

Cloud Computing als politische Herausforderung

Vielen ist „die Cloud“ ein Begriff, fast alle verwenden ihn. Die größten Anbieter kommen aus den USA,¹ Europa hinkt trotz einiger Bemühungen nach wie vor hinterher. Unter Cloud Computing versteht man Dienste, um Daten zu speichern und auf diese über das Internet zugreifen zu können. Cloud Services sind aber auch gemietete Software und Rechenleistung aus unterschiedlichen Rechenzentren eines Betreibers. Für die NutzerInnen ist dabei oft völlig unklar, wo genau ihre Daten tatsächlich gespeichert sind bzw. woher sie ihre Software beziehen.

Cloud Computing lässt sich als spezielle Form des IT-Outsourcings begreifen. Dementsprechend ergeben sich ähnliche Probleme, insbesondere was die Abhängigkeit von Anbietern betrifft. Verstärkt wird dies noch durch die Intransparenz für die NutzerInnen. Cloud Computing bietet zwar mehr Flexibilität und Datenmobilität, es ist aber im Grunde eine virtuelle Form der Zentralisierung. Damit ergeben sich noch mehr Abhängigkeit und Gefahren für Ausfälle – also weniger Ausfallsicherheit.² Die Resilienz eines Unternehmens ist somit von der Resilienz des Cloud-Betreibers abhängig.

Insbesondere für staatliche Stellen und gesellschaftlich relevante Institutionen und Unternehmen können Cloud Services als kritische Infrastrukturen begriffen werden. Wie kann im Sinne der digitalen Souveränität der Akteure (siehe auch Thema [Digitale Souveränität](#)) ein möglichst minimiertes Risiko erzielt werden? Sind die Nutzungsbedingungen und vor allem die Diversifizierung des Dienstleister-Portfolios hinreichend?

Im globalen Wettbewerb sind insbesondere Microsoft, Amazon und IBM mit etwa einem Drittel Marktanteil relevante Akteure,³ die aus europäischer Sicht kritischer Beurteilung bedürfen. Dies umso mehr, als in Zeiten der Covid-19-Pandemie deutlich wurde, dass an vielen öffentlichen und privaten Stellen US-amerikanische Cloud Services verstärkt genutzt werden und damit weitere Abhängigkeiten geschaffen werden. Eine besondere Bedeutung haben dabei die Themen Datenhoheit, Schutz der Privatsphäre und die Anfälligkeit für Missbrauch. Eine steigende Anzahl an Datenverlusten verdeutlicht dementsprechende Gefahren für die Privatsphäre des Einzelnen genauso wie für sensible Geschäftsdaten und die Funktionsfähigkeit wirtschaftlicher und gesellschaftlicher Prozesse (Leimbach et al. 2014).⁴

¹ de.statista.com/statistik/daten/studie/150979/umfrage/marktanteile-der-fuehrenden-unternehmen-im-bereich-cloud-computing/.

² heise.de/newsticker/meldung/Blitzschlag-in-den-USA-stoert-Azure-Active-Directory-4155496.html; wired.de/collection/tech/amazon-cloud-ausfall-ein-simpler-tippfehler-war-schuld.

³ Amazon bekommt auch das Cloud-Monopol für das US-Militär, siehe fm4.orf.at/stories/2942129/.

⁴ Siehe auch kaspersky.com/about/press-releases/2018_costly-cloud-breaches; blog.storagecraft.com/7-infamous-cloud-security-breaches/; forbes.com/sites/louiscolombus/2018/07/27/ibms-2018-data-breach-study-shows-why-were-in-a-zero-trust-world-now/#.

Mit der Datenschutzgrundverordnung verfügt die EU nun über einen mehr oder weniger vereinheitlichten Rechtsrahmen, was die Entstehung europäischer Anbieter befördern könnte. Das deutlich bessere Datenschutzniveau in der EU kann auch global als positiver Wettbewerbsfaktor genutzt werden. Dementsprechend wurde die European Open Science Cloud (EOSC)-Initiative⁵ ins Leben gerufen, um eine Plattform zum Austausch von Daten für ForscherInnen, Innovatoren und Unternehmen sowie BürgerInnen bereitzustellen. Als weitere europäische Initiative gilt GAIA-X,⁶ die einen gemeinsamen Rahmen und Standards für den Datenaustausch in Cloud-Lösungen zu etablieren versucht. Nicht zuletzt wird in der im Februar 2020 vorgestellten Datenstrategie der Europäischen Kommission Cloud-Lösungen eine hohe Priorität zugewiesen.⁷

Darüber hinaus besteht Bedarf an offenen, und damit überprüfbaren Sicherheitsstandards und Cloud-Architekturen (siehe Thema [Dezentralisierte Kollaborationsformen](#)), sodass sichergestellt werden kann, dass keine Hintertüren oder sog. „lawful interception“-Schnittstellen zum legalen Abhören eingeplant sind, die die Sicherheit von Cloud Services (auch als [kritische Infrastruktur](#)) massiv gefährden. Mögliche Regulierungen zum besonderen Schutz und dem Verbot der Weitergabe von Cloud-Daten an Dritte könnten angedacht werden. Insgesamt könnten die Rahmenbedingungen und mögliche Erfolgsfaktoren für eine erfolgreiche europäische/österreichische Initiative ausgelotet werden.

Zitierte Quellen

Leimbach, T. et al. (2014) Potential and Impacts of Cloud Computing Services and Social Network Websites – Study IP/A/STOA/FWC/2008-096/Lot4/C1/SC8; Science and Technology Options Assessment – European Parliamentary Research Service: Brussels, [europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET\(2014\)513546_EN.pdf](http://europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf).

⁵ eosc-portal.eu.

⁶ gaia-x.eu.

⁷ ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf.