Digitale Souveränität

Maßnahmen zum Schutz

[10.02.2020] Cloud-Dienste und die Abhängigkeit von großen Playern gefährden die digitale Souveränität des Staates. Fünf Maßnahmen können zum Schutz dieser Souveränität beitragen. Der Weg ist nicht leicht, aber es gibt keine Alternative.

Die Digitalisierung hat die Geschäftsmodelle der Software-Branche verändert. Immer mehr Hersteller verlagern ihre Lösungen in die Cloud. On premise, also lizenzbasierte Modelle für die Nutzung von Software, die lokal in eigener Verantwortung betrieben wird – das war gestern. Cloud Computing gestaltet Vertrieb und Nutzung von Software einfacher für alle: Hersteller können ihre Geschäftsmodelle an den Kundenbedarf anpassen, die Kunden wiederum profitieren davon, dass sie die Software überall über das Web nutzen können. Solange diese Balance nicht gestört wird, ist alles gut. Ein Risiko besteht jedoch dann, wenn es zu Störungen kommt. Sei es, dass der Zugriff auf die Cloud-Services wegen Netzproblemen nicht funktioniert. Sei es, dass dieser Zugriff absichtlich unterbrochen wurde, zum Beispiel, weil in einem eskalierten Handelsstreit zwischen den Vereinigten Staaten von Amerika und der EU Cloud-Dienste US-amerikanischer Hersteller für europäische Kunden nicht mehr verfügbar sind.

Digitale Lebensadern der Verwaltung gekappt

Man stelle sich vor, eine Behörde irgendwo in Deutschland wird arbeitsunfähig, weil ihnen der Zugriff auf den Teil ihrer IT verwehrt wird, der Cloud-Dienste nutzt, die in den Vereinigten Staaten verwaltet werden. Grund sind die großen Abhängigkeiten in der Informationstechnik von einzelnen Anbietern. Ein solches Szenario kann folgendermaßen entstehen:
Im Sommer 2018 sind die Beziehungen zwischen den USA und der Europäischen Union auf einem Tiefpunkt. US-Präsident Donald Trump hat einen Handelsstreit vom Zaun gebrochen, um die heimische Wirtschaft zu bevorzugen. Damit widerspricht er den Regeln des Freihandels. Fiktiv weitergedacht: Der Präsident will noch mehr Druck auf die EU ausüben und schaltet IT-Services ab, die in Europa aus den Vereinigten Staaten erbracht werden. Hiesige Behörden oder Unternehmen können von jetzt auf gleich nicht mehr auf ihre Software oder Daten zugreifen, die in US-amerikanischen Clouds gespeichert sind. Was dazu führte, dass die digitalen Lebensadern der deutschen Verwaltung gekappt sind, von der Kommune in der Altmark und im Westerwald bis zu Parlament und Regierung in Berlin.
Dieses Szenario ist nicht übertrieben, denn im digitalen Zeitalter ist die Informationstechnik das Betriebssystem für fast alle und alles. Verwaltung, Wirtschaft, Privatleben – ohne IT kaum noch denkbar. Bitter erleben mussten das zum Beispiel im vergangenen Jahr Neustadt am Rübenberge und das Berliner Kammergericht. Wochenlang arbeiteten ihre Verwaltungen ungewollt offline und wieder mit Papier, weil Kriminelle ihre IT lahmgelegt hatten.

Kernaufgabe des Staates

Die fiktiv kaltgestellte Verwaltung und die wirklich angegriffenen Behörden eint eines: Ihre digitale Souveränität wurde verletzt. Mit digitaler Souveränität ist gemeint: Die Hoheit über die eigenen Daten oder die vom Staat genutzten IT-Infrastrukturen zu haben und zu wahren. Wenn die IT eines Staates ausfällt oder geschädigt wird, kann er seinen Aufgaben nicht mehr nachkommen. Ein Staat, der seine digitale Souveränität nicht verteidigen kann, ist ein schwacher Staat. Er kann manipuliert, gehackt, ausspioniert

werden. Dann ist in der Folge auch die digitale Souveränität der Bürger verletzt. Denn ein angreifbarer Staat kann nicht mehr garantieren, die Daten seiner Bürger zu schützen.
Digitale Souveränität kann von vielen Seiten bedroht werden. Es braucht dazu keinen fiktiv so eskalierten Handelsstreit. Man denke nur an die 2019 geführte Debatte, ob der chinesische Netzwerkausrüster Huawei Deutschland mit seiner 5G-Technik auf- und ausrüsten darf. Kritiker befürchten den Kill Switch, also die Möglichkeit, dass Deutschlands Netze über eingebaute Hintertüren aus China manipuliert werden können.
Es gibt Stimmen, die sagen, Daten seien das Öl des 21. Jahrhunderts. In der Tat sind sie kostbar: für Staat und Wirtschaft Basis für das Verwalten und Geschäfte, für jeden Einzelnen ein digitales Abbild seiner Identität. Wer unsere Daten hat, der kennt uns – mal mehr, mal weniger. Im digitalen Zeitalter gehört der Schutz der digitalen Souveränität deshalb zu den Kernaufgaben des Staates. Fünf Maßnahmen tragen dazu bei.

Alternativen suchen und entwickeln

Erstens ist der Schutz der digitalen Souveränität eng an die Sicherheit von IT-Infrastrukturen gebunden. Als Betreiber der staatlichen Informationstechnik ist es vor allem die Aufgabe öffentlicher IT-Dienstleister, die ihnen anvertrauten IT-Systeme und Daten zu schützen. Das bedeutet in der praktischen Umsetzung auf vielen Ebenen Vorsorge zu treffen, um die Unverletzlichkeit der staatlichen IT herzustellen, zum Beispiel durch den Betrieb von sicheren Rechenzentren und Netzen, einen datenschutzkonformen Betrieb von Software, vertrauenswürdige und datenschutzkonforme Cloud-Lösungen und ein professionelles IT-Management. IT-Sicherheit ist dabei ein ständiger Prozess. Technik verändert sich; Maßnahmen für IT-Sicherheit müssen stets angepasst und präventiv vorgedacht werden.
Als zweite Maßnahme müssen Abhängigkeiten vermieden werden. Das Szenario „Präsident dreht den Hahn ab“ kann nur dann Wirklichkeit werden, wenn die Abhängigkeit von einzelnen Infrastrukturen oder bestimmten Herstellern sehr groß ist. Wer alles auf ein Pferd setzt, kann alles verlieren. Der IT-Dienstleister Dataport zum Beispiel verfolgt deshalb schon seit seiner Unternehmensgründung eine Multi-Supplier-Strategie, setzt also bei der Beschaffung auf mehrere Hersteller.
Es gibt natürlich Marktmächte, an denen Verwaltung wie IT-Dienstleister bislang kaum vorbeikommen. Deshalb müssen der Staat und seine Dienstleister Alternativen suchen oder entwickeln. Das ist die dritte Maßnahme. Alternativen zu marktbeherrschenden Produkten können Open-Source-Lösungen sein. Dataport entwickelt gerade für das Land Schleswig-Holstein eine Open-Source-Lösung, die in Schulen Produkte der gängigen und marktbeherrschenden Microsoft Suite ablösen soll.

Gemeinsam stark

Die vierte Maßnahme ist ein gemeinsames Handeln. Nur so wird es möglich sein, sich gegenüber großen Playern zu behaupten. Kein öffentlicher IT-Dienstleister wird sich alleine gegen globale Interessen von IT-Riesen oder mächtigen Präsidenten durchsetzen. Nur mit Kooperation und gebündelten Kompetenzen wird es gelingen, ein ernsthaftes Gegengewicht zu schaffen, das allzu großen technischen Abhängigkeiten gegenüber den großen Playern vorbeugt und Alternativen schafft. Dafür müssen föderale Schranken überwunden werden, die Kooperationen und das arbeitsteilige Entwickeln von wegweisenden Lösungen oft noch erschweren. Das Ziel sollte eine Cloud der öffentlichen IT-Dienstleister sein, die aus ihren sicheren Rechenzentren gemeinsam Services für alle Verwaltungen erbringen.
Fünftens sollten sich die deutsche Politik, ihre Verwaltung und ihre IT-Dienstleister so aufstellen, dass im Chor mit entsprechenden Stimmen aus Europa ein ernsthaftes Gegengewicht entsteht zu politischen, wirtschaftlichen oder schlicht auch kriminellen Akteuren, die – mit welcher Motivation auch immer – die digitale Souveränität von Staaten und Bürgern brechen können und damit auch die Souveränität des

Bürgermeisters in der Altmark oder im Westerwald gefährden. Das ist kein leichter Weg. Aber es gibt keine Alternative.

()

Dieser Beitrag ist in der Ausgabe Februar 2020 von Kommune21 im Schwerpunkt Digitale Souveränität erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Cloud Computing, Digitale Souveränität