Mythen rund um Cloud Computing

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland

Stand: Dezember 2015

Microsoft

Sicherheit

Mythos:

Die Cloud ist unsicherer als mein eigenes Rechenzentrum

Aussage: Richtig ist, dass der Betrieb eines Cloud-Rechenzentrums sehr aufwändig ist.

Diese werden von einer Vielzahl von Spezialisten entwickelt und betrieben. Dementsprechend haben Cloud-Rechenzentren regelmäßig einen sehr hohen IT-Sicherheitsstandard, oftmals ist dieser höher als in einem vom Kunden selbst betriebenen Rechenzentrum.

Dies bestätigt u.a. auch eine Analyse von Gartner.

Microsoft

http://www.gartner.com/newsroom/id/2889217

Mythos:

Daten sind in der Cloud nicht sicher. Deswegen darf ein deutsches Unternehmen das Risiko nicht eingehen

Aussage:

Richtig ist, dass die Geschäftsleitung eines Unternehmens bei der Einschaltung von IT-Dienstleistern immer eine Risikoabwägung vornehmen muss.

Dies kann dazu führen, dass Unternehmen sich entscheiden, bestimmte Datenverarbeitungen (wie Forschung & Entwicklung) ausschließlich mit eigenem Personal, „on premise“ und auf Hardware ohne Internetverbindung durchzuführen.

Für den weitaus größten Teil der Datenverarbeitung ist eine Datenverarbeitung in der Cloud aus Risikogesichtspunkten grundsätzlich nicht ausgeschlossen.

Microsoft

Strafbarkeit

Microsoft

Mythos:

Bei einem amerikanischen Anbieter greifen die Support-Mitarbeiter aus der ganzen Welt auf meine Daten zu. Dadurch kann ich mich strafbar machen

Aussage: Richtig ist, dass außer-europäische Microsoft Support-Mitarbeiter nur in seltenen Fällen Zugang zu Kundendaten benötigen, nämlich außerhalb der Betriebszeiten in der EU und sofern die Problemlösung im Einzelfall einen solchen Zugang erfordert.

Die Tatsache, dass ein Zugriff geografisch aus den USA erfolgt, führt jedenfalls an sich nicht zu einer Strafbarkeit.

Microsoft

Mythos:

Es gibt so viele branchenspezifische Gesetzgebungen und auch Strafnormen, die es nicht erlauben Cloud Computing zu nutzen. Beispielsweise für Anwälte, Krankenhäuser, Versicherungen, …

Aussage:

Richtig ist, dass diese Regelungen nur in vergleichsweise wenigen Branchen gelten, nämlich für Berufsträger im Gesundheitsbereich, in den freien Berufen (Anwalt, Wirtschafts-/Buchprüfung, Steuern), für Mitarbeiter in öffentlich anerkannten Sozialberatungsstellen und im privaten Kranken-, Unfall- oder Lebensversicherungsbereich. Auch für die öffentliche Hand gelten besondere Geheimhaltungspflichten.

Das bedeutet aber nicht, dass Cloud Computing immer unzulässig oder gar strafbar wäre. Wenn z.B. technisch durch Verschlüsselung eine Kenntnis des Cloud Anbieters vom Inhalt der Daten ausgeschlossen ist, ist die Nutzung auch nach diesen branchenspezifischen Normen zulässig.

Dieses rechtliche Risiko ist übrigens nicht Cloud-spezifisch, sondern gilt immer, wenn solche Geheimnisträger IT-Dienstleister für die Datenverarbeitung einschalten.

Datenschutz & Compliance

Microsoft

Mythos:

Die Nutzung der Cloud ist aus Datenschutz-, Datensicherheits- bzw. Compliancegründen unzulässig

Aussage: Richtig ist, dass es sich um drei unterschiedliche Aspekte handelt, die jeweils separat bewertet werden müssen.

Microsoft stellt hierzu transparent für diese drei Bereiche Informationen für seine Kunden und Partner zur Verfügung.

- Office 365 Trust Center: https://products.office.com/de-de/business/office-365-trust-center-cloud-computing-security
- Azure Trust Center: https://azure.microsoft.com/de-de/support/trust-center
- CRM Online Trust Center: http://www.microsoft.com/en-us/trustcenter/CloudServices/Dynamics
- Intune Trust Center: http://www.microsoft.com/de-de/server-cloud/products/intune-trust-center/overview.aspx

Microsoft

Mythos:

Die Nutzung einer Cloud ist unzulässig, weil ich kein Auditrecht habe

Aussage: Richtig ist, dass Microsoft vertragliche Auditrechte vorsieht. Grundsätzlich kommt der Kunde seiner datenschutzrechtlichen Verpflichtung zur Überprüfung der IT-Sicherheit nach, indem Microsoft seine Rechenzentren jährlich durch externe Auditoren überprüfen lässt. Dem Kunden wird es ermöglicht, diese Prüfberichte einzusehen.

Microsoft

Verarbeitung im Ausland

Microsoft

Mythos:

Ganz aktuell: Der Rat der IT Beauftragten der Bundesressorts empfiehlt nur die deutsche Cloud (Beschluss 2015/5)

Aussage: Richtig ist, dass die Empfehlung nur für Einrichtungen des Bundes gilt und nur für schützenswerte Informationen (z.B. Betriebs- und Geschäftsgeheimnisse oder sensible Informationen über IT-Infrastrukturen des Bundes).

Sie gilt gerade nicht für die Privatwirtschaft oder die Verwaltung der Länder. Ab 2016 bietet Microsoft die Microsoft Cloud Technologie auch aus deutschen Rechenzentren an.

Microsoft

Mythos:

Es macht einen großen Unterschied, ob das Rechenzentrum in Deutschland oder in einem anderen EU-Staat steht

Aussage:

Richtig ist, dass es grundsätzlich aufgrund der Waren- und Dienstleistungsfreiheit in der EU für den Kunden rechtlich keinen Unterschied macht, wo das Rechenzentrum in der EU steht.

Nur soweit in der Cloud Dokumente verarbeitet werden, die steuerrechtlich relevant sind, kann eine Genehmigung der Steuerbehörden für die Nutzung außerhalb Deutschlands erforderlich sein.

Wenn Kunden in der Cloud steuerrelevante Daten speichern wollen und keine solche Genehmigung einholen möchten, können sie ab 2016 auch die Microsoft Cloud Technologie mit deutschem Rechenzentrum nutzen.

Microsoft

Mythos:

Personenbezogene Daten dürfen nicht außerhalb der EU verarbeitet werden

Aussage: Richtig ist, dass eine Übermittlung an Stellen außerhalb der EU (oder ein Zugriff von außerhalb der EU) nur dann zulässig ist, wenn bei dem Empfänger ein angemessenes Datenschutzniveau besteht. Microsoft nimmt den Datenschutz sehr ernst und hat seine Verträge der Datenschutzaufsicht zur Begutachtung vorgelegt.

Die in der Art. 29-Datenschutzgruppe zusammengeschlossenen Datenschutzaufsichtsbehörden der EU-Staaten haben daraufhin entschieden, dass die Microsoft Cloud Verträge die Anforderungen der EU-Standardvertragsklauseln an ein angemessenes Datenschutzniveau erfüllen.

Personenbezogene Daten dürfen auf dieser Basis auch außerhalb der EU verarbeitet werden.

Microsoft

Mythos:

Sensitive personenbezogene Daten (z.B. über die Gesundheit oder Religion) dürfen nicht außerhalb der EU verarbeitet werden

Aussage: Richtig ist, dass auch sensitive personenbezogene Daten außerhalb der EU im Rahmen der von Microsoft seinen Cloud Diensten standardmäßig zugrunde gelegten Auftragsdatenverarbeitung verarbeitet werden dürfen.

Dies ergibt sich aus der Rechtsprechung des Europäischen Gerichtshofs, der es den Mitgliedsstaaten verbietet, im nationalen Recht Beschränkungen vorzusehen, die in der EU-Datenschutzrichtlinie nicht enthalten sind.

Microsoft

Mythos:

Aufgrund der Safe-Harbor-Entscheidung des EuGH vom 6.10.2015 sind Clouds, die Datentransfers in die USA beinhalten, unzulässig

Aussage:

Richtig ist, dass der EuGH nur das Safe-Harbor-Abkommen für ungültig erklärt hat. Damit ist ein US-Datentransfer nicht per se unzulässig, sondern bleibt aufgrund anderer Rechtsgrundlagen weiterhin möglich.

Der EuGH hat festgestellt, dass nur er allein die Kompetenz besitzt, Rechtsakte der Unionsorgane für nichtig oder ungültig zu erklären. Ein solcher, weiterhin verbindlicher Rechtsakt für den Transfer von personenbezogenen Daten an Empfänger außerhalb der EU sind die sog. EU-Standardvertragsklauseln, auf die Microsoft den Datentransfer für seine Core Cloud Services stützt.

Microsoft

Mythos:

Die Datenschutzaufsichtsbehörden erteilen aufgrund der Safe-Harbor-Entscheidung keine Genehmigung für die Cloud Nutzung mehr

Aussage: Richtig ist, dass der Düsseldorfer Kreis, das Abstimmungsgremium der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, am 26. Oktober 2015 erklärt hat, für sog. Binding Corporate Rules und individualisierte Datenexportverträge ab sofort keine neuen Genehmigungen für Datentransfers in die USA zu erteilen.

Microsoft ist mit seinen Cloud Services hiervon nicht betroffen, weil es die Cloud Services weder auf Basis von Binding Corporate Rules noch auf Basis individualisierter Datenexportverträge erbringt.

Microsoft

Mythos:

Unsere Firma hat strenge Regelungen zum Datenschutz. Ein US Cloud Betrieb ist nicht erlaubt

Aussage: Richtig ist, dass sich die Datenschutzregelungen zunächst aus dem Gesetz ergeben. Natürlich kann jedes Unternehmen frei entscheiden, welche Anbieter es nutzen möchte und sich freiwillige Beschränkungen auferlegen.

Eine gesetzliche Pflicht zum Ausschluss von US Cloud Anbietern aus Gründen des Datenschutzes besteht jedenfalls nicht.

Microsoft

Mythos:

NSA, FBI und Co. können auf alle US Clouds zugreifen

Aussage: Richtig ist, dass Nachrichtendienste und Behörden in den USA wie in der EU einem gesetzlichen Auskunftsverfahren folgen müssen, wenn sie von einem Cloud Anbieter Informationen herausverlangen.

Gegen den Zugriff durch Geheimdienste setzt Microsoft u.a. Verschlüsselungstechnologien ein, auch in der Übermittlung von Daten zwischen ihren Rechenzentren.

Microsoft

Mythos:

Der Patriot Act erlaubt den amerikanischen Behörden Zugriff auf Kundendaten auch außerhalb der USA

Aussage:

Richtig ist, dass diese Rechtsfrage noch nicht abschließend geklärt ist. Insoweit ist in den USA ein gerichtliches Verfahren anhängig, das sich mit dieser Frage beschäftigt.

In den unteren Instanzen hat es zwar ein Urteil gegeben, das Microsoft zur Herausgabe von Daten aus seinem irischen Rechenzentrum auf Basis des US-Rechts verpflichtet hat. Dieses Urteil ist aber **nicht rechtskräftig** und Microsoft hat hiergegen Berufung eingelegt.

Microsoft ist – wie viele andere US-amerikanische IT-Anbieter auch – der Auffassung, dass das US-Recht keine Geltung im Ausland hat und sich US-Behörden über Rechtshilfeersuchen über die zuständigen europäischen Behörden Daten aus Rechenzentren in der EU herausgeben lassen müssen. Microsoft wird dieses Verfahren – wenn nötig – bis zum höchsten US-Gericht, dem US Supreme Court, führen, um seine Rechtsauffassung zu verteidigen.

Es hat im Übrigen bis zum Tag der Erstellung dieses Dokuments keinen Fall gegeben, in dem Microsoft einer US-Behörde Daten von einem deutschen Unternehmen herausgegeben hat. Überhaupt sind Daten von deutschen Unternehmenskunden noch nie an eine Behörde herausgegeben worden.

Microsoft

Mythos:

Die deutsche Microsoft Cloud ist auch nicht sicherer, die NSA bzw. US-Behörden werden dennoch die Daten herausverlangen können

Aussage:

Richtig ist, dass Kundendaten in der Microsoft Cloud in Deutschland vor US behördlichen oder richterlichen Anordnungen zusätzlich durch ein Datentreuhändermodell geschützt werden.

T-Systems agiert als Datentreuhänderin im Auftrag des Kunden und muss jede einzelne Datenherausgabe an Dritte freigeben. Microsoft selbst hat keinen Zugang zu den Daten ohne Freigabe von T-Systems und kann daher an US-Behörden keine Daten herausgeben.

T-Systems verpflichtet sich vertraglich gegenüber dem Kunden, dass eine Datenherausgabe nur nach deutschem Recht erfolgt.

Microsoft

Vertrag

Microsoft

Mythos:

Die SLAs amerikanischer Cloud Anbieter sind nicht „enterprise grade“, d.h. beim Ausfall des Service wird nur die ausgefallene Leistung nicht berechnet, während bei einer deutschen Cloud vom deutschen Provider Pönalen bezahlt werden

Aussage:

Richtig ist, dass das US-amerikanische Recht weitergehende Möglichkeiten des Haftungsausschlusses erlaubt als das deutsche. Letztlich sind Haftung und Vergütung zwei Seiten derselben Medaille.

Aufgrund geringerer Haftungsrisiken kann ein US-Anbieter ggf. günstiger anbieten. Für den Kunden ist es damit die kommerzielle Frage, welche Prämie ihm eine weitergehende Haftung im konkreten Anwendungsfall wert ist.

Microsoft