-Standardvertragsklauseln, die von der Europäischen Kommission online bereitgestellt werden.[22] Eine Datenübermittlung in die USA ist nur dann zulässig, wenn sich die Datenzentren den sog. Safe-Harbour-Bestimmungen unterworfen haben. Diese zwischen der EU und den USA im Jahr 2000 getroffene Vereinbarung soll ebenfalls ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen gewährleisten, indem sich diese auf die in der Safe-Harbour-Vereinbarung vorgegebenen Grundsätze verpflichten. Insbesondere seit dem Bekanntwerden der NSA-Spähaffäre im Jahr 2013 ist dieses Abkommen jedoch in die Kritik geraten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aufgrund des umfangreichen Datenzugriffs der USA bekanntgegeben, dass die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für

[22] EU Model Contracts, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

die Datenübermittlung in die USA unter dem Safe-Harbour-Abkommen erteilen. Auch das EU-Parlament fordert, das Safe-Harbour-Abkommen auszusetzen.

Unterdessen gibt es derzeit Überlegungen, wie die Kontrollpflicht nach § 11 Abs. 2 Satz 4 BDSG im Cloud-Computing-Zeitalter sinnvoll umgesetzt werden kann. Nach dieser Vorschrift hat sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Da sich persönliche Vorortkontrollen angesichts der u. U. zahlreichen beteiligten Unternehmen als kaum praktikabel erweisen, wird diskutiert, ob es ausreichend ist, wenn sich die Auftraggeber die Eignung der von den Auftragnehmern getroffenen technischen oder organisatorischen Maßnahmen von Dritten in Form von Testaten, Zertifikaten oder Audits nachweisen lassen.

Die Arbeitsgruppe »Rechtsrahmen des Cloud-Computing« des Technologieprogramms »Trusted Cloud« (vgl. Abschnitt 2.1) hat in diesem Zusammenhang in einem rechtspolitischen Thesenpapier eine vereinheitlichte Testatlösung als praktikable Alternative zur persönlichen Vor-Ort-Kontrolle des Auftraggebers vorgeschlagen.[23] Die Prüfkriterien für die Erteilung eines Testats sollen nach der Vorstellung der Arbeitsgruppe auf gesetzlicher Grundlage einheitlich für alle europäischen Mitgliedstaaten gelten. Dafür wurden von der Arbeitsgruppe Vorschläge gemacht, wie eine derartige Testatlösung in die EU-Datenschutz-Grundverordnung, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch Unternehmen EU-weit vereinheitlicht werden sollen, integriert werden können. Die Bundesregierung hat die Ergebnisse der Arbeitsgruppe aufgegriffen und auf EU-Ebene einen Formulierungsvorschlag eingereicht, wie die Vorschläge zum Cloud-Computing sachgerecht in der Datenschutz-Grundverordnung umgesetzt werden können.

Verschlusssachenanweisungen

Beim Einsatz von Cloud-Technologien sind auch die Vorschriften zur Arbeit mit Verschlusssachen (VS) zu beachten. In Bundesbehörden und bundesunmittelbaren öffentlich-rechtlichen Einrichtungen sind diese in der »Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA)« geregelt. Für die Arbeit mit Verschlusssachen existieren in den Bundesländern eigene Vorschriften. Neben eventuellen Dokumentationspflichten sind vor allem die Vorschriften über den zulässigen Einsatz von IT-Systemen von Bedeutung. So haben die Geheimschutzbeauftragten z. B. eine Überprüfung dahingehend zu veranlassen, ob die erforderlichen Geheimschutzmaßnahmen getroffen sind, bevor IT-Systeme erstmals für VS eingesetzt werden. Zur Unterstützung können die Geheimschutzbeauftragten das BSI hinzuziehen, bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen soll das BSI zudem beratend hinzugezogen werden.

Urheberrecht

Vor dem Beginn der Cloud-Computing-Maßnahmen müssen auch urheberrechtliche Fragen geklärt werden. Insbesondere wenn der Cloud-Anbieter Software der Verwaltung in der Cloud-Umgebung installieren muss, ist sicherzustellen, dass der Cloud-Anbieter die entsprechenden urheberrechtlichen Nutzungsrechte wie etwa das Recht zur Vervielfältigung aus § 69c Nr. 1 Urheberrechtsgesetz (UrhG) und das Recht zur öffentlichen Zugänglichmachung aus § 69c Nr. 4 UrhG vom Softwarehersteller eingeräumt bekommt. Eine davon getrennte und noch nicht abschließend geklärte Frage ist, ob die Verwaltung als Kunde eigene Nutzungsrechte benötigt, wenn der Cloud-Anbieter insbesondere beim PaaS-Modell Softwareumgebungen zur Verfügung stellt. Dies wird jedoch überwiegend

[23] Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz_RZ_gesamt.pdf

verneint. Viele darüber hinausgehende im Zusammenhang mit dem Urheberrecht diskutierte Fragen, insbesondere bzgl. des anwendbaren Rechts und der jeweils zuständigen Gerichte, stellen sich für die öffentliche Verwaltung nicht, wenn es sich um eine rein private und innerdeutsche Cloud handelt.

Vergaberecht

Will die öffentliche Verwaltung Cloud-Dienste nutzen, handelt es sich um einen öffentlichen Auftrag, der in der Regel öffentlich auszuschreiben ist und bei dem das wirtschaftlichste Angebot den Vorzug erhalten muss. Zunächst ist jedoch zu klären, ob die beabsichtigte Leistung überhaupt dem Vergaberechtsregime unterliegt oder ob nicht die Voraussetzungen für eine sog. Inhouse-Vergabe vorliegen. Dies ist indes nur dann der Fall, wenn die Cloud-Dienstleister ausschließlich in öffentlicher Hand sind und ihre Dienste allenfalls zu einem kleinen Teil auf dem privaten Markt anbieten. Muss hingegen ein Vergabeverfahren durchgeführt werden, ist zu klären, welches Vergabeverfahren einzuhalten ist. Ist z. B. aufgrund der Komplexität der Beschaffung keine Leistungsbeschreibung möglich, stellt evtl. das Verhandlungsverfahren oder der wettbewerbsrechtliche Dialog eine Alternative dar. Ist indes ein offenes oder nichtoffenes Verfahren einzuhalten, ist ein Schwerpunkt auf eine detaillierte und diskriminierungsfreie Leistungsbeschreibung zu legen. Dabei ist insbesondere zu berücksichtigen, dass Cloud-Dienstleistungen partiell auch im Wettbewerb zu anderen, »klassischen« IT-Angeboten stehen. Eine Ausschreibung hat diese Gleichwertigkeit zu berücksichtigen, mit der Folge, dass evtl. auch bei der Beschaffung von herkömmlicher IT-Infrastruktur Cloud-Angebote zugelassen werden müssen. Auf der anderen Seite ist u. U. eine Beschränkung lediglich auf Cloud-Leistungen ebenso unzulässig. Um den o. g. datenschutzrechtlichen Vorgaben gerecht zu werden, müssen zudem Vertragsklauseln vorgesehen werden, die den Anbieter zu bestimmten rechtlichen, technisch-infrastrukturellen und organisatorischen Maßnahmen verpflichten. Ob ein Anbieter dies zu leisten imstande ist, sollte daher bereits im Vergabeverfahren i. R. d. Leistungsfähigkeit geprüft werden. Aufgrund der Komplexität der vergaberechtlichen Fragen ist die Hinzuziehung von Rechtsexperten zu empfehlen.

Organisationsrecht

Aus organisationsrechtlicher Sicht ist darauf zu achten, dass das gewählte Cloud-Modell nicht in Konflikt mit dem sog. Verbot der Mischverwaltung gerät. Nach diesem Grundsatz sind die Verwaltungszuständigkeiten von Bund und Ländern grundsätzlich voneinander getrennt und dürfen – selbst mit Zustimmung der Beteiligten – nur in den vom Grundgesetz vorgesehenen Fällen zusammengeführt werden. Eine Cloud-Nutzung wird jedoch nicht in Konflikt mit diesem Grundsatz geraten, wenn nicht die Erledigung von Sachaufgaben betroffen ist, sondern sich die Zusammenarbeit auf die Wahrnehmung von Dienst- und Unterstützungsfunktionen beschränkt, wozu in der Regel auch der Aufbau und Betrieb von IT-Infrastrukturen zählen wird.

Den genannten Herausforderungen bzgl. des beim Datenschutz-, Urheber- und Vergaberechts lassen sich am ehesten durch die Realisierung einer »privaten« Cloud in Verantwortung der öffentlichen Verwaltung begegnen. Ziel muss eine Bündelung der Soft- und Hardware-Ressourcen innerhalb der öffentlichen Verwaltung sein, realistisch zunächst bezogen auf bestimmte Teilbereiche. Als mögliches Umsetzungsmodell kommt dabei perspektivisch die Gründung eines sog. »Shared Service Centers« in Betracht. Darunter versteht man ein Organisationsmodell zur Bereitstellung von internen Dienstleistungen für mehrere Organisationseinheiten mittels gemeinsamer Nutzung von Ressourcen innerhalb einer Organisation. Eine derartige Bündelung der vorhandenen Hardware und der Softwarelizenzen, perspektivisch kombiniert mit einer zeit- und nutzungsabhängigen Abrechnung bei einem Dienstleistungszentrum wäre geeignet, den derzeitigen Abstimmungsbedarf bei der Beschaffung zu minimieren. Ein wirklicher Mehrwert entstünde indes nur dann, wenn der Organisationseinheit eine eigene Rechtspersönlichkeit zukäme, sodass jeweils nur ein Auftragsdatenverarbeitungsverhältnis entstünde.

5.2 ORGANISATORISCHE ANFORDERUNGEN

Die Auslagerung von IT-Diensten in die Cloud impliziert Änderungen der eigenen Organisationsstruktur auf verschiedenen Ebenen, z. B.:

- Rechte und Rollen, die innerhalb der eigenen Organisation definiert sind, müssen auf das Rollenmodel, das der Dienstleister in der Benutzerverwaltung der Dienstleistung vorgesehen hat, abgebildet werden. Dies ist nicht immer möglich oder einfach: Sieht der Dienstleister z. B. nur die Rolle des Benutzers und des Administrators vor, können komplexere Hierarchien nur schwer abgebildet werden.
- IT-Management-Prozesse wie Kapazitätsmanagement und Änderungsmanagement können nicht einfach von einer (klassischen) internen IT auf die Cloud übertragen werden. Kapazitäten müssen entsprechend der dynamischen Skalierung von Cloud-Diensten anders geplant und verwaltet werden. Änderungen werden vom Dienstleister vorgenommen: Verfahren zur Kontrolle solcher Änderungen durch den Kunden sind zu etablieren (Information, Erfolgskriterien, Fallback-Strategien).
- Die zentralisierte Bereitstellung von Diensten erfordert möglicherweise die Implementierung entsprechender zentralisierter Organisationsstrukturen innerhalb der eigenen Behörde. Andererseits werden Aufgaben, die bisher von der eigenen IT bearbeitet wurden, obsolet. Ein Beispiel ist das Einspielen von Sicherheits-Updates, das nun vom Dienstanbieter übernommen wird.

Entsprechend müssen Verantwortlichkeiten und Organisationsstrukturen der eigenen Behörde auf mögliche Änderungen überprüft werden. Die Migration der eigenen IT (ganz oder teilweise) in die Cloud ist immer auch unter dem Gesichtspunkt dieser Änderungen zu betrachten.

5.3 TECHNISCHE ANFORDERUNGEN

Im öffentlichen Sektor existieren spezielle architektonische Vorgaben, die bei Implementierung und Betrieb großer IT-Systeme und deren Infrastruktur zu beachten sind. So definiert beispielsweise SAGA[24] spezielle Sicherheitszonen, in denen die Komponenten für Zugang, Logik, Datenspeicherung und Management bereitgestellt werden. Bei der Überführung existierender IT-Systeme in eine Cloud-Infrastruktur bzw. bei der Realisierung neuer IT-Systeme sind diese Vorgaben zu beachten, d. h. vom Anbieter der Cloud-Dienste in geeigneter Form vorzusehen.

Cloud-Dienste werden im Allgemeinen für verschiedene Mandanten angeboten, die über unterschiedliche Netze auf die Dienste zugreifen. So können Zugriffe über Internet, Intranet, und Verwaltungs- bzw. Unternehmensnetze unterschieden werden. Der Cloud-Anbieter muss geeignete Mechanismen implementieren, um Mandanten und Zugriffsnetze sicher voneinander zu trennen und den Übergang zwischen den Netzen, wo erforderlich und zulässig, in sicherer Form zu ermöglichen. Technisch sind die Ressourcen und Daten unterschiedlicher Kunden durch native Cloud-Mechanismen so voneinander abzugrenzen, dass wechselseitige Zugriffe auf die jeweiligen Datenbestände nur dann möglich sind, wenn diese zwingend notwendig sind.

Beim Angebot von Cloud-Diensten sind zwei Situationen zu unterscheiden: die Migration existierender IT-Dienstleistungen in die Cloud und die Bereitstellung neuer Cloud-Dienste. Existierende IT-Dienste nutzen die IT-Infrastruktur ihres IT-Anbieters. Darunter sind Betriebssysteme, Middleware, Datenbanken und spezielle Plattformen wie eine eGovernment-Suite mit Formularserver, Dokumentenmanagement usw. zu verstehen. Diese

[24] SAGA-Spezifikation, http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

Infrastruktur ist im Allgemeinen lizensiert. Für Betrieb und Wartung existieren zumeist Verträge und interne Prozesse (Governance). Mitarbeiter sind speziell geschult. In dieser Situation ist zu entscheiden, ob die existierende IT-Infrastruktur in die Cloud portiert wird oder ob die existierenden IT-Dienstleistungen auf die in der Cloud existierende Cloud-Infrastruktur aufgesetzt werden. Im ersten Fall besteht die Gefahr, dass die IT-Infrastruktur nur eingeschränkt von der Cloud unterstützt wird. Dafür können die Dienste unverändert übernommen werden. Im zweiten Fall wird die Infrastruktur optimal unterstützt, dafür müssen die Dienste angepasst werden. Eine Abwägung zwischen Investitionsschutz und nachhaltigen Einsparungen sowie Abschätzungen von technischem Migrationsaufwand, Schulungsaufwand und Änderungsaufwand für Governance sind durchzuführen.

Bei der Bereitstellung neuer Cloud-Dienste spielt der Migrationsaufwand eine geringere Rolle. Es ist aber ebenfalls zu beachten, dass der Betrieb einer Cloud-Infrastruktur mit den darüber angebotenen Diensten einen erheblichen Aufwand an Schulungen und Anpassungen von betrieblichen Prozessen bedeutet. Je moderner das Dienstangebot ohne Cloud ist (Virtualisierung, modulare Systemarchitektur), desto stärker ist auf die Verträglichkeit der vorhandenen mit den cloud-basierten Konzepten für Erstellung und Betrieb der Software zu achten. Je älter das Dienstangebot ohne Cloud ist, desto größer ist der architektonische, technische und organisatorische Sprung in die Cloud.

5.4 SICHERHEIT

Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit müssen auch in der Cloud gewährleistet werden. Ob und unter welchen Bedingungen Daten und Anwendungen der öffentlichen Verwaltung in die Cloud verlagert werden können, hängt von deren Schutzbedürftigkeit ab. Diese kann nur durch eine individuelle Sicherheitsanalyse ermittelt werden.

Einen kompakten Einstieg und Überblick über Informationssicherheit in der Cloud liefert das BSI-Eckpunktepapier zum Cloud-Computing, in dem die wichtigsten organisatorischen, personellen, infrastrukturellen und technischen Maßnahmen beschrieben werden.[25]

Eine Detaillierung von Risiken und Maßnahmen erfolgt in den neuen IT-Grundschutzbausteinen »Cloud Management« für Cloud-Dienstanbieter und »Cloud-Nutzung« für die Nutzer, die als Grundlage für das Festlegen von angemessenen Sicherheitsanforderungen dienen. Ergänzend sind auch die Bausteine »Virtualisierung« und »Speicherlösungen/Cloud Storage« zu beachten.[26]

Das Ziel des Bausteins »Cloud Management« ist, Empfehlungen für sichere Bereitstellung, Verwaltung und Betrieb von Cloud-Diensten zu geben. Die Gefährdungen und Maßnahmen für das Cloud Management werden dargestellt und umfassen die Bereiche Mandantenfähigkeit, Orchestrierung[27] von Cloud-Ressourcen und Automatisierung in der Cloud-Verwaltung. Primär richten sich die Beschreibungen von Gefährdungen und Maßnahmen an Cloud-Dienstanbieter, die Dienste für KMUs und Behörden aus der privaten Cloud heraus bereitstellen.

Im Baustein »Cloud-Nutzung« wird die Auswahl und Vertragsgestaltung mit Cloud-Dienstanbietern, deren Auditierung, die Planung der Migration, sichere Kommunikation mit dem Anbieter, Integration in das Sicherheitskonzept und die Notfallvorsorge behandelt. Wesentlich für die Entscheidung für einen Cloud-Dienstanbieter ist, dass vertrauenswürdige Anbieter transparent darlegen, welche Sicherheitsmaßnahmen zum

[25] BSI, Cloud-Computing Eckpunktepapier, Februar 2012, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html
[26] BSI, Vorabversion Grundschutz-Bausteine Cloud-Management, Cloud-Nutzung, Virtualisierung und Speicherlösungen/Cloud Storage, 2014 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Download/download_node.html
[27] Oberbegriff für Provisionierung und De-Provisionierung eines Dienstes, d. h. der Vorgang seiner Bereitstellung bzw. seiner Abschaltung.

Standardangebot gehören, welche zusätzlich eingekauft werden können, und für welche Sicherheitsmaßnahmen die Kunden selbst verantwortlich sind.

Der Baustein »Virtualisierung« beschreibt, wie Virtualisierungstechnologien in den Informationsverbund eingebracht werden können und unter welchen Voraussetzungen virtuelle Infrastrukturen sicher betrieben werden können.

Der Baustein »Speicherlösungen/Cloud Storage« bezieht sich allgemein auf den Betrieb von Speicherlösungen, beschreibt jedoch auch Sicherheitsrisiken und -anforderungen, die sich aus der Verwendung von Datenspeicher, der als Cloud-Dienst bereitgestellt wird, ergeben.

Für Sicherheitsmaßnahmen, mit denen die Cloud-Anwendungen selbst abgesichert werden können, sind die Grundschutzbausteine Webanwendungen und Webservices relevant.

6. FAHRPLAN: IN FÜNF STATIONEN IN DIE CLOUD

Der folgende »Fahrplan«, also die Beschreibung eines Prozesses, ist notwendigerweise unvollständig: Im Kontext dieser Informationsschrift ist es nicht möglich, z. B. jeden Aspekt einer Beschaffungsmaßnahme im öffentlich-rechtlichen Umfeld zu behandeln. Wir konzentrieren uns deshalb auf solche Themen, die für den spezifischen Fall der Migration von IT-Diensten in die Cloud relevant sind. Es ist noch zu bemerken, dass – obwohl wir uns auf das Szenario »private Cloud« konzentrieren – die meisten der im Folgenden angestellten Überlegungen unabhängig vom konkreten Betriebsmodell des Dienstanbieters sind: Ein Anbieter öffentlicher Cloud-Dienste, der alle Anforderungen der Ausschreibung erfüllt, ist ein durchaus valider Anbieter für eine Behörde (vgl. hierzu aber auch die Diskussion in Abschnitt 1.5).

6.1 GRUNDSÄTZLICHE ÜBERLEGUNGEN

Bevor die Reise losgehen kann, sind einige grundsätzliche Überlegungen anzustellen.

– Wie in den vorhergehenden Abschnitten dargestellt, bietet die Cloud große Potenziale, beinhaltet aber auch Risiken, die im Augenblick aus der behördlichen Perspektive nur schwer abzuschätzen sind. Dies wird sich mit der Durchführung erfolgreicher Cloud-Migrationen oder innovativen Nutzungen der Cloud durch die Verwaltungen in der Zukunft ändern. Im Augenblick muss jedoch zur Vorsicht geraten werden: Beispiele für gescheiterte ÖPP-Modelle und Outsourcing-Vorhaben gibt es seit Jahren in auskömmlicher Zahl. Deshalb ist die Entscheidung für die Cloud kritisch zu hinterfragen: Herkömmliche IT-Dienstleister oder eine Modernisierung der internen IT sollten als Alternativen stets berücksichtigt werden.
– Auch der Weg in die Cloud ist angemessen durch Rückfall- und Exit-Strategien abzusichern. Es gilt: Je weiter ein Vorhaben voranschreitet, desto gravierender sind die wirtschaftlichen, technischen und organisatorischen Auswirkungen eines Scheiterns. Einige Beispiele:

- Können Mittel zur Wiederbeschaffung eigener IT kurzfristig bereitgestellt werden?
- Ist eine Wiederherstellung der alten Organisationsstruktur möglich?
- Kann versetztes oder abgebautes Personal kurzfristig wieder eingestellt oder zurückversetzt werden?
- Stellt der Markt genügend alternative Anbieter zur Verfügung, falls der ursprünglich gewählte Anbieter aufgrund von Unzuverlässigkeit, Insolvenz oder erheblichen Preissteigerungen gewechselt werden muss?
- Ist die Wiedergewinnung von Daten mit vertretbarem technischem und finanziellem Aufwand möglich?

6.2 STATION 1: BEDARFSANALYSE

Am Anfang einer jeden Migration in die Cloud muss eine Bedarfsanalyse erfolgen, d. h. die Bestandsaufnahme und Identifikation von Funktionen, die ausgelagert werden können. Für neue Dienstleistungen ist es ebenso erforderlich, die notwendigen Bedarfe zu identifizieren und mit der IT-Strategie der Behörde abzustimmen.

Im Einzelnen muss die Bedarfsanalyse die im Folgenden beschriebenen Themen behandeln. Es ist dabei wichtig, diese Bereiche nicht als kausale Abfolge von Schritten zu verstehen (Erstens: Zielsetzung; Zweitens: Anforderung definieren; usw.), sondern als sich gegenseitig beeinflussende Themen: Sollte z. B. die Marktanalyse zeigen, dass Anforderungen durch augenblicklich verfügbare Anbieter nicht erfüllt werden können, ist die Anforderungsliste im Rahmen der Zielsetzungen des Migrationsprojekts zu variieren. Zudem sollte berücksichtigt werden, dass in den vorbereitenden Phasen einer Beschaffung ein Dialog mit potenziellen Anbietern durchaus möglich ist. Eine frühzeitige Einbeziehung behördlicher und privatwirtschaftlicher Anbieter für Cloud-Lösungen ist hilfreich, um das Verständnis für Anforderungen einerseits und technische und wirtschaftliche Potenziale andererseits zu schärfen.

Zielsetzung. Welche Ziele sollen durch die Auslagerung erreicht werden? Geht es um die Verlagerung von Anschaffungs- auf operative Kosten für ein spezifisches Fachverfahren? Ist die primäre Motivation die Nutzung externer Kompetenz, die im eigenen Haus nicht vorhanden ist? Oder soll ein neues Projekt die hauseigenen Ressourcen nicht belasten?

Anforderungsdefinition. Welche technischen und geschäftlichen Anforderungen ergeben sich aus dem geplanten Vorhaben? Hierbei ist darauf zu achten, dass Anforderungen möglichst anbieter- und technologieneutral beschrieben werden, um Abhängigkeiten zu vermeiden. Auch ist darauf zu achten, dass Interoperabilitäts- und Portabilitätsanforderungen formuliert werden: Es muss möglich sein, den Anbieter mit vertretbarem finanziellem und technischem Aufwand zu wechseln.

Marktanalyse und Markterkundung. Weiterhin ist die Frage zu beantworten, ob der Markt überhaupt Dienstleistungen bereitstellt, die diese Anforderungen erfüllen. Deshalb sind potenzielle Anbieter zu identifizieren und deren Angebot zu prüfen. Vorbereitend zur eigentlichen Beschaffung sollte hier bereits ein Dialog mit potenziellen Anbietern angestrebt werden. Weiterhin ist festzulegen, für welche Anforderungen eine Anpassung an die Marktsituation überhaupt möglich ist (z. B. ist ein angemessenes Sicherheitsniveau immer zu gewährleisten).

Kosten/Nutzenanalyse. Schließlich sind die voraussichtlichen Kosten der Migration und des anschließenden Betriebs gegen den angestrebten Nutzen aufzuwiegen. Hierbei sind einerseits die Kosten des augenblicklichen Betriebs (oder Investitionskosten) zu berücksichtigen, andererseits müssen Qualitätsmerkmale der augenblicklich vorhandenen Lösungen in Beziehung zu potentiellen Cloud-Angeboten gesetzt werden. Schließlich muss auch die Frage beantwortet werden, ob eine Modernisierung der eigenen IT-Infrastruktur (also z. B. die Implementierung einer privaten Cloud innerhalb der eigenen Organisation) einer Dienstauslagerung vorzuziehen ist.

6.3 STATION 2: RISIKOANALYSE

Eine Risikoanalyse setzt sich immer aus den folgenden Elementen zusammen:

- Identifikation potenzieller Gefährdungen und die Einschätzung ihrer Eintrittswahrscheinlichkeit sowie der potentiellen Schadenshöhe im Falle des Eintritts.
- Identifikation geeigneter Gegenmaßnahmen und ihres Aufwands bzw. ihrer Kosten.
- Bewertung der Auswirkungen des Eintretens einer Gefährdung, sollten Gegenmaßnahmen erfolglos sein.
- Definition von Maßnahmen zu deren Steuerung von Restrisiken.

Die Risikoanalyse zielt also primär nicht darauf ab, Gefährdungen grundsätzlich zu eliminieren, sondern darauf, Risiken zu managen: Risiken mit geringer Eintrittswahrscheinlichkeit und niedrigem Schadenspotenzial können möglicherweise einfach akzeptiert werden, da die Implementierung entsprechender Gegenmaßnahmen höhere Kosten als der eigentliche Schadensfall verursacht. Im behördlichen Umfeld ist allerdings noch zu berücksichtigen, dass bestimmte Risiken unter keinen Umständen akzeptiert werden können, z. B.:

- Gefährdung der behördlichen Kernaufgaben,
- Gefährdung der Grundrechte des Bürgers sowie Rechte juristischer Personen.

Risiko- und Bedarfsanalyse können nicht unabhängig voneinander durchgeführt werden. Aus identifizierten Risiken können sich zusätzliche oder modifizierte Anforderungen, eine Neubewertung der Marktsituation oder eine veränderte Einschätzung der Kosten der angestrebten Cloud-Lösung ergeben. Dabei ist ein angemessenes Sicherheitsniveau zu gewährleisten: Bei zu hohen Kosten ist der Eintritt in die Cloud kritisch zu hinterfragen.

Wie schon im Zusammenhang mit der Bedarfsanalyse (Abschnitt 6.2) dargestellt, ist die Einbeziehung potenzieller Anbieter empfehlenswert, um Risiken und die Effektivität entsprechender Gegenmaßnahmen und die Auswirkungen ihres Versagens realistisch einschätzen zu können. Hierzu bietet sich die Verwendung einer etablierten Methodik an, wie sie z. B. in den ISO-Normen der 31000-er Reihe beschrieben wird.[28]

Im Einzelnen sollte die Risikoanalyse die folgenden Punkte behandeln:

Sicherheit. Sicherheitsanforderungen sind im behördlichen Umfeld von primärer Bedeutung. Allerdings sollte berücksichtigt werden, dass nicht alle Daten und Prozesse, die im Rahmen des Migrationsvorhabens in die Cloud ausgelagert werden sollen, ein gleichermaßen hohes Schutzniveau haben: Der Betrieb einer öffentlich zugänglichen Webseite, die allgemeine Bürgerinformationen zur Verfügung stellt, wird anders zu bewerten sein als die Speicherung von personenbezogenen Daten. Es gilt: Erhöhte Sicherheit verursacht erhöhte Kosten.

Im Übrigen sollte eine der etablierten Methoden zur Risikoanalyse verwendet werden, z. B.:

- Die Risikoanalyse auf der Basis von IT-Grundschutz des BSI.[29]
- Die bereits erwähnten ISO-Normen der 31000-er Reihe zum Thema Risikomanagement.
- Speziell im Zusammenhang mit Cloud-Computing ist auch der ENISA-Report zur Sicherheits-Einschätzung von Cloud-Diensten zu nennen.[30]

Konformität. Neben rechtlichen Konformitätanforderungen (vgl. Abschnitt 4.1) sind hier insbesondere auch Anforderungen zur Dienstqualität (z. B. nach ISO 9000)[31] und zum Dienstmanagement (z. B. nach ISO/IEC 20000 oder ITIL)[32] zu nennen. Schließlich ist Vertragskonformität sicherzustellen.

Kontrolle. Im Unterschied zur Inhouse-IT, die direkt innerhalb der Behörde gesteuert werden kann, erfolgt die Steuerung eines externen Dienstleisters meist über Dienstgütezusicherungen (*service level agreements*, SLAs). Daraus ergeben sich einerseits Implikationen bzgl. der Vertragsgestaltung mit dem Anbieter (Welchen Funktionsumfang und Dienstqualität darf die beauftragende Behörde erwarten? Welche Möglichkeiten zur Einflussnahme sind gegeben? Was geschieht, wenn eine Zusicherung verletzt wird?), andererseits sind auch technische und organisatorische Aspekte zu berücksichtigen: Moderne Cloud-Dienste stellen Überwachungswerkzeuge (Monitoring) zur Verfügung, die eine direkte Überprüfung der Dienstqualität durch den Kunden erlauben und damit einen direkten Nachweis von Verletzungen der Dienstgütevereinbarung ermöglichen. Die Nutzung solcher Überwachungsfunktionen muss aber in der technischen Infrastruktur und den Organisationsstrukturen des Kunden etabliert werden.

Umstellung der eigenen Organisation. Die Auswirkungen der Auslagerung von internen IT-Funktionen in die Cloud auf die Organisationsstruktur der auslagernden Behörde dürfen nicht unterschätzt werden. Deshalb ist es notwendig, interne Prozesse möglichst genau zu erfassen und ihr Verhältnis zu den genutzten IT-Diensten zu verstehen. Weiterhin sollten alle beteiligten Ebenen frühzeitig eingebunden werden, um einen konfliktfreien Migrationsprozess zu gewährleisten.

---

[28] ISO 31000 Risk Management, http://www.iso.org/iso/home/standards/iso31000.htm

[29] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Bundesamt für Sicherheit in der Informationstechnik, 2008, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Risikoanalyse/risikoanalyse_node.html

[30] European Network and Information Security Agency (ENISA), Cloud Computing - Benefits, risks and recommendations for information security, ENISA, 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[31] ISO 9000 Qualitätsmanagement, http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

[32] Die Information Technology Infrastructure Library (ITIL) ist ein insbesondere auch in Deutschland akzeptierter Ansatz zum Management von IT-Dienstleistungen, http://www.itil-officialsite.com/home/home.asp

Migrationsrisiken. Schließlich ist der Transformationsprozess, der von der Verwendung der eigenen Infrastruktur zur Nutzung von Cloud-Diensten führt, mit Risiken behaftet. Kann die Durchführung behördlicher Aufgaben während der Migration gewährleistet werden? Ist mit Leistungseinbußen zu rechnen? Wie kritisch sind deren Auswirkungen? Was geschieht, wenn die Migration insgesamt scheitert (z. B. aufgrund einer unerfüllbaren Anforderungsdefinition)?

6.4 STATION 3: WAHL EINES AUSSCHREIBUNGSVERFAHRENS

In Abhängigkeit von der Komplexität und Detailliertheit der Leistungsbeschreibung besteht für die Behörde ein gewisser Spielraum bzgl. der Wahl des geeigneten Ausschreibungsverfahrens. Dabei sind die rechtlichen Aspekte bereits in Abschnitt 5.1 diskutiert worden. Deshalb soll an dieser Stelle nur noch auf Cloud-spezifische Aspekte hingewiesen werden:

Cloud-Computing ist nicht nur eine Neuauflage klassischer Dienstleistungsmodelle; wie die Betrachtungen in dieser Informationsschrift zeigen, hat die Nutzung von Cloud-Diensten insbesondere auch organisatorische und technische Implikationen, die Auswirkungen auf die Art haben, in der behördliche Aufgaben erfüllt werden. Deshalb müssen Risiken möglichst sowohl auf Kunden- als auch auf Anbieterseite verstanden und Migrationsszenarien durch beide Seiten planbar gemacht werden. Dementsprechend sollte die Verfahrenswahl auch unter dem Gesichtspunkt der Förderung eines offenen Dialogs erfolgen.

6.5 STATION 4: AUFTRAGSVERGABE

Damit der Auftraggeber (Behörde) eine Auswahl treffen kann, ist die eindeutige Beschreibung der Zuschlagskriterien notwendig. Im Rahmen von Cloud-Computing sind neben Kostenaspekten insbesondere folgende Kriterien von Bedeutung: Erreichbarkeit, Verfügbarkeit und wohldefinierte Dienstgütevereinbarung.

Die Bewertung der Eignung des Anbieters bezieht sich auf seine juristische Person: Die grundsätzliche Eignung eines Bieters muss positiv festgestellt werden, bevor Wertungs- und Zuschlagkriterien auf das Angebot angewendet werden.

Die beauftragende Behörde wird also die wirtschaftliche und finanzielle Leistungsfähigkeit eines potentiellen Anbieters berücksichtigen. Darüber hinaus sind auch datenschutzrechtliche Vorgaben von Interesse: Der Anbieter muss sich zu relevanten rechtlichen, technischen und organisatorischen Standards verpflichten (hierzu kann auch zählen, dass Daten und Prozesse nur auf europäische bzw. deutsche Rechenzentren ausgelagert werden).

Bei der Gestaltung des Vertrags ist folgendes zu beachten:

- Mängelrechte und ggf. Vertragsstrafen sind zu vereinbaren: Welche Haftungs- und Gewährleistungsrechte gelten im Fall einer Störung des Dienstbetriebs?
- Auch die Haftung des Kunden gegenüber dem Anbieter ist zu berücksichtigen (z. B.: Schädigung des Anbieters durch die Nichteinhaltung von Sicherheitsstandards durch den Kunden). Ohne explizite vertragliche Regelung haftet der Kunde nach den allgemeinen gesetzlichen Vorschriften.
- Um das Vorliegen von Mängeln nachzuweisen, sollten leistungsorientierte Bestandteile der Dienstleistung präzise formuliert werden und sich auf überprüfbare Eigenschaften der Diensterbringung beziehen (z. B. Verfügbarkeit[33], Support, Reaktionszeiten, maximale Ausfallzeit usw.); zu dem sind

[33] Eine Verfügbarkeit von 99 % im Jahr bedeutet immer noch, dass die Systeme eines Anbieters fast vier Tage im Jahr ausfallen können, ohne dass dies vertragswidrig wäre. Die Verfügbarkeit von IT-Dienstleistungen ist für behördliche Kunden außerordentlich wichtig.

Rechtsfolgen bei der Verletzung der vereinbarten Leistungsparameter festzulegen.
- Zu dem sollten Kündigungsrechte der Vertragsparteien eindeutig formuliert werden. Dies umfasst insbesondere Fristen für eine ordentliche Kündigung und etwaige Sonderkündigungsrechte, also vor allem, wann ein wichtiger Grund im Sinne des § 314 BGB vorliegt. Um ein »lock-in« zu vermeiden, sollte zusätzlich darauf geachtet werden, dass eine Strategie für ein Exit-Management vertraglich festgelegt wird. Dies schließt ein:

    - Die Einräumung der Möglichkeit einer angemessenen Verlängerung der Dienstleistung, um die Beeinträchtigung der Geschäftsprozesse des Kunden möglichst gering zu halten.
    - Mechanismen zur Unterstützung bei der Daten-Rückübertragung.
    - Die Unterstützung beim Transfer von Know-how und sonstige Leistungen zur De-Migration.

6.6 STATION 5: MIGRATION

Zur Vorbereitung der eigentlichen Migration müssen die folgenden Fragestellungen beantwortet werden:

- Welche technischen Systeme werden auf einen Betrieb aus der Cloud umgestellt? (Dies sollte allerdings bereits in der Bedarfsanalyse-Phase geklärt werden).
- Welche technischen Systeme innerhalb der eigenen Infrastruktur sind betroffen? Dies betrifft mit Sicherheit Netzwerkkonfigurationen, Datenbanken, Komponenten zur Nutzerverwaltung usw.
- Welche organisatorischen Änderungen werden durch die Verwendung von Cloud-Diensten notwendig. Sind Kompetenzen und Berechtigungen entsprechend angepasst? Sind die entsprechenden Personen ausreichend geschult?
- Ist ein Sicherheitskonzept verfügbar, das die neue Organisation berücksichtigt?
- Ist ein Konzept verfügbar, das das Migrationsvorhaben in Einzelschritte unterteilt und dabei für jeden Schritt Erfolgskriterien und Fallback-Strategien definiert?

Grundsätzlich existieren drei verschiedene Migrationsverfahren:

- **Big Bang.** Bei diesem Verfahren werden alle zu migrierenden Dienste auf einmal für alle Benutzer gleichzeitig umgestellt. Dieses Szenario erfordert gute Planung und i. d. R. einige Testmigrationen. Ein Big Bang ist dort anzuwenden, wo ein Doppelbetrieb kostenintensiv oder organisatorisch schwer durchführbar ist. Die Definition effektiver Fallback-Strategien ist meist eine komplexe Aufgabe.
- Die **schrittweise Migration** erfolgt in mehreren Phasen, in denen jeweils eine Gruppe von Benutzern oder ein bestimmtes Teilsystem umgestellt werden, wobei ein Doppelbetrieb nur jeweils für eine Phase aufrechterhalten werden muss. Die Komplexität einer solchen Migrationsstrategie ist gut beherrschbar; insbesondere können Erfahrungen aus einer Migrationsphase sofort in der darauffolgenden umgesetzt werden. Es ist jedoch zu beachten, dass nicht alle Migrationsvorhaben einfach in Einzelschritte zerlegbar sind.
- Der **optionale Pilotbetrieb** kann in Verbindung mit den vorher genannten Strategien verwendet werden. Hierbei wird die Migration für eine ausgewählte Benutzergruppe prototypisch durchgeführt. Die hierbei gewonnenen Erfahrungen werden bei der Planung der eigentlichen Migrationsdurchführung berücksichtigt.

7. AUSBLICK

Die Migration von IT-Funktionen in die Cloud ist ein komplexer Vorgang, der eine hohe Anzahl von Themenfeldern aus verschiedenen Bereichen berührt. Diese Informationsschrift versucht querschnittshaft einen Überblick über diese Themen zu verschaffen und diskutiert das rechtliche, technische und organisatorische Umfeld unter besonderer Berücksichtigung des Themas Sicherheit. Dabei wurde versucht, jeweils solche Fragestellungen zu adressieren, die sich aus der besonderen Herausforderung des Cloud-Computing ergeben. Die Informationsschrift intendiert zum Beispiel nicht, dem Leser einen vollständigen Wegweiser zur Durchführung einer Ausschreibung für IT-Dienstleistungen zu geben, sondern konzentriert sich auf die Punkte, die in der spezifischen Situation »Migration in die Cloud« wichtig sind.

Der »Fahrplan« behandelt die Migration von Inhouse-IT in die Cloud. Die Metapher »Fahrplan« legt dabei nahe, dass mit der Durchführung von Schritt Fünf die Endstation erreicht sei. Das ist jedoch nicht der Fall. Eine Behörde sollte fortlaufend prüfen, ob Cloud-Projekte zur Steigerung der Effizienz der Aufgabenerfüllung führen können, und auch für bereits ausgelagerte Projekte stets validieren, ob die geplanten Zielsetzungen erreicht werden konnten: Im Zweifelsfall ist auch ein »Insourcing« zu erwägen.

Die Cloud bietet die Möglichkeit, IT-Dienstleistungen ohne hohe Investitionsaufwände und innerhalb kürzester Zeit in Anspruch zu nehmen. Die sich daraus ergebende Flexibilisierung der IT-Landschaft innerhalb der Behörde, aber auch zwischen Behörden und zum Bürger, erhöht sicher die Komplexität der damit verbundenen Beschaffungs- und Betriebsprozesse. Allerdings bieten sich auch Chancen zur Optimierung der Verwaltung, die nicht ungenutzt bleiben sollten.

ABKÜRZUNGEN

BDSG	Bundesdatenschutzgesetz
BMWi	Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
ENISA	European Network and Information Security Agency
ETSI	European Telecommunication Standards Institute
EU	Europäische Union
FuE	Forschung und Entwicklung
IaaS	infrastructure as a service, Infrastruktur als Dienst
IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnologie
ITDZ	IT-Dienstleistungszentrum Berlin
KMU	Kleine und mittlere Unternehmen
LDI	Landesbetrieb Daten und Informationen
NSA	National Security Agency – US-amerikanischer Nachrichtendienst
OSS	operational support systems, Betriebsunterstützungssysteme
PaaS	platform as a service, Plattform als Dienst
SaaS	software as a service, Software als Dienst
SLA	service level agreement, Dienstgütezusicherung
UrhG	Urheberrechtsgesetz
VS	Verschlusssache
VSA	Verschlusssachen-Anweisung

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 1404 (Grafik: Fraunhofer FOKUS)