

von Maria Wastlschmid

Vertrauen in die Cloud – aber sicher?

Microsoft Azure ist eine offene und flexible Cloud-Plattform, die das schnelle Erstellen, Bereitstellen und Verwalten von Infrastruktur und Anwendungen in einem globalen Netzwerk von Rechenzentren ermöglicht, die von Microsoft verwaltet werden. Spätestens beim Thema „globales Netzwerk von Rechenzentren“ horchen die meisten auf und denken direkt an die Sicherheit ihrer Daten.

Auch für Microsoft stehen der Schutz und die Sicherheit der Daten ganz vorne. So streben wir seit vielen Jahren danach, im Hinblick auf Sicherheit, Datenschutz und Compliance bestmögliche Maßnahmen zu ergreifen, und sind dabei nach aktuellem Stand führend im Markt.

Der für Microsoft Azure Services zuständige Bereich kümmert sich um sämtliche Prozesse rund um innovative, nachhaltige, kosteneffiziente sowie hochverfügbare Ressourcen und bedient mit Diensten wie Azure, Bing, Hotmail, MSN, Office 365 und Xbox Live mehr als eine Milliarde Kunden und zwanzig Millionen Unternehmen in über 76 Märkten weltweit.

Die Microsoft-Rechenzentren liegen geografisch voneinander getrennt und erfüllen die wichtigsten Branchenstandards, wie etwa ISO/IEC 27001:2013, bezüglich Sicherheit und Zuverlässigkeit. Zusätzlich zu den umfassenden physischen Sicherheitsmechanismen für Rechenzentren, Netzwerke und

Mitarbeiter integriert Microsoft Azure Sicherheitsverfahren auf Anwendungs- und Plattformebene, um die Sicherheit für Anwendungsentwickler und Dienstadministratoren zu verbessern. Es werden regelmäßige Tests durchgeführt, um die Sicherheitskontrollen und -prozesse zu verbessern und die Dienste zu härten.

Ein besonders wichtiger Teil unseres Produkt- und Servicelebenszyklus ist der Datenschutz. Wir gehen mit unseren Maßnahmen transparent um und verwalten die von uns gespeicherten Daten verantwortungsbewusst. Beispielsweise die Microsoft Online Services Datenschutzerklärung dient als Leitlinie für Kunden und erläutert die für die Verwendung von Cloud-Diensten geltenden spezifischen Richtlinien.

Auch der Speicherort von Daten wirft häufig Fragen auf. Azure Nutzer können die geografische(n) Region(en) der Microsoft-Rechenzentren auswählen, in denen ihre Daten gespeichert werden. Aus Gründen der Datenredundanz behalten wir uns vor, Kundendaten an einen anderen Ort innerhalb einer geografischen Region (z. B. innerhalb Europas) zu übertragen. Blob- und Tabellendaten werden zum Beispiel zwischen zwei Teilregionen mit derselben Hauptregion repliziert, um im Fall großer Katastrophen zusätzliche Datenbeständigkeit zu bieten. Wir übertragen dagegen keine Kundendaten an Standorte außerhalb der geographischen Hauptregion, die der Kunde auswählt, es sei denn, es wäre erforderlich, um Kundensupport bereitzustellen, ein Problem mit dem Dienst zu beheben, rechtliche Bestimmungen einzuhalten oder wenn der Kunde eine derartige Übertragung von Kundendaten bei der Konfiguration des Kontos aktiviert.

Um trotzdem die strengen Datenschutzgesetze der EU einhalten zu können, verfügt Microsoft über die Zertifizierung des US-Handelsministeriums als sicherer Hafen („Safe Harbour“). Diese erlaubt die rechtmäßige Übertragung persönlicher Daten aus der EU zur Bearbeitung durch Microsoft an Orte außerhalb der EU.

Darüber hinaus bieten wir eine Datenverarbeitungsvereinbarung und Modellklauseln für EU-Verträge, die zusätzliche vertragliche Garantien im Zusammenhang mit der Übertragung persönlicher Daten für In-Scope-Dienste enthalten. Die EU-Datenschutzgruppe für Artikel 29 hat mit einer offiziellen Genehmigung die Umsetzung dieser EU-Modellklauseln durch Microsoft als übereinstimmend mit den strengen Datenschutznormen zertifiziert, die internationale Datenübertragungen durch die Firmen in ihren Mitgliedsstaaten regeln.

Damit erfüllt Microsoft die Datenschutzgesetze, die im Allgemeinen für die Bereitstellung einer Cloud Services-Plattform durch Microsoft gelten. Dennoch liegt es in der Verantwortung der Kunden, zu entscheiden, ob Microsoft Azure und die jeweiligen Anwendungen, die in Azure ausgeführt werden sollen, die entsprechenden Gesetze und Bestimmungen für die Branche und das Verwendungsszenario der Kunden erfüllen. Zur Unterstützung bei dieser Bewertung stellen wir detaillierte Informationen zu unseren Sicherheitskompatibilitätsprogrammen zur Verfügung.

Microsoft Azure strebt unter anderem die jährliche ISO/IEC 27001:2013-Zertifizierung durch die British Standards Institution (BSI) an sowie die jährliche Attestierung von SOC 1 und 2.

Weitere Details rund um das Thema Sicherheit, Datenschutz und Compliance haben wir Lesern im Vertrauenscenter auf der Azure-Webseite zur Verfügung gestellt und hoffen damit, ein wenig Klarheit in dieses komplexe Thema zu bringen: <http://azure.microsoft.com/de-de/support/trust-center/>



Maria Wastlschmid

hat an der Dualen Hochschule Ravensburg Betriebswirtschaftslehre studiert und verschiedene Positionen bei Advantest im Marketing und bei cosmobrandlab im Key Account Management besetzt. Vor sechs Jahren wechselte sie zu Microsoft Deutschland GmbH als Audience Marketing Manager, worauf sie in der Cloud & Enterprise Business Group nacheinander Forefront, System Center und nun Microsoft Azure als Produkt Manager verantwortete. Seit Anfang des Jahres ist sie im strategischen Business Development für Microsoft Azure tätig. Maria.Wastlschmid@microsoft.com



Microsoft Azure

Infografik

Die Microsoft-Infografik beschreibt detailliert, welche Sicherheitskomponenten bei Microsoft Azure zum Tragen kommen – von Authentifizierung und Zugang über Netzwerksicherheit, Verschlüsselung und Schutz der Privatsphäre bis hin zu umfassender Angriffsabwehr und der Einhaltung von internationalen Sicherheitsnormen und Zertifizierungen.



Download unter www.idl.eu/infografik-azure

Nur in englischer Version verfügbar