Sicher in die Cloud – Cloud Security für die öffentliche Verwaltung

pwc | Microsoft

www.pwc.de/cloudsecurity

In einer zunehmend digitalisierten Welt wird die Nutzung von Cloud-Diensten wie beispielsweise Microsoft Azure oder Microsoft 365 auch für Regierungsbehörden und öffentliche Institutionen immer wichtiger. Doch mit den Vorteilen der Cloud gehen auch Sicherheitsherausforderungen einher. Wie der Weg in die Cloud sicher gelingt, wie die optimale Cloud-Architektur aussieht und welche Maßnahmen ergriffen werden müssen, um die Daten in der Cloud sicher und compliant zu schützen, lesen Sie hier.

Chancen und Herausforderungen der Cloud

Chancen

Cloud-Lösungen wie Microsoft Azure sind wichtig für die öffentliche Verwaltung, weil …

- Cloud die Flexibilität mitbringt, die es für die Digitalisierung der öffentlichen Verwaltung braucht.
- Cloud eine effiziente Nutzung von Ressourcen sowie Kostenersparnissen ermöglicht.
- Cloud die Nutzung von verbreiteten Anwendungen, wie beispielsweise aus Microsoft 365, weiteren Tools oder generell modernen IT-Architekturen, ermöglicht.

Herausforderungen

Die Cloud ist herausfordernd für die öffentliche Verwaltung, weil …

- eine große Anzahl an Vorgaben in Bezug auf Sicherheit und Compliance eingehalten werden müssen (z. B. Rechtsvorschriften, Cybersicherheit, Datenschutz).
- bestehende Fachverfahren oder ganze IT-Architekturen neu aufgebaut oder transformiert werden müssen.
- wechselnde Anforderungen oder Vorgaben von der politischen Ebene beachtet werden müssen.
- vorhandene Kompetenzen und Prozesse in der Cloud nicht direkt anwendbar sind (z. B. Fachkräftemangel).

Für den Weg in die sichere Cloud gilt es, aus den relevanten Standards die wesentlichen Anforderungen und richtigen Maßnahmen abzuleiten.

Standards

Zu den grundlegenden Standards gehören zum Beispiel der IT-Grundschutz, der Mindeststandard für die Cloud und die Datenschutz-Grundverordnung (DSGVO). Diese bilden das Fundament für eine sichere Cloud-Nutzung, indem sie klare Richtlinien und Best Practices für den Umgang mit sensiblen Daten und Informationssystemen vorgeben.

Anforderungen

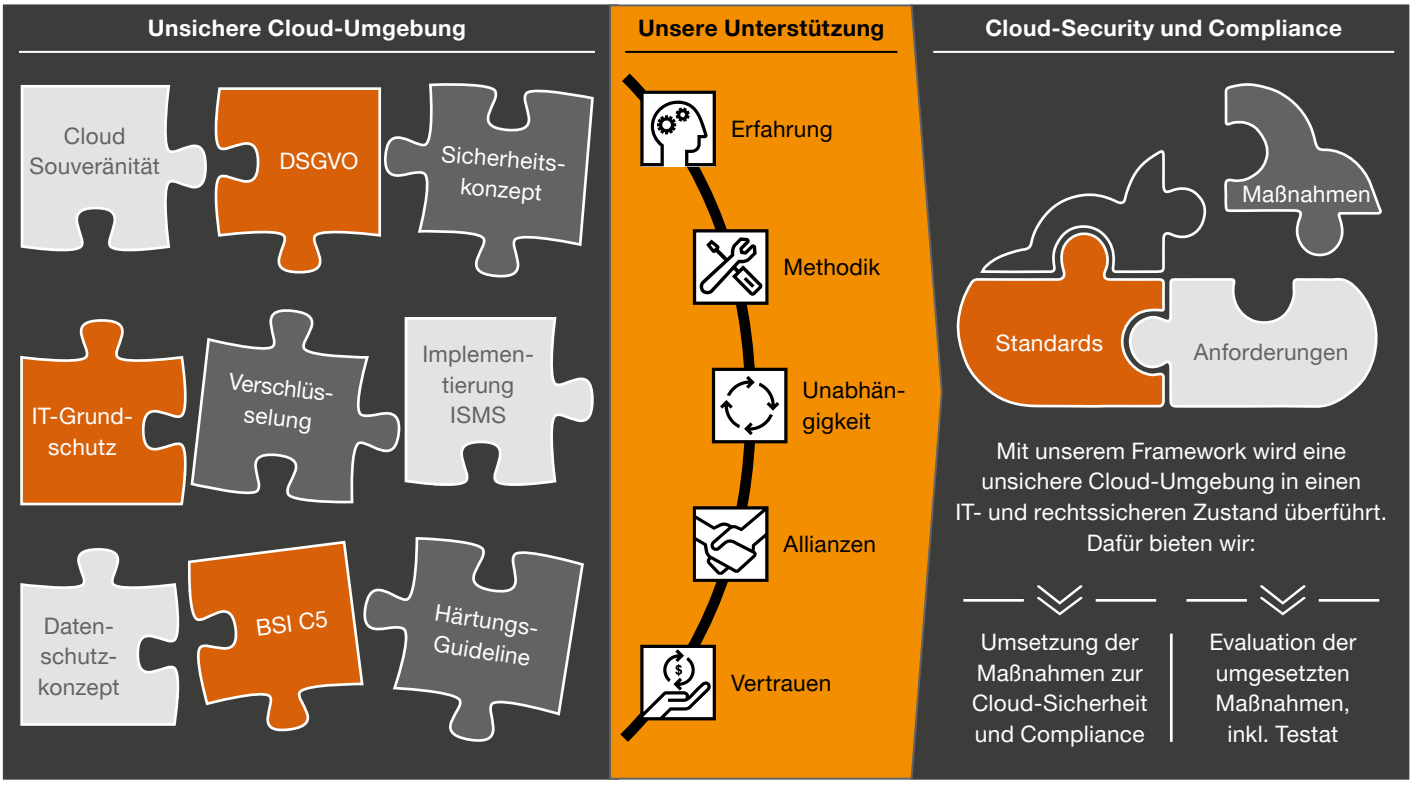
Darüber hinaus sind bestimmte Anforderungen zu beachten, um eine sichere Cloud-Infrastruktur zu gewährleisten. Dazu gehört die Implementierung eines Informationssicherheitsmanagementsystems (ISMS), um Risiken proaktiv zu identifizieren und zu bewältigen. Die Cloud-Souveränität spielt ebenfalls eine entscheidende Rolle, da sie sicherstellt, dass die Kontrolle über die Daten und Systeme in der Hand der Organisation bleibt. Ein umfassendes Datenschutzkonzept ist ebenfalls unerlässlich, um die Einhaltung der DSGVO sicherzustellen und das Vertrauen der Bürger in den Umgang mit ihren Daten zu stärken.

Maßnahmen

Um diesen Anforderungen gerecht zu werden, sind verschiedene Maßnahmen erforderlich. Dazu gehören die Erstellung eines umfassenden Sicherheitskonzepts, das alle relevanten Aspekte der Cloud-Sicherheit abdeckt. Eine Härtungs-Guideline hilft dabei, die Sicherheit der Cloud-Infrastruktur durch die Implementierung von Best Practices und Sicherheitsrichtlinien zu verbessern. Dazu zählt auch der Einsatz von Cloud-nativen Security Tools wie beispielsweise der Microsoft Defender for Cloud oder das SIEM Tool Sentinel. Darüber hinaus ist die Verschlüsselung ein wesentlicher Bestandteil der Cloud-Sicherheit, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten.

Indem öffentliche Institutionen sich an diese Standards, Anforderungen und Maßnahmen halten, können sie einen sicheren Weg in die Cloud einschlagen und damit die Vorteile der Cloud-Nutzung voll ausschöpfen. Dies ist vor allem dann der Fall, wenn so auch der Einsatz einer Public Cloud wie Microsoft Azure möglich ist.

Aus einer unsicheren Cloud-Umgebung wird mit unserer Unterstützung eine IT- und rechtssichere Lösung.



Wie sollten Ihre Cloud-Architektur und die ersten Schritte zur Cloud-Sicherheit und Compliance aussehen?

Cloud-Architektur

Für Cloud-Architekturen gibt es folgende Möglichkeiten, die je nach Anwendungsfall kombiniert werden sollten:

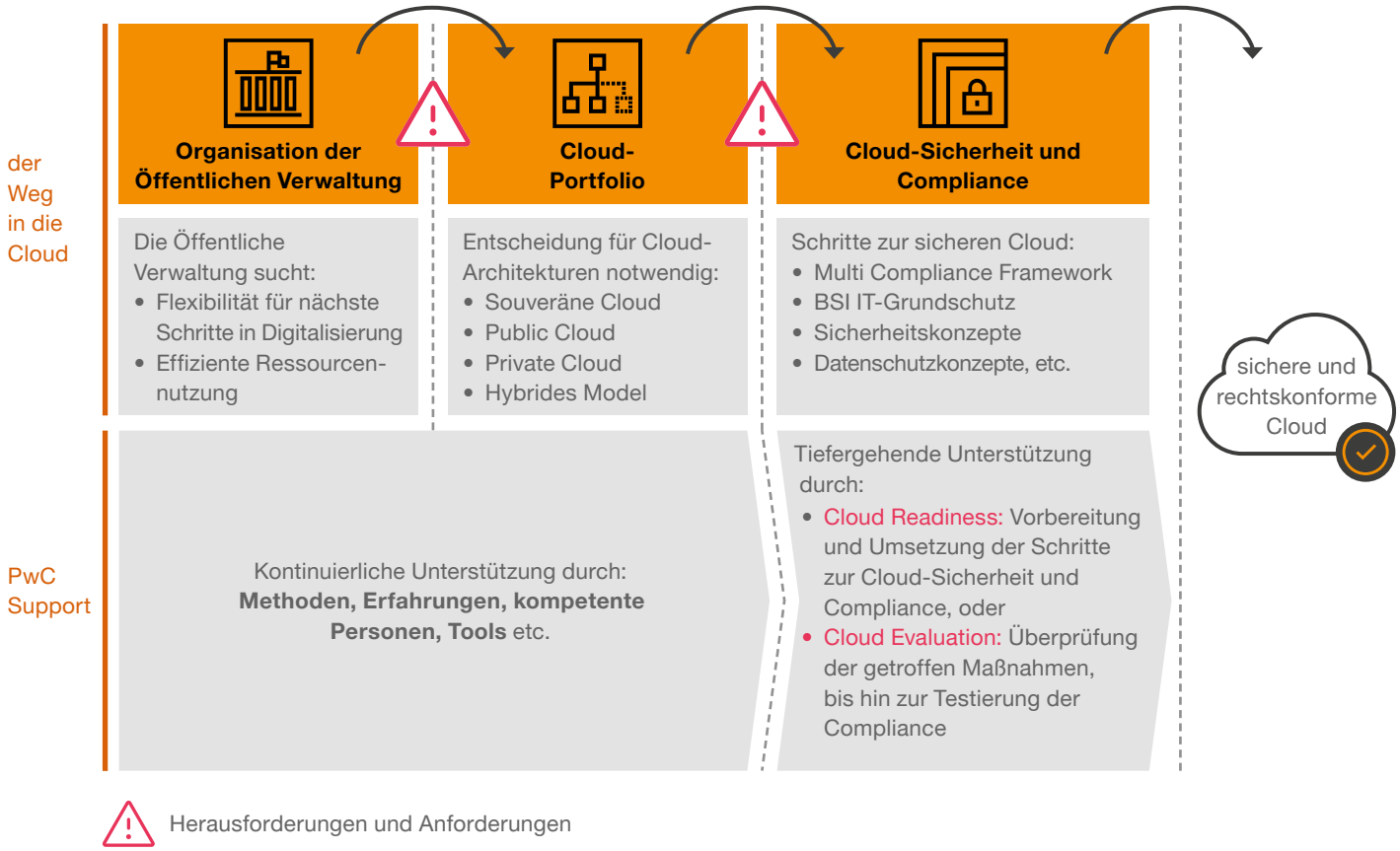
- Souveräne Cloud: Die souveräne Cloud erfüllt die höchsten Ansprüche des BSI und erlaubt hohen Einfluss auf die Daten, den Betrieb und die verwendete Technik. Beispiel: Delos Cloud
- Public Cloud: Die Public Cloud ist für grundsätzlich jeden nutzbar und verspricht eine hohe Leistungsfähigkeit bei geringen Kosten, wobei verschiedene Tools zu deren Sicherheit und Compliance eingesetzt werden. Beispiel: Microsoft Azure, Amazon Web Service (AWS)
- Private Cloud: Die Private Cloud verfügt über eine dedizierte Infrastruktur für den jeweiligen Kunden und erlaubt somit hohen Einfluss auf Maßnahmen für Sicherheit und Compliance. Beispiel: Private Cloud der T-Systems
- Hybrides Modell: Eine Mischung von verschiedenen Cloud-Arten, je nach Anforderungen der Daten

Handlungsleitfaden

Folgende Schritte sollten zuerst unternommen werden, um Sicherheit und Compliance in der Cloud zu ermöglichen:

- Aufbau eines Multi-Compliance Frameworks, zur Einhaltung der zahlreichen Standards und Anforderungen
- Aufbau eines Multi-Compliance Management Systems zur Umsetzung und Steuerung von Vorgaben und Anforderungen, inklusive der engen Verbindung mit bestehenden Management Systemen z. B. für Informationssicherheit (ISMS) oder Qualität (QMS)
- Umsetzung eines BSI IT-Grundschutz-Check und Ableitung von entsprechenden Maßnahmen
- Checklisten und/oder Mängellisten für zahlreiche Standards und Anforderungen
- Entwicklung und Umsetzung von Sicherheits- und Datenschutz-Konzepten: Sowohl organisatorisch als auch technisch, zum Beispiel durch die Nutzung von Tools wie Microsoft Defender for Cloud.

Auf dem Weg in eine sichere und rechtskonforme Cloud kann PwC gemeinsam mit Strategy& vielfältig unterstützen



Ihre Ansprechpersonen

PwC Deutschland

Regulatorik

André Glenzer
Partner
Tel.: +49 160 94470376
andre.glenzer@pwc.com

Cloud Security

Aleksei Resetko
Partner
Tel.: +49 1511 4268214
aleksei.resetko@pwc.com

Jonas Winkel
Manager
Tel.: +49 1515 2891453
jonas.winkel@pwc.com

Microsoft Deutschland

Antje Buchholz
Manager
Tel.: +49 89 31765902
antje.buchholz@microsoft.com

Dominik Roithmeier
Security Specialist
Tel.: +49 172 7162201
droithmeier@microsoft.com

Über uns
Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 151 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Mehr als 14.000 engagierte Menschen an 20 Standorten. Rund 2,93 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

www.pwc.de