Simulierte Souveränität

Ein altbekannter Begriff schleicht sich in den letzten Jahren verstärkt in die Schlagwortgewitter von Cloud-Anbietern, in Strategiepapiere der EU und selbst in den nachverhandelten Haushaltsplan des Bundes ein: digitale Souveränität. Souveränität war in der Vergangenheit eigentlich auf das Individuum gemünzt: Unter Datensouveränität verstand man, selbst entscheiden zu können, ob und wohin die eigenen Nutzerdaten abfließen – lösbar mit Open Source, politisch umgesetzt mit Cookiebannern.

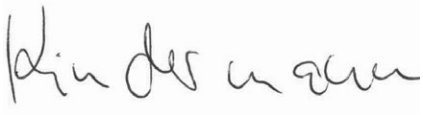
Mittlerweile ist der Begriff aber weiter gefasst. Deutschland macht sich Sorgen um seine digitale Souveränität, die EU bezeichnet sie als wichtiges Ziel ihrer Digitalstrategie – und die Hyperscaler richten „Souvereign Cloud Regions“ ein. Das sei wichtig, um Unternehmen, Verwaltung und Bürger zu schützen. Schließlich wäre es unschön, wenn sich Unternehmen anderer Länder einen unfairen Wettbewerbsvorteil verschaffen könnten – durch Geschäftsgeheimnisse oder die mühsam gesammelten IoT- und Nutzerdaten heimischer Betriebe, die in irgendwelchen internationalen Clouds liegen. Im Ernstfall hätte ein Staat die Macht, Cloud-Strukturen in Konkurrenzländern einfach abzuschalten. Und Insolvenzen oder Übernahmen können jedwede Cloud-Struktur in Firmenhand kompromittieren. Es geht hier also nicht mehr nur um Privatsphäre, sondern um Geld und kritische Infrastruktur – plötzlich gibt es Handlungsbedarf.

Auf den Bedarf reagieren die Cloud-Anbieter gerne mit dem Versprechen, ihre Services in Rechenzentren anzubieten, die sich auf geschütztem Boden befinden. Überall dort, wo die deutsche DSGVO wirkt, ist die Cloud souverän, oder anders: Datenhoheit per Baukran. Die Grundidee ist dabei nicht verkehrt, denn gerade nach relevanten Gesetzgebungen wie dem EU Data Act wäre es gut, wenn man im Notfall auch auf die Geräte schauen könnte, um das Einhalten von Richtlinien zu gewährleisten.

Nur leider bleiben diese „souveränen“ Clouds auch dann noch Teil der Struktur internationaler Hyperscaler, wenn sie auf deutschem Boden stehen. Die Software bleibt ein proprietäres Gewächs und die Schaltzentrale sitzt weiterhin in den USA. Dort hat der Geheimdienst aber immer noch unbeschränkten Zugriff auf jeden Datentropfen, der sich im System der Hyperscaler bewegt. Und wandert der Blick zum Nutzer, dorthin, wo ein großer Teil der mitunter sensiblen Datenhaufen entsteht, erschließt sich schnell, dass IoT-Geräte, Smartphones, Apps oder Heimrechner ihre Nutzerdaten sowieso nicht in einer souveränen deutschen Cloud sammeln würden, sondern viel lieber nach Hause in die USA oder nach China funken.

Die Politik selbst macht hierbei einen Schritt vor und zwei zurück: Um Unabhängigkeit zu erlangen, begibt sie sich nur allzu schnell in die Hände derer, die etwas von der Cloud verstehen, von denen sie sich eigentlich aber hätte unabhängig machen müssen. Der Bund versuchte das schon Jahre zuvor mit der Deutschland Cloud – ausgerechnet in Partnerschaft mit Microsoft. Zurzeit wird die Verwaltung in die Cloud gehievt – wofür es erst mal Einkäufe in Milliardenhöhe bei Oracle braucht.

Die eigentlich wirksame Maßnahme, um echte Souveränität zu gewährleisten, liegt auf der Hand: quelloffene Systeme, in denen Datentransfers nachvollzogen werden können. Ansätze wie der offene Souvereign Cloud Stack, der auch unter Gaia-X liegt, weisen dabei in die richtige Richtung. Währenddessen streicht man die Förderung von FOSS im diesjährigen Haushaltsplan aber auf die Hälfte zusammen und ordert proprietäre Systeme mit dem „Souverän“-Aufkleber kräftig nach. Die Entscheider hören das Werbeversprechen zu gerne und die Anbieter geben es genauso gerne ab – lieber simulierte Souveränität als echte Unabhängigkeit.



KORNELIUS KINDERMANN

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover